United States Department of State

Bureau for International Narcotics and Law Enforcement Affairs

International Narcotics Control Strategy Report

Volume II

Money Laundering and Financial Crimes

March 2008

Table of Contents
Volume II

Legislative Basis for the INCSR 3
Introduction 4
Mobile Payments—A Growing Threat 11
Bilateral Activities 14
Training and Technical Assistance 14
Department of State 14
International Law Enforcement Academies (ILEAs) 16
Board of Governors of the Federal Reserve System (FRB) 18
Drug Enforcement Administration (DEA), Department of Justice 19
Federal Bureau of Investigation (FBI), Department of Justice 20
Federal Deposit Insurance Corporation (FDIC) 20
Financial Crimes Enforcement Network (FinCEN), Department of Treasury 21
Immigration and Customs Enforcement, Department of Homeland Security (DHS) 22
Trade Transparency Units (TTUs) 23
Other ICE Programs 23
Internal Revenue Service (IRS), Criminal Investigative Division (CID) Department of Treasury 24
Office of the Comptroller of the Currency (OCC), Department of Treasury 26
Office of Overseas Prosecutorial Development, Assistance and Training, the Asset Forfeiture and Money Laundering Section, & Counterterrorism Section (OPDAT, AFMLS, and CTS), Department of Justice 27
Training and Technical Assistance 27
Money Laundering/Asset Forfeiture 27
Resident Legal Advisors 29
Terrorism/Terrorist Financing 29
Organized Crime 32
Fraud/Anticorruption 33
Justice Sector Reform 35
Office of Technical Assistance (OTA), Treasury Department 36
Assessing Training and Technical Assistance Needs 36
Anti-Money Laundering and Counter-Terrorist Financing Training 37
Support for Financial Intelligence Units 38
Casino Gaming 38
Money Services Businesses 38
Insurance 39
Regional and Resident Advisors 39
Treaties and Agreements 40
Treaties 40
Agreements 41
Multi-Lateral Organizations & Programs 42
The Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRBs) 42
The Egmont Group of Financial Intelligence Units 43

The Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering *45*
Training and Technical Assistance 45
Pacific Anti-Money Laundering Program (PALP) *46*
Mentoring 46
Legislative Drafting 47
Capacity Building Initiatives 48
Case support 49
Mutual evaluations 50
United Nations Global Programme Against Money Laundering *50*
The Mentoring Program 51
Mentoring & Financial Intelligence Units 52
Computer-Based Training 52
Other GPML Initiatives 53
Law Enforcement Cases **54**
Operation TNT—Contract Fraud 54
Drug Trafficking Organization—Laundering via Bulk Cash Smuggling and the Purchase of Real Estate and Automobiles 54
Trade-based Money Laundering/Black Market Exchange 55
Bulk Cash Smuggling, Casas de Cambio, and the Black Market Peso Exchange 55
Recent Terrorist Financing Prosecutions 55
Holy Land Foundation 56
Chiquita Brands Pays Terrorist Group AUC 56
Money Laundering to Support Terrorism 56
Material Support to Hamas 57
Rendering Assistance to a Khalistan Commando Force 57
Major Money Laundering Countries **58**
Vulnerability Factors *59*
Changes in INCSR Priorities for 2007 ..... *60*
Country/Jurisdiction Table *62*
Introduction to Comparative Table *63*
Comparative Table *65*
Country Reports **74**
Afghanistan 74
Albania 78
Algeria 81
Angola 83
Antigua and Barbuda 84
Argentina 87
Aruba 91
Australia 93
Austria 98
Bahamas 102
Bahrain 105
Bangladesh 108
Barbados 110
Belarus 113
Belgium 117
Belize 122
Bolivia 125
Bosnia and Herzegovina 129
Brazil 132

British Virgin Islands 136
Bulgaria 139
Burma 143
Cambodia 146
Canada 149
Cayman Islands 152
Chile 154
China, People's Republic of 159
Colombia 163
Comoros 168
Cook Islands 171
Costa Rica 174
Côte d'Ivoire 177
Cyprus 181
Czech Republic 187
Dominica 192
Dominican Republic 195
Ecuador 197
Egypt, The Arab Republic of 200
El Salvador 203
France 206
Germany 208
Ghana 211
Gibraltar 214
Greece 216
Grenada 221
Guatemala 223
Guernsey 227
Guinea-Bissau 229
Guyana 232
Haiti 233
Honduras 236
Hong Kong 240
Hungary 244
India 248
Indonesia 253
Iran 257
Iraq 260
Ireland 264
Isle of Man 267
Israel 270
Italy 274
Jamaica 277
Japan 280
Jersey 284
Jordan 287
Kenya 290
Korea, Democratic Peoples Republic of 293
Korea, Republic of 294
Kuwait 298
Laos 301
Latvia 303
Lebanon 308
Liechtenstein 312
Luxembourg 314
Macau 318

Malaysia 323
Mexico 327
Moldova 331
Monaco 335
Morocco 338
The Netherlands 339
Netherlands Antilles 345
Nicaragua 347
Nigeria 351
Pakistan 355
Palau 358
Panama 361
Paraguay 365
Peru 369
Philippines 373
Poland 377
Portugal 380
Qatar 383
Romania 386
Russia 390
Samoa 394
Saudi Arabia 396
Senegal 398
Serbia 401
Seychelles 404
Sierra Leone 407
Singapore 409
Slovak Republic 413
South Africa 417
Spain 419
St. Kitts and Nevis 425
St. Lucia 427
St. Vincent and the Grenadines 429
Suriname 431
Switzerland 434
Syria 438
Taiwan 442
Tanzania 447
Thailand 448
Turkey 453
Turks and Caicos 457
Ukraine 459
United Arab Emirates 463
United Kingdom 470
Uruguay 474
Uzbekistan 476
Vanuatu 481
Venezuela 484
Vietnam 487
Yemen 490
Zimbabwe 492

Common Abbreviations

AML	Anti-Money Laundering
APG	Asia/Pacific Group on Money Laundering
ARS	Alternative Remittance System
CFATF	Caribbean Financial Action Task Force
CTF	Counter-Terrorist Financing
CTR	Currency Transaction Report
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
DOS	Department of State
EAG	Eurasian Group to Combat Money Laundering and Terrorist Financing
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
GAFISUD	Financial Action Task Force on Money Laundering in South America
GIABA	Inter-Governmental Action Group against Money Laundering
IBC	International Business Company
ICE	U.S. Immigration and Customs Enforcement
IFI	International Financial Institution
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
INL	Bureau for International Narcotics and Law Enforcement Affairs
IRS	Internal Revenue Service
IRS-CID	Internal Revenue Service, Criminal Investigative Division
MENAFATF	Middle East and North Africa Financial Action Task Force
MLAT	Mutual Legal Assistance Treaty
MOU	Memorandum of Understanding
NCCT	Non-Cooperative Countries or Territories
OAS	Organization of American States
OAS/CICAD	OAS Inter-American Drug Abuse Control Commission
OFC	Offshore Financial Center
PIF	Pacific Islands Forum
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
UN Drug Convention	1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
UNGPML	United Nations Global Programme against Money Laundering
UNODC	United Nations Office for Drug Control and Crime Prevention
UNSCR	United Nations Security Council Resolution
USAID	Agency for International Development
USG	United States Government

MONEY LAUNDERING AND FINANCIAL CRIMES

Legislative Basis for the INCSR

The Money Laundering and Financial Crimes section of the Department of State's International Narcotics Control Strategy Report (INCSR) has been prepared in accordance with section 489 of the Foreign Assistance Act of 1961, as amended (the "FAA," 22 U.S.C. § 2291). The 2008 INCSR is the 25th annual report prepared pursuant to the FAA.[1]

The FAA requires a report on the extent to which each country or entity that received assistance under chapter 8 of Part I of the Foreign Assistance Act in the past two fiscal years has "met the goals and objectives of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances" (the "1988 UN Drug Convention")(FAA § 489(a)(1)(A)).

Although the Convention does not contain a list of goals and objectives, it does set forth a number of obligations that the parties agree to undertake. Generally speaking, it requires the parties to take legal measures to outlaw and punish all forms of illicit drug production, trafficking, and drug money laundering: to control chemicals that can be used to process illicit drugs; and to cooperate in international efforts to these ends. The statute lists action by foreign countries on the following issues as relevant to evaluating performance under the 1988 UN Drug Convention: illicit cultivation, production, distribution, sale, transport and financing, money laundering, asset seizure, extradition, mutual legal assistance, law enforcement and transit cooperation, precursor chemical control, and demand reduction.

In attempting to evaluate whether countries and certain entities are meeting the goals and objectives of the 1988 UN Drug Convention, the Department has used the best information it has available. The 2008 INCSR covers countries that range from major drug producing and drug-transit countries, where drug control is a critical element of national policy, to small countries or entities where drug issues or the capacity to deal with them are minimal. In addition to identifying countries as major sources of precursor chemicals used in the production of illicit narcotics, the INCSR is mandated to identify major money laundering countries (FAA §489(a)(3)(C)). The INCSR is also required to report findings on each country's adoption of laws and regulations to prevent narcotics-related money laundering (FAA §489(a)(7)(c). This report is the section of the INCSR that reports on money laundering and financial crimes.

A major money laundering country is defined by statute as one "whose financial institutions engage in currency transactions involving significant amounts of proceeds from international narcotics trafficking" (FAA § 481(e)(7)). However, the complex nature of money laundering transactions today makes it difficult in many cases to distinguish the proceeds of narcotics trafficking from the proceeds of other serious crime. Moreover, financial institutions engaging in transactions involving significant amounts of proceeds of other serious crime are vulnerable to narcotics-related money laundering. This

[1] The 2008 report on Money Laundering and Financial Crimes is a legislatively mandated section of the U.S. Department of State's annual International Narcotics Control Strategy Report. This 2008 report on Money Laundering and Financial Crimes is based upon the contributions of numerous U.S. Government agencies and international sources. A principal contributor is the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), which, as a member of the international Egmont Group of Financial Intelligence Units, has unique strategic and tactical perspective on international anti-money laundering developments. FinCEN is the primary contributor to the individual country reports. Another key contributor is the U.S. Department of Justice's Asset Forfeiture and Money Laundering Section (AFMLS) of Justice's Criminal Division, which plays a central role in constructing the Money Laundering and Financial Crimes Comparative Table and provides international training. Many other agencies also provided information on international training as well as technical and other assistance, including the following: Department of Homeland Security's Bureau of Immigration and Customs Enforcement; Department of Justice's Drug Enforcement Administration, Federal Bureau of Investigation, and Office for Overseas Prosecutorial Development Assistance; and Treasury's Internal Revenue Service, the Office of the Comptroller of the Currency, and the Office of Technical Assistance. Also providing information on training and technical assistance are the independent regulatory agencies, Federal Deposit Insurance Corporation, and the Federal Reserve Board.

year's list of major money laundering countries recognizes this relationship by including all countries and other jurisdictions whose financial institutions engage in transactions involving significant amounts of proceeds from all serious crime. The following countries/jurisdictions have been identified this year in this category:

Major Money Laundering Countries in 2008

Afghanistan, Antigua and Barbuda, Australia, Austria, Bahamas, Belize, Brazil, Burma, Cambodia, Canada, Cayman Islands, China, Colombia, Costa Rica, Cyprus, Dominican Republic, France, Germany, Greece, Guatemala, Guernsey, Haiti, Hong Kong, India, Indonesia, Iran, Isle of Man, Israel, Italy, Japan, Jersey, Kenya, Latvia, Lebanon, Liechtenstein, Luxembourg, Macau, Mexico, Netherlands, Nigeria, Pakistan, Panama, Paraguay, Philippines, Russia, Singapore, Spain, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay, and Venezuela.

The Money Laundering and Financial Crimes section provides further information on these countries/entities and United States money laundering policies, as required by section 489 of the FAA.

Introduction

This year's Volume II of the INCSR on Money Laundering highlights continuing threats and vulnerabilities posed by money laundering and terrorist financing to U.S. national security and to the stability of the global financial system. The 2008 Volume II also reflects the current and latest trends used by criminals and terrorists to launder, move, and store the fruits of their illicit activities. Some of these methodologies include: the continuing use of banks and money service businesses as gateways to the global financial system; bulk cash smuggling; trade-based money laundering and value transfer; legal entities such off-shore financial centers and international business centers; casinos and "virtual" casinos; and new payment methods sometimes also identified as "e-money."

Twenty-five years ago, the Department of State was mandated by Congress to examine the challenges and threats from narcotics-related money laundering. Although it is sometimes difficult to obtain data on money laundering systems and trends, via reporting reflected in this edition from our worldwide diplomatic posts and the domestic law enforcement and regulatory communities, we are able to glean increasingly greater insights. We can say with certainty that the use of offshore financial centers, casinos, and the Internet is demonstrably growing at alarming rates. Virtual money laundering is a reality and at this time is immune to traditional money laundering countermeasures. If ignored, 'virtual' money laundering will pose a threat to our financial sector. In the following section, we expand on one facet of the virtual threat: "mobile payments." Similarly, in years past, Volume II has taken a leading role in early-on highlighting other typologies of concern such as the Black Market Peso Exchange (BMPE), bulk cash smuggling, and trade-based money laundering. These laundering systems are now widely recognized by many governments around the world, the Financial Action Task Force (FATF), and other international organizations.

In 2007, we continue to see that increasingly sophisticated criminal organizations, terrorists, kleptocrats and other illicit actors seek out the weak links in global anti-money laundering and counter-terrorist finance countermeasures. This report also gives numerous examples of the determination of law enforcement to dismantle these illicit activities. As of year-end 2007, nine more jurisdictions have criminalized money laundering beyond drugs, bringing the total to 180 jurisdictions that have done so. Similarly, 19 more jurisdictions have criminalized terrorist financing, bringing the total to 137.

In assessing progress in both domestic and global anti-money laundering/counter-terrorist finance efforts, historical perspective is sometimes useful. We can measure incremental steps of progress, highlight continuing areas of concern, and learn how to better focus scarce training and assistance resources. A review also reinforces the importance of these efforts. For example, the International Monetary Fund (IMF) estimates the magnitude of money laundering is about 3-5 percent of the world's Gross Domestic Product (GDP). Using 2007 World Bank data, global GDP is approximately $72.3 trillion. In other words, international money laundering can be estimated at between approximately $2.17 and $3.61 trillion a year, which is larger than the current U.S. budget. Ten years ago, the generally accepted estimate of international money laundering was in the range of $300-$500 billion. Although international economic growth accounts for a large percentage of the increase in international money laundering, there is also a greater understanding of new threats, methodologies, and diverse laundering systems. Throughout the 25 successive editions of this report, we have continued to see how, outside of crimes of passion, criminals are still primarily motivated by greed.

Volume II of the INCSR is a valuable tool to assist in our "look back." For example, a number of worrisome laundering "trends and typologies" were included in the 1997 and 1998 editions of the Money Laundering and Financial Crimes Section. The entries make familiar reading today, particularly if compared to threats articulated in the U.S. interagency 2007 National Money Laundering Strategy.

Ten years ago, one of the primary money laundering concerns was the Black Market Peso Exchange (BMPE). Earlier editions of this report have described how the Colombian cartels sell U.S. currency derived from drug trafficking to black market peso brokers in Colombia, who, with their U.S.-based agents, place the currency into U.S. bank accounts while trying to circumvent Bank Secrecy Act reporting requirements. The exchangers then sell monetary instruments drawn on their bank accounts in the United States to Colombian importers who use these instruments to purchase foreign trade goods. The 1998 report stated that the BMPE "is the single most efficient and extensive money laundering scheme in the Western Hemisphere." A review of this year's country reports shows that the BMPE is alive and well. In fact, there is increasing realization that similar black market exchange systems are found in diverse locales such as the Tri-Border region of Argentina, Brazil, and Paraguay; trade goods in Dubai and elsewhere are being purchased with Afghan drug proceeds; and Chinese and European manufactured trade items are being purchased through narcotics-driven systems similar to the BMPE.

The 1998 edition of this report stated that bulk cash smuggling is "one of the most utilized" money laundering techniques in the United States and around the world. Almost ten years later, this assessment still holds true. In 2007, the National Money Laundering Strategy stated that,

> "The smuggling of bulk currency out of the United States is the largest and most significant drug-money laundering threat facing law enforcement. Deterring direct access to U.S. financial institutions by criminals does not prevent money laundering if illicit proceeds can still reach U.S. accounts through indirect means."

As if to illustrate these observations, in January 2007, a Colombian National Police Money-Laundering Unit, trained by U.S. law enforcement authorities, seized a record $80 million worth of drug proceeds in cash and gold in one law enforcement operation in Cali, Colombia. At the time, this was the largest cash seizure in the Western Hemisphere. The record was short lived. Two months later, Mexican law enforcement authorities, working with U.S. law enforcement, raided a Mexico City residence and discovered over two tons of currency, mostly in $100 banknotes, totaling $205 million, as well an additional $2 million equivalent in other currencies. These high-profile seizures give added impetus to efforts taking place around the world to implement the FATF's Special Recommendation IX on bulk cash smuggling. The dollars, euros, pesos, various other currencies, and gold seized in the two raids constitute the face of modern day crime transactions. The seizures also highlight the global

nature of the international narcotics industry, the enormous sums of money involved, and the complexity of the money laundering challenge.

The 1998 edition of the Money Laundering and Financial Crimes section discussed how the international gold trade is being used to launder significant amounts of criminally derived funds. The report stated, "There is an obvious need for countries to have better tools to combat this problem and to monitor the international movement of gold." Ten years after this statement, it has become increasingly apparent that precious metals and stones are used to launder money, transfer value, and finance terror. (Both al Qaeda and the Taliban have publicly announced various "rewards" offered in gold for acts of terror carried out by jihadists.) Gold is both a commodity and, depending on the form, a *de facto* bearer instrument. A review of this year's edition shows that Vietnam, Saudi Arabia, Taiwan, Japan and other countries all have various forms of reporting requirements on the international transportation of gold. For example, in May 2007, the Saudi Ministry of Finance announced that people coming into and going out of the Kingdom of Saudi Arabia are required to declare to customs officials at exit and entry points the amount of cash, precious stones, jewelry, and metals such as gold that they carry with them exceeding 60,000 Saudi riyals (approximately $16,000).

More than a decade ago, U.S. criminal investigators first became concerned about trade-based money laundering by examining glaring anomalies in the international gold trade. It took the intelligence and law enforcement communities far too long to understand that historically and culturally trade is used in various forms of value transfer and to provide counter valuation in alternative remittance systems such as hawala. Shortly after September 11, the Department of State, in collaboration with the Departments of Homeland Security (DHS) and Treasury, made the combating of trade-based money laundering a key part of our anti-money laundering efforts. Since then, others have recognized this urgency, including the FATF.

Trade fraud is found around the world. It is particularly damaging in those developing countries hard-pressed for revenue. For example, according to this year's submission on Bangladesh, customs duties account for approximately 40-50 percent of annual government income. To help address these vulnerabilities, the State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL) provided funding to DHS to establish prototype Trade Transparency Units (TTUs) in the South American Tri-Border countries of Argentina, Brazil, and Paraguay. TTUs examine import and export data to identify anomalies that could be indicative of customs fraud, trade-based money laundering, and/or underground finance. The concept is simple, efficient, and expanding. It was specifically endorsed in the 2007 National Money Laundering Strategy where it was noted that, "Often the most complex money laundering methods involve the use of international trade to disguise funds transfers."

Ten years ago, this report also noted that,

> "Nonbank financial institutions (NBFIs) continue to be used as sites for money laundering in the United States despite a number of efforts at both federal and state levels, with over 200,000 NBFIs in the United States, monitoring of these businesses for money laundering is a complicated matter."

The 2007 National Money Laundering Strategy acknowledged the continuing problem and called for the enhancement of financial transparency in what is now generally called money services businesses (MSBs). MSBs include money transmitters, check cashers, currency exchangers, hawaladars, as well as issuers, sellers, and redeemers of money orders, traveler's checks, and stored value. According to the report, less than 20 percent of MSBs are registered with Treasury's Financial Crimes Enforcement Network (FinCEN), as is required. A review of FATF mutual evaluations and current country reports in this year's edition reveal that most jurisdictions are similarly struggling with issues of registration, transparency, and reporting in the MSB industry. This should come as no surprise. The 1997 INCSR discussed the challenges of regulating exchange houses and remittance systems such as "hawala in the

Middle East, cambios in Latin America, and NBFIs of all types in the Western financial community." The report prophetically added, "Systems for regulating them to discourage their use to launder the proceeds of crime are essential, but will fail unless they take into account the very informality that makes them effective and desirable."

Ten years ago, new payment technologies were in their infancy. The 1998 INCSR predicted that,

> "Electronic money (e-money) has the potential to make it easier for criminals to hide the source of their proceeds and move those proceeds without detection. While the application of new technologies to electronic or cyber-payments is still in its infancy, it is prudent to recognize their potentially broader impact. The technology exists which could permit these systems to combine the speed of the present bank-based wire transfer systems with the anonymity of currency."

The envisioned era is here. The rapid growth of global mobile payments (m-payments) demands particular attention. There are less than one billion bank accounts worldwide but approximately three billion cell phones. In some areas of the world, sending and receiving money or credit by phone is now commonplace. While m-payments have enormous potential for good, the risk that criminal and terrorist organizations will co-opt m-payment services is real. Financial transparency is problematic. Regulators and law enforcement are finding themselves hard-pressed to respond to rapid development in e-payment methodologies.

The 2007 National Money Laundering Strategy report discusses the promotion of transparency in the ownership of legal entities, particularly corporations, limited liability companies (LLCs), and trusts. This issue was elaborated on nearly a decade ago in earlier editions of the INCSR, which highlighted the growing threat posed to global financial stability by the 60 offshore financial centers (OFCs), whose defining characteristic is to a lesser or greater degree, the lack of transparency. An OFC is a jurisdiction where an intentional effort has been made to attract foreign business by deliberate government policies such as the enactment of tax and other fiscal incentives: "business friendly," lax or nonexistent supervisory regimes; freedom from common regulatory constraints, such as exchange controls and disclosure requirements; and secrecy enforced by law. OFCs also enable the formation of international business companies (IBCs), banks, trusts (some with "flee clauses"), and other vehicles formed by management and trust companies, or by intermediaries such as lawyers or accountants. Particularly troublesome are "off-the shelf" IBCs, purchased via the Internet, with nominee directors from a different country that effectively provide anonymity to the true beneficial owners.

Although 13 of the 15 jurisdictions listed by the Financial Action Task Force on its initial 2000 list of Non-Cooperative Countries and Territories (NCCTs) had OFCs or were themselves offshore financial jurisdictions, a ten-year review shows that the FATF exercise has done little to stop the growth of the offshore financial sector. In fact, the opposite appears to be true. For example, in 1998, the British Virgin Islands licensed 300,000 IBCs; today more than 800,000 are registered. Similarly, after the U.S. and the international community forced the closing of Nauru's nearly 400 shell banks, 300 banks, nearly all thought to be "shell banks," were found to be registered in the Comoros. The government of Moldova, in spite of being advised of the risk of doing so, recently considered developing its own OFC. Likewise, Jamaica is considering opening an OFC in 2009. Recently, the Government of Ghana has established an offshore financial sector, mandating that the Bank of Ghana authorize offshore banks.

The 2007 National Money Laundering Strategy stated that casinos are cash-intensive businesses that often provide financial services and money laundering opportunities. In fact, the concern that the exchange of cash for casino chips and related money transfer and account services make casinos vulnerable to money laundering has been with us for many years. Today, the number of gaming establishments in the U.S. is growing, driven by Native American tribes. Casinos on Native American

reservations bring in more money than Las Vegas and Atlantic City combined. Money laundering schemes using casinos have been reported by both domestic and foreign law enforcement.

In most parts of the world there is extensive casino development. Countries hope that gaming will provide added revenue and employment. However, particularly in the developing world, there are few anti-money laundering regulations and little oversight or control. For example, in Latin America, there is rapid casino development, but only Panama and Chile have viable AML programs in the gaming industry. Peru recently passed a new gaming law, aimed at identifying the owners of hundreds of currently unregulated gambling establishments. In the Caribbean, the industry is largely unregulated, except for in the Bahamas and the Grenadines. Casinos exist in most of sub-Saharan Africa, but only South Africa has a regulatory structure that deals with casinos. Most countries in Asia have gaming industries and observers have expressed concerns about money laundering vulnerabilities. According to the Macau country report, gaming revenue in the first nine months of 2007 exceeded the 2006 total and accounts for well over 50 percent of Macau's gross domestic product (GDP). Macau is fast approaching Las Vegas as an international gambling destination. Eastern European and Central Asian countries also face AML challenges with the industry. Diverse jurisdictions need to take their "first steps" in addressing the very real anti-money laundering threats related to casinos. It is only developed countries such as Australia, the United States, and those in Western Europe that regularly incorporate money laundering countermeasures that meet international standards in their gaming industry. However, even those countries with relatively strong oversight, the money laundering threat posed by casinos continues to grow.

So, too does the threat of "virtual casinos"—gambling via the Internet. A decade ago, 15 of the 60 offshore jurisdictions were known to have registered "virtual casinos" in their jurisdiction. Although a few such sites were located in the OFCs in the Pacific, the vast majority were located in the Caribbean Basin, with Costa Rica and Antigua and Barbuda, each reportedly having licensed hundreds of virtual casinos, with typical fees a decade ago reportedly ranging from $75,000 (for a sports betting shop) to $100,000 (for a virtual casino license.) As reported in the 1999 INCSR, the Pacific island jurisdictions were thought to generate nearly $1.2 million a month from these license fees. Internet gambling executed via the use of credit cards, Internet payment service providers, and offshore banks represents yet another powerful vehicle for criminals to launder funds from their illicit sources and to evade taxes. These Internet gaming sites are a particularly difficult problem for law enforcement, as the beneficial owner may live in one country, with the anonymous corporation registered in another country, and the server located in yet a third country. Although illegal for use by U.S. citizens, thousands of U.S. individuals have Internet gaming accounts with Internet gaming providers in foreign jurisdictions. Current estimates are that these gaming sites earn between $6 to $8 billion dollars annually from U.S. citizens alone. As such, Internet gaming has the potential of becoming a greater money laundering threat than actual physical casinos.

In spite of the continued threats by money launderers and terrorist financiers, a brief historical review of countries' AML/CTF efforts does demonstrate success stories. For example, the following is a small sampling from the country reports of miscellaneous "steps" towards progress in 2007:

- Argentina and Mexico criminalized terrorist financing.
- Italy had over 600 money laundering convictions.
- Ghana has a new anti-money laundering law.
- There has been a decline in offshore banks and trusts in the Bahamas.
- Brazil had 190 money laundering convictions.

- Israel, formerly labeled "noncooperative" under FATF's NCCT guidelines, has systematically established an AML/CTF regime that adheres to world standards, and has several on-going money laundering cases.
- Chile had four money laundering convictions, the first under its new penal system.
- Currently, Antigua and Barbuda does a very good job of regulating the Internet casinos and is probably the world leader in dealing with AML issues with the Internet gaming industry. In fact, their regulations in this area have been copied by other highly regulated Internet gaming jurisdictions such as the Isle of Man.
- The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the West African Groupe Inter-gouvernemental d'Action Contre le Blanchiment d'Argent et Le Financement du Terrorisme en Afrique de l"Oueste (GIABA) conducted their first mutual evaluations.
- Colombia had 47 money laundering convictions.
- The Republic of Korea Financial Intelligence Unit has analyzed 79,325 suspicious transaction reports and referred 7,184 cases to law enforcement, resulting in 3,661 investigations, with 1,402 cases resulting in indictments and prosecutions for money laundering.
- Armenia, Bangladesh, Bahamas, Cambodia, Canada, Costa Rica, Cuba, Gabon, Ghana, Guinea-Bissau, Kuwait, Luxembourg, Maldives, Moldova, Morocco, Pakistan, Papua New Guinea, Portugal, Qatar, Sweden, Macedonia, Uruguay, Zambia, Zimbabwe all became parties to the United Nations Convention against Corruption.
- Bosnia-Herzegovina obtained seven convictions for money laundering in the first seven months of 2007.
- China became a member of the FATF.
- The Egmont Group established a formal Secretariat and the FIUs of Armenia, Belarus, India, Nigeria, Niue and Syria became Egmont members.

Unfortunately, the review also highlights countries that are regressing, such as Uzbekistan, which suspended its AML law for the next six years, as well as continuing global AML/CTF pariahs: particularly North Korea and Iran. U.S. Treasury press releases and a 2007 entry in the U.S. Federal Register cited "the involvement of North Korean Government agencies and front companies in a wide variety of illegal activities, including drug trafficking and the counterfeiting of goods and currency." In October 2007, the FATF released a statement of concern noting that:

> "Iran's lack of a comprehensive AML/CTF regime represents a significant vulnerability within the international financial system. FATF calls upon Iran to address on an urgent basis its AML/CTF deficiencies. FATF members are advising their financial institutions to take the risk arising from the deficiencies in Iran's AML/CTF regime into account for enhanced due diligence."

Iran is currently the only country for which FATF has publicly identified such a significant AML/CTF vulnerability. Both North Korea and Iran are still designated by the U.S. State Department as state sponsors of terrorism.

The "year in review" summary of the 1997 edition asked a question in bold type face that is just as pertinent today: "**Are the laws being implemented?**" A review of the 2008 country reports prompts the following question: "**Are the laws being enforced?**" Unfortunately, the ten-year time frame shows that far too many countries that boast solid AML/CTF standards and infrastructures are still

simply not enforcing their laws. This is true in all corners of the world and for both developed and developing countries alike.

A review of recent data demonstrates that some jurisdictions are having trouble converting their anti-money laundering policies and programs into investigations, prosecutions, and convictions. In some cases, the lack of enforcement is due to lack of capacity, but in far too many others it is due to a lack of political will. In addition, too many jurisdictions are getting caught up in the AML/CTF process and losing sight of the objective.

Over the last ten years, we have made substantial progress collecting financial intelligence. In the United States alone, approximately 18 million pieces of financial intelligence are collected every year. Countless million more financial intelligence reports are produced overseas. We have nearly succeeded in creating global financial transparency in traditional financial institutions. During the past decade, the Egmont Group of financial intelligence Units has grown almost exponentially and now has 106 members. However, success should not be measured by the number of suspicious transaction reports received, analyzed, and disseminated—although undoubtedly the reporting of financial intelligence has a deterrent effect. Financial intelligence is simply the process; the means to an end. Rather, the objective continues to be anti-money laundering and counter-terrorism finance convictions. Convictions, combined with asset seizure and forfeiture are the true deterrents, the most meaningful "measurable," and the bottom line. Far too many jurisdictions continue to fall short in this regard.

Almost twenty years ago, in an early experiment in international anti-money laundering cooperation, the U.S. Customs Service and the Italian Guardia di Finanza (fiscal police) jointly combated Italian/American organized crime—the mafia—by examining illicit money flows between Italy and the United States. Appropriately enough, the task force was called Operation Primo Passo or "first step." At the time, Italy's anti-money laundering infrastructure was in its infancy and prosecutions and convictions were problematic. Today, a review of the 2008 Money Laundering and Financial Crimes section of the INCSR shows that Italy's anti-money laundering/ counter-terrorist financing system is now called "comprehensive" by the International Monetary Fund. With approximately 600 money laundering convictions a year, Italy has one of the highest rates of successful prosecutions in the world. Countries that are currently taking their "first steps" in constructing viable AML/CTF regimes together with countries that continue to struggle to implement policies, procedures and norms should be heartened by the 20 year Italian example, and of more recent successes in Chile, Colombia, Poland, Slovenia, Serbia, and South Korea. With skill, dedication, courage, training, equipment, and political will, much can be accomplished, although a review of continuing money laundering threats demonstrates that much remains to be done. Most importantly, a renewed focus on money laundering enforcement measured by successful investigations and prosecutions is required.

The USG training and technical assistance program has been very effective in helping countries take the necessary steps to combat money laundering and the financing of terrorism. Primarily coordinated and funded by the State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL) and the Office of the Coordinator of Counterterrorism (S/CT), our continuing goal is to simultaneously strengthen regional anti-money laundering organizations, and build comprehensive AML/CTF regimes in individual countries. Working with the USG interagency legal, law enforcement, and financial regulatory communities, as well as with multi-lateral organizations and partner countries, we seek to maximize the institution-building benefits of our assistance by delivering it in both sequential and parallel steps. The steps are tailored to each country's unique needs as determined by threat assessments and concentrate on the following core areas: legal, regulatory, financial intelligence, and enforcement.

The experience of nearly two decades has demonstrated that generally, regional training, while more expensive than bilateral training, is ultimately more effective. Regional training greatly enhances the probability of neighboring countries cooperating and sharing information with one another. Likewise,

long-term training, whether regional or bilateral, is considerably more expensive but infinitely more effective than the usual one-week seminars and short-term training courses that characterize USG efforts. Long-term training and resident advisors enable trainees to take "ownership" of the process, which enhances implementation and sustainability. Unfortunately, primarily due to demands of daily work requirements, the number of USG expert long-term trainers is insufficient to meet global demand. During the past decade, a significant portion of INL's anti-money laundering budget has been used to fund long-term mentors from the UNODC Global Program against Money Laundering as well as through large regional programs with residential mentors in the Caribbean and Pacific. The overriding challenge in our global efforts to provide continued expert effective training and technical assistance is the continued dilemma of there not being enough resources to meet increasing demand for our programs particularly to fund a sufficient number of long-term resident mentors where they are desperately needed. To partially offset our inadequate budget, we have also co-funded mentors in the Mekong Delta and Central Asia regions with the World Bank.

A periodic review of our training and assistance efforts sometimes highlights disappointments and frustrations, but also demonstrates hard-won success. We believe such review is essential to sustain and strengthen gains. Moreover, we are focusing increasingly scarce financial resources and quality trainers in areas that demonstrate the greatest need and the political commitment necessary to develop viable, sustainable anti-money laundering/terrorist financing regimes.

Our review also underscores the truisms that money is the lifeblood of terrorism and that focusing adequate resources on the money trail is still one of the most valuable tools law enforcement has to combat international crime. Similarly, international criminals have tremendous financial resources and spare no expense to corrupt government and law enforcement officials. They also have extensive worldwide networks to support their operations and are inherently nimble, adapting quickly to change. To effectively address this serious threat, we know that we must use our best efforts to apply and coordinate all of the available resources of the federal government and work closely with our foreign counterparts. Sustained global cooperation and support is the surest path to success as we drain the money supply that the criminal networks need to stay in business. To accomplish this, we must continue to support the international community with the tools, capabilities, and resources needed to reduce the growing threats posed by transnational crime, money laundering, and illicit activities.

Mobile Payments—A Growing Threat

In the United States and around the world, law enforcement continues to struggle with the many low-tech but highly effective ways criminals launder money and finance terrorism. Over the last several years, the INCSR Volume II has brought attention to some of these methods and has chronicled progress in developing countermeasures. Two prominent examples are bulk cash smuggling and trade-based money laundering. Unfortunately, while fighting the twin threats of money laundering and terrorist financing, we are also witnessing a plethora of new, high-tech value transfer systems that can be abused. Some of the most innovative are electronic payment products. FATF calls them "new payment methods" or NPMs. They are also sometimes called "e-money" or "digital cash." Examples include Internet payment services, prepaid calling and credit cards, digital precious metals, electronic purses, and mobile payments or "m-payments." Driven by a remarkable convergence of the financial and telecommunications sectors, the rapid global growth of m-payments demands particular attention. M-payments can take many forms but are commonly point of sale payments made through a mobile device such as a cellular phone, a smart phone, or a personal digital assistant (PDA).

Worldwide, there are fewer than one billion bank accounts, but approximately three billion cell phones. In developing countries and often cash based societies in South Asia, Latin America, and Africa, mobile communications proliferate, leapfrogging old landline technology. At the same time,

there is a growing worldwide trend away from paper and towards electronic payments. It is only logical that the startling advances in communications are followed by innovations in m-payments. There are already indications that money launderers and those that finance terrorism will avail themselves of the new m-payment systems. Responsible jurisdictions must find a balance between the expediency of m-payments, particularly in the developing world, and the need to guard against abuse.

According to the International Monetary Fund, Africa is enjoying its best period of economic expansion since the era of independence. In efforts to sustain growth, many donor governments and nongovernmental organizations agree that promoting financial services in Africa, where only an estimated 20 percent of families have bank accounts, should be encouraged. Ethiopia, Uganda, and Tanzania have less than one bank branch per 100,000 people. As a result, millions of Africans, primarily in rural areas, store money at home or keep savings in the form of cattle or gold. High inflation, currency devaluations, and scarce resources mean many turn to purchases of high value goods to retain the value of their money. As a result of these and other conditions, many Africans use informal savings clubs or underground financial systems. The rapid spread of cell phones may be a major contributor to developing much-needed access to financial services. South Africa, Congo, and Kenya, are examples of countries where financial services are now being offered via cell phones. Subscribers can pay bills, transfer money, receive credits, open accounts, and check balances. Workers can be paid by phone. Before leaving on a trip, a subscriber can deposit money and then withdraw funds at the other end, which has many advantages over carrying a significant amount of cash. Cell phone money and credit transfers allow communities to bypass both brick-and-mortar banks and ATMs. The new mobile technology potentially provides a "virtual ATM" to every bearer of a mobile phone.

The World Bank estimates that global remittances exceed one quarter of a trillion dollars annually. Increasingly, in many areas, m-payments provide a new option to expatriates and "guest workers" that wish to send part of their wages home to support their families. M-payment transfers are replacing the use of traditional banks and money service businesses that historically have charged high fees for small transfers. M-payments also provide fast, safe, efficient value transfer service, which will encourage some users to bypass the use of underground remittance systems such as hawala.

The following is an example of how money can be moved via cell phones:

- The sender gives cash for transfer to a remittance center, plus a fee of approximately 3-5 percent (fees generally depend on the amount transferred, and there are generally limits on the amount that can be transferred at one time).
- The remittance center transfers the amount electronically through the phone company to the receiver's cell phone account.
- The recipient receives a text message with notice of the transfer of credit to his or her "electronic wallet."
- The recipient goes to a licensed outlet, retail store, or even a fast-food restaurant to pick up the cash or use the credit. For example, in a restaurant the patron connects to the cash register with his or her cell phone, enters a personal identification number (PIN), and authorizes payment. The entire transaction takes just a few seconds. The entity that provides the goods, services or disburses the cash may also charge a small fee.

Unfortunately, these same promising m-payment developments in Africa, Asia, and elsewhere will assuredly bring abuse of the m-payments systems as well. There are numerous money laundering and terrorist financing implications and many potential scenarios, but "digital value smurfing"—a term coined by the Asian Development Bank—represents a very clear threat. In traditional money laundering, "smurfs" or "runners" deposit or place small amounts of illicit or "dirty" money into financial institutions in ways that do not trigger financial transparency reporting requirements. Today,

digital smurfs are able to bypass regulated banks and their financial reporting requirements and exchange dirty money for digital value in the form of stored value cards or mobile payment credits. Proceeds of crime or contributions to terrorist organizations can now be transferred via cell phones. With such transfers, criminals avoid the risk of physical cash movement, bypass financial transparency reporting requirements, and rapidly send digital value across a country or around the world. Further advantages for money launderers employing digital value smurfing instead of traditional money brokers include the quick conversion of cash to digital value, and the potential to integrate different digital value pools such as SMART cards, on-line accounts, and Internet payment clearing services.

Unfortunately, there is little financial intelligence on most forms of NPMs, including m-payments. Many law enforcement and intelligence agencies currently have little expertise in m-payment methodologies and technology. This gap in expertise is often coupled with a lack of codified authority to examine abuses in the communications systems. Moreover, most m-payment networks have security features that hinder law enforcement and intelligence services in their efforts to detect suspect transactions.

A lack of physical evidence further handicaps law enforcement investigations, as there may not be any cash or cash equivalents to monitor or seize. If value is transferred electronically and the conveyor or recipient phone is destroyed, it may be impossible to reconstruct or determine the information that was on the phone. If both a mobile phone service and the funds used to facilitate m-payments are prepaid, the service provider may not fully identify its customers due to the absence of credit risk. The problems could be compounded by the use of false identification to obtain subscriber status or to purchase or rent m-payment services. Using prepaid cellular phones could allow criminals to buy handsets incognito and use their minutes without leaving a trace of their calling records.

Some countries, such as the Philippines, embrace m-payment innovations. According to the Asian Development Bank, 35 percent of the people in the Philippines have cell phones, while 95 percent of the rest have access to cell phones via friends or family. Even traditionally inaccessible areas increasingly have cell phone coverage. As a result, m-payments are rapidly growing in popularity and are commonly used to pay bills, buy goods, and transfer cash. In addition, Philippine workers in approximately 18 countries, including the United States, can use their cell phones to send money home.

The Philippines is one of the few countries proactively taking steps to monitor and regulate m-payments. Service providers have worked closely with the Central Bank and the financial intelligence unit to comply with anti-money laundering laws and regulations. Carriers are regulated as money service businesses. Following “know-your-customer” policies, the authorized subscriber must register in person with the service provider and present a valid photo identification document to either put cash in or take cash out of the system. There are also limits on the size of the customer’s “electronic wallet.” For example, the maximum a subscriber can transfer at one time is 10,000 pesos (approximately $247), or a maximum of 40,000 pesos (approximately $990) a day and 100,000 pesos (approximately $2,475) per month. However, the regulations and limits do not eliminate the vulnerabilities that false identification and networks of “digital smurfs” pose.

The United States currently has few safeguards against abuse of m-payments. M-payment service providers in the United States are classified as money service businesses and, in theory, must register with the United States FIU, the Financial Crimes Enforcement Network (FinCEN). However, most money service businesses do not comply with registration requirements and there is little enforcement of the regulations.

The NPM issue is briefly mentioned in the 2007 National Money Laundering Strategy:

“FinCEN, in coordination with the federal banking regulators and the industry, will issue guidance and develop regulatory definitions and requirements under the BSA for stored value products and payment

systems." Unfortunately, there has been little progress in formulating and disseminating guidance and our traditional money laundering countermeasures are not adequate to address the looming threat posed by abuse of m-payments to today's e-banking and cashless system.

In the digital age, it is increasingly difficult to "follow the money." The FATF and numerous organizations and governments worldwide recognize the use of NPMs, including m-payments, as a growing threat. Much work and creative thinking will be required to maintain the advantages NPMs, including m-payments offer, while at the same time preventing exploitation and misuse by money launderers and terrorist financiers and simultaneously protecting user privacy and the integrity of the global financial systems.

Bilateral Activities

Training and Technical Assistance

During 2007, a number of U.S. law enforcement and regulatory agencies provided training and technical assistance on money laundering countermeasures and financial investigations to their counterparts around the globe. These courses have been designed to give financial investigators, bank regulators, and prosecutors the necessary tools to recognize, investigate, and prosecute money laundering, financial crimes, terrorist financing, and related criminal activity. Courses have been provided in the United States as well as in the jurisdictions where the programs are targeted.

Department of State

The Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL) Crime Programs Division teams help to strengthen criminal justice systems and the abilities of law enforcement agencies around the world to combat transnational criminal threats before they extend beyond their borders and impact our homeland. Through its international programs, as well as in coordination with other INL offices and U.S. government agencies, the INL Crime Programs Division addresses a broad cross-section of law enforcement and criminal justice sector areas including: counternarcotics; demand reduction; money laundering, financial crime, and terrorist financing; corruption, smuggling of goods; illegal migration; trafficking in persons; domestic violence; border controls; document security; cybercrime; intellectual property rights; law enforcement; police academy development; and assistance to judiciaries and prosecutors. While this report is limited to training and assistance to combat money laundering and the financing of terrorism, anticorruption training is closely related to USG anti-money laundering/counter-terrorist financing training, and frequently mirrors it: For example, INL's anticorruption initiatives help to 1) establish shared global anticorruption standards such as the United Nations Convention against Corruption, subscribed to by 107 countries; 2) strengthen global political will to fight corruption and to implement multilateral anti-corruption commitments; 3) increase international cooperation to prosecute corruption, identify and prevent access by kleptocrats to financial systems, deny safe haven to corrupt officials, and identify, recover, and return proceeds of corruption; and 4) provide anticorruption assistance that strengthens legal frameworks and builds capacity of critical law enforcement and rule of law institutions, such as police, investigators, prosecutors, judges, ethics offices, auditors, inspectors general, and other oversight, regulatory and law enforcement officials.

INL and the Department's Office of the Coordinator for Counterterrorism (S/CT) co-chair the interagency Terrorist Finance Working Group (TFWG) and together implement a multimillion dollar training and technical assistance program designed to develop or enhance the capacity of a selected group of more than two dozen countries that have been used or are vulnerable to being used to finance

terrorism. As is the case with the more than 100 other countries to which INL-funded training was delivered in 2007, the capacity to thwart the funding of terrorism is dependent on the development of a robust anti-money laundering regime. Supported by and in coordination with the Department of State, the Department of Justice, Department of Homeland Security, Department of Treasury, the Federal Deposit Insurance Corporation, and various nongovernmental organizations, the TFWG member agencies offer law enforcement, regulatory and criminal justice programs worldwide. This integrated approach includes assistance with the drafting of legislation and regulations that comport with international standards, and the training of law enforcement, the judiciary and bank regulators, as well as the development of financial intelligence units capable of collecting, analyzing and disseminating financial information to foreign analogs. Courses have been provided in the United States as well as in the jurisdictions to which the programs are targeted.

Nearly every federal law enforcement agency assisted in this effort by providing basic and advanced training courses in all aspects of financial criminal investigation. Likewise, bank regulatory agencies participated in providing advanced anti-money laundering/counterterrorist financing training to supervisory entities. In addition, INL made funds available for the intermittent or full-time posting of legal and financial mentors at selected overseas locations. These advisors work directly with host governments to assist in the creation, implementation, and enforcement of anti-money laundering and financial crime legislation. INL also provided several federal agencies funding to conduct multi-agency financial crime training assessments and develop specialized training in specific jurisdictions to combat money laundering.

The success of the Brazilian Trade Transparency Unit (TTU), less than nine months after being established in late 2005, augurs well for the newer TTUs of Argentina and Paraguay. The Argentine TTU has uncovered a major trade-based anomaly that law enforcement is currently investigating. In 2006, INL obligated funds to the Department of Homeland Security to establish a TTU in Southeast Asia and, in 2007, to develop a TTU in Mexico. Similar to the Egmont Group of financial intelligence units that examines and exchanges information gathered through financial transparency reporting requirements, an international network of TTUs will foster the sharing of disparities in trade data between countries and be a potent weapon in combating customs fraud and trade-based money laundering. Trade is the common denominator in most of the world's alternative remittance systems and underground banking systems. Trade-based value transfer systems have also been used in terrorist finance.

The success of the Caribbean Anti-Money Laundering Program (CALP) convinced INL that a similar type of program for small Pacific island jurisdictions had the potential of developing viable anti-money laundering/counterterrorist regimes. Accordingly, INL contributed $1.5 million to the Pacific Islands Forum to develop the Pacific Island Anti-Money Laundering Program (PALP). The objectives of the PALP are to reduce the laundering of the proceeds of all serious crime and the financing of terrorist financing by facilitating the prevention, investigation, and prosecution of money laundering. The PALP's staff of resident mentors provides regional and bilateral mentoring, training and technical assistance to the Pacific Islands Forum's 14 non-FATF member states for the purpose of developing viable regimes that comport with international standards. The PALP is now in its second year. INL will contribute a total of $6 million to the Pacific Islands Forum for the four-year PALP project.

In FY07, INL obligated $1.7 million for the United Nations Global Program against Money Laundering (GPML). In addition to sponsoring money laundering conferences and providing short-term training courses, the GPML instituted a unique longer-term technical assistance initiative through its mentoring program. The mentoring program provides advisors on a year-long basis to specific countries or regions. GPML mentors provided assistance to the Secretariat of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and to the Horn of Africa countries targeted by the President's East Africa Counterterrorism Initiative. GPML resident mentors provided country-specific assistance to the Philippines' FIU, and asset forfeiture assistance to Namibia, Botswana, and

Zambia. The mentor provided legal inputs to amend relevant legislation in each country, and initiated and monitored the Prosecutor Placement Program, an initiative aimed at placing prosecutors from the region for a certain period of time within the Asset Forfeiture Unit of the National Prosecuting Authority (NPA) in South Africa. The GPML mentors in Central Asia and the Mekong Delta are assisting the countries in those regions to develop viable anti-money laundering/counterterrorist financing regimes. The GPML continues to develop interactive computer-based programs that are translated into several languages and distributed globally.

INL continues to provide significant financial support for many of the anti-money laundering bodies around the globe. During 2007, INL supported the Financial Action Task Force (FATF), the international standard setting organization. INL continued to be the sole U.S. Government financial supporter of the FATF-style regional bodies, including the Asia/Pacific Group on Money Laundering (APG), the Council of Europe's MONEYVAL, the Caribbean Financial Action Task Force (CFATF), the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the South American Financial Action Task Force (GAFISUD). INL also financially supported the Organization of American States (OAS) Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering and the OAS Inter-American Counter-Terrorism Committee.

As in previous years, INL training programs continue to focus on an interagency and multilateral approach and on bringing together, where possible, foreign law enforcement, judicial and financial supervisory and regulatory authorities. This approach encourages an extensive dialogue and exchange of information. This approach has been used successfully in Asia, Central and South America, Central Asia, and Central and Eastern Europe. INL also provides funding for many of the regional training and technical assistance programs offered by the various law enforcement agencies, including assistance to the International Law Enforcement Academies.

International Law Enforcement Academies (ILEAs)

The mission of the regional ILEAs has been to support emerging democracies, help protect U.S. interests through international cooperation, and promote social, political and economic stability by combating crime. To achieve these goals, the ILEA program has provided high-quality training and technical assistance, supported institution building and enforcement capability, and fostered relationships of American law enforcement agencies with their counterparts in each region. ILEAs have also encouraged strong partnerships among regional countries, to address common problems associated with criminal activity.

The ILEA concept and philosophy is the result of a united effort by all participants—government agencies and ministries, trainers, managers, and students—to achieve the common foreign policy goal of international law enforcement. The goal is to train professionals who will craft the future of the rule of law, human dignity, personal safety and global security.

The ILEAs are a progressive concept in the area of international assistance programs. The regional ILEAs offer three different types of programs. The Core program, a series of specialized training courses and regional seminars tailored to region-specific needs and emerging global threats, typically includes 50 participants, normally from three or more countries. The specialized courses, comprised of about 30 participants, are normally one or two weeks long and often run simultaneously with the Core program. Lastly, there are regional seminars with different topical foci; these have included transnational crimes, financial crimes, and counterterrorism.

The ILEAs help to develop an extensive network of alumni who exchange information with their U.S. counterparts and assist in transnational investigations. These graduates are also expected to become the leaders and decision-makers in their respective societies. The Department of State works with the Departments of Justice (DOJ), Homeland Security (DHS) and Treasury, and with foreign governments

to implement the ILEA programs. To date, the combined ILEAs have trained over 20,000 officials from over 75 countries in Africa, Asia, Europe and Latin America. The ILEA budget averages approximately $16 to 18 million annually.

Africa. ILEA Gaborone (Botswana) opened in 2001. The main feature of this ILEA is a six-week intensive personal and professional development program, called the Law Enforcement Executive Development Program (LEEDP), for law enforcement mid-level managers. The LEEDP brings together approximately 42 participants from several nations for training on topics such as combating transnational criminal activity, supporting democracy by stressing the rule of law in international and domestic police operations, and by raising the professionalism of officers involved in the fight against crime. ILEA Gaborone also offers specialized courses for police and other criminal justice officials to enhance their capacity to work with U.S. and regional officials to combat international criminal activities. These courses concentrate on specific methods and techniques in a variety of subjects, such as counterterrorism, anti-corruption, financial crimes, border security, drug enforcement, firearms and many others.

Instruction is provided to participants from Angola, Botswana, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia, Djibouti, Ethiopia, Kenya, Uganda, Nigeria, Cameroon, Comoros, Congo, the Democratic Republic of Congo, Gabon and Madagascar. Burundi, Rwanda, Sierra Leone, Ghana, Guinea and Senegal are projected to join the program during the latter part of 2008.

United States and Botswana trainers provide instruction. ILEA Gaborone has offered specialized courses on money laundering/terrorist financing-related topics such as Criminal Investigation (presented by FBI) and International Banking & Financial Forensic Program (presented by DHS and the Federal Law Enforcement Training Center), and International Money Laundering Scheme (presented by ICE). ILEA Gaborone trains approximately 500 students annually.

Asia. ILEA Bangkok (Thailand) opened in March 1999. This ILEA focuses on enhancing the effectiveness of regional cooperation against the principal transnational crime threats in Southeast Asia—illicit drug trafficking, financial crimes, and alien smuggling. The ILEA provides a Core course (the Supervisory Criminal Investigator Course or SCIC) of management and technical instruction for supervisory criminal investigators and other criminal justice managers. In addition, this ILEA presents one Senior Executive program and about 18 specialized courses—each lasting one to two weeks—in a variety of criminal justice topics. The principal objectives of the ILEA are the development of effective law enforcement cooperation within the member countries of the Association of Southeast Asian Nations (ASEAN), East Timor and China (including Hong Kong and Macau), and the strengthening of each country's criminal justice institutions to increase its abilities to cooperate in the suppression of transnational crime.

Instruction is provided to participants from Brunei, Cambodia, East Timor, China, Hong Kong, Indonesia, Laos, Macau, Malaysia, Philippines, Singapore, Thailand and Vietnam. Subject matter experts from the United States, Thailand, Japan, Netherlands, Philippines and Hong Kong provide instruction. ILEA Bangkok has offered specialized courses on money laundering/terrorist financing-related topics such as Computer Crime Investigations (presented by FBI and DHS) and Complex Financial Investigations (presented by IRS, FBI and DEA). Total annual student participation is approximately 800.

Europe. ILEA Budapest (Hungary) opened in 1995. Its mission has been to support the region's emerging democracies by combating an increase in criminal activity that emerged against the backdrop of economic and political restructuring following the collapse of the Soviet Union. ILEA Budapest offers three different types of programs: an eight-week Core course, Regional Seminars and Specialized courses in a variety of criminal justice topics. Instruction is provided to participants from Albania, Armenia, Azerbaijan, Bulgaria, Croatia, Czech Republic, Georgia, Hungary, Kazakhstan,

Kyrgyz Republic, Latvia, Lithuania, Macedonia, Moldova, Montenegro, Poland, Romania, Russia, Serbia, Slovakia, Slovenia, Tajikistan, Turkmenistan, Ukraine and Uzbekistan.

Trainers from 17 federal agencies and local jurisdictions from the United States, Hungary, Canada, Germany, United Kingdom, Netherlands, Ireland, Italy, Russia, Interpol and the Council of Europe provide instruction. ILEA Budapest has offered specialized courses on money laundering/terrorist financing-related topics such as Investigating/Prosecuting Organized Crime and Transnational Money Laundering (both presented by DOJ/OPDAT). ILEA Budapest trains approximately 800 students annually.

Global. ILEA Roswell (New Mexico) opened in September 2001. This ILEA offers a curriculum comprised of courses similar to those provided at a typical Criminal Justice university/college. These three-week courses have been designed and are taught by academicians for foreign law enforcement officials. This Academy is unique in its format and composition with a strictly academic focus and a worldwide student body. The participants are middle to senior level law enforcement and criminal justice officials from Eastern Europe; Russia, the states of the former Soviet Union; Association of Southeast Asian Nations (ASEAN) member countries; and the People's Republic of China (including the Special Autonomous Regions of Hong Kong and Macau); and member countries of the Southern African Development Community (SADC) plus other East and West African countries; the Caribbean, Central and South American countries. The students are drawn from pools of ILEA graduates from the Academies in Bangkok, Budapest, Gaborone and San Salvador. ILEA Roswell trains approximately 350 students annually.

Latin America. ILEA San Salvador was established in 2005. The training program for the newest ILEA is similar to the ILEAs in Bangkok, Budapest and Gaborone and will offer a six-week Law Enforcement Management Development Program (LEMDP) for law enforcement and criminal justice officials as well as specialized courses for police, prosecutors, and judicial officials. In 2008, ILEA San Salvador will deliver four LEMDP sessions and approximately 16 Specialized courses that will concentrate on attacking international terrorism, illegal trafficking in drugs, alien smuggling, terrorist financing, financial crimes, culture of lawfulness and accountability in government. Components of the six-week LEMDP training session will focus on terrorist financing (presented by the FBI), international money laundering (presented by ICE) and financial evidence/money laundering application (presented by DHS/FLETC and IRS). The Specialized course schedule will include courses on financial crimes investigations (presented by DHS/ICE) and money laundering training (presented by IRS). Instruction is provided to participants from: Argentina, Bardados, Bahamas, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, Jamaica, Nicaragua, Panamá, Paraguay, Perú, Trinidad and Tobago, Uruguay and Venezuela. ILEA San Salvador trains approximately 800 students per year

The ILEA Regional Training Center located in Peru opened in 2007. The center will augment the delivery of region-specific training for Latin America and will concentrate on specialized courses on critical topics for countries in the Southern Cone and Andean Regions. The RTC is projected to train approximately 240 students per year.

Board of Governors of the Federal Reserve System (FRB)

An important component in the United States' efforts to combat and deter money laundering and terrorist financing is to verify that supervised organizations comply with the Bank Secrecy Act (BSA) and have programs in place to comply with the Office of Foreign Assets Control (OFAC) sanctions. Under the auspices of the Federal Financial Institutions Examination Council's (FFIEC) BSA/Anti-Money Laundering (AML) Working Group, the federal bank regulatory agencies, Financial Crimes Enforcement Network (FinCEN), OFAC, and the Conference of State Banking Supervisors collaborated in the development of the FFIEC's BSA/AML Examination Manual, released in 2005 and

updated in 2006. In 2007, the manual was updated again to further clarify supervisory expectations, incorporate new regulatory issuances, and respond to industry requests for additional guidance.

Internationally, the FRB conducted training and provided technical assistance to bank supervisors and law enforcement officials in AML and counterterrorist financing (CTF) tactics in partnership with regional supervisory groups or multilateral institutions, including the South East Asian Central Banks, and the Caribbean Association of Indigenous Bankers. In 2007, the FRB provided training and/or technical assistance to regulators and bankers in Russia and Mexico. In addition, the FRB sponsored an AML examination seminar in Chicago for bank supervisors from 25 different countries.

Due to the importance that the FRB places on international standards, the FRB's AML experts participate regularly in the U.S. delegation to the Financial Action Task Force (FATF) and the Basel Committee's AML/CTF expert group. The FRB is also an active participant in the U.S. Treasury Department's ongoing Private Sector Dialogue conferences, attending the Latin American session in Bogotá and the Middle East and North Africa meeting in Dubai this year. Staff also meets frequently with industry groups and foreign supervisors to support industry best practices in this area.

The FRB presented training courses on 'International Money Movement' to domestic law enforcement agencies, including the Department of Homeland Security's Bureau for Immigration and Customs Enforcement (DHS/ICE), as well as at the Federal Law Enforcement Training Center (FLETC) during 2007.

Drug Enforcement Administration (DEA), Department of Justice

The Office of Financial Operations provided anti-money laundering and/or asset forfeiture training in 2007 to officials from Thailand, Australia, Belgium, Aruba, Peru, Canada, Indonesia, and Mexico.

The DEA Office of International Training facilitated three Department of Justice (DOJ)/Asset Forfeiture Money Laundering Seminars to foreign audiences: (1) International Asset Forfeiture Seminar, (2) Advanced International Asset Forfeiture Seminar, and (3) Money Laundering Seminar. During fiscal year 2007, a total of 214 participants were trained at Basic and Advanced Asset Forfeiture/Money Laundering Seminars from the following countries: Cyprus, Indonesia, Mexico, Israel, and New Zealand. The core topics in the International Asset Forfeiture Seminar include: financial investigations; case study; tracing hidden assets; DEA asset forfeiture procedures and U.S. forfeiture law; international asset forfeiture sharing and cooperation; debriefing of financial sources of information. Elective topics include: the business of asset forfeiture (processing and managing seized assets); document exploitation; operational management of an asset forfeiture unit; operation and utilization of FinCEN resources; ethical considerations in the use of asset forfeiture funds; analysis of net worth income and practical application and use of undercover bank accounts. The Advanced Course includes core topics of: international case studies; the use of the Internet in money laundering; international banking; international issues in money laundering and forfeiture; DEA asset forfeiture procedures and practical applications. Elective topics include: reverse undercover sting operations; use of undercover bank accounts; ethical considerations in the use of asset forfeiture funds; tracing the origins of financial assets; document exploitation; use of suspicious activity reports to initiate and pursue investigations; and terrorist financing. Course topics are determined by the investigative capacity and experience level of the participants and the money laundering laws of the host nation. The International Asset Forfeiture and Money Laundering program is coordinated by the International Training Section of DEA in a joint effort with the Department of Justice.

Federal Bureau of Investigation (FBI), Department of Justice

During 2007, with the assistance of State Department funding, Special Agents and other subject matter experts of the Federal Bureau of Investigation (FBI) continued their extensive international training in terrorist financing, money laundering, financial fraud, racketeering enterprise investigations, and complex financial crimes. The FBI's International Training and Assistance Unit (ITAU), is located at the FBI Academy in Quantico, Virginia. ITAU coordinates with the Terrorist Financing and Operations Section of the FBI's Counterterrorism Division, as well as other divisions within FBI Headquarters and in the field, to provide instructors for these international initiatives. FBI instructors, who are most often intelligence analysts, operational Special Agents or Supervisory Special Agents from headquarters or the field, rely on their experience to relate to the international law enforcement students as peers and partners in the training courses.

The FBI regularly conducts training through the International Law Enforcement Academies (ILEA) in Bangkok, Thailand; Budapest, Hungary; Gaborone, Botswana; and San Salvador, El Salvador. In 2007, the FBI delivered training in white collar crime investigations to 240 students from ten countries at ILEA Budapest. At the ILEA Bangkok, the FBI provided training to 50 students from Thailand in the Supervisory Criminal Investigators course and 50 students from Thailand in a Complex Financial Investigations course. Similarly, at the ILEA Gaborone, the FBI provided terrorist financing training to 161 students from 23 African countries and at the ILEA San Salvador, training was provided to 151 students from El Salvador, Guatemala, Nicaragua, and Honduras.

The FBI also provided training to officials in Jordan, Pakistan, Qatar, Bosnia-Herzegovina, South Africa, Latvia, Bangladesh, and Kuwait. This training includes FBI participation in a Combating Money Laundering & Terrorism Financing Seminar that the Department of Justice's Office of Overseas Prosecutorial Development delivered to 45 students in Jordan. It also includes the one-week Terrorism Financing and Money Laundering initiatives that the FBI regularly conducts jointly with the Internal Revenue Service, Criminal Investigative Division, and which included 136 international students in 2007. In its other training programs, held at the FBI Academy, the FBI included blocks or instruction on terrorist financing and/or money laundering for 39 students from 16 Latin American countries participating in the Latin American Law Enforcement Executive Development Seminar, and for 28 students from 11 Middle Eastern and Northern African countries participating in the second Arabic Language Law Enforcement Executive Development Seminar, and 40 students from Mexico for a special Mexican Law Enforcement Executive Development Seminar. Terrorist financing instruction was also included in the FBI's Pacific Training Initiative, which served 55 participants from ten countries: Australia, Cambodia, China, Hong Kong, India, Japan, Korea, Malaysia, Philippines, and Thailand. The FBI provided training to 50 students from Malaysia in a Forensic Accounting course.

Federal Deposit Insurance Corporation (FDIC)

In 2007, the FDIC continued to work in partnership with several federal agencies to combat money laundering and the global flow of terrorist funds. Additionally, the FDIC planned and participated in missions to assess vulnerabilities to terrorist financing activity worldwide, including developing and implementing plans to assist foreign governments in their efforts. To accomplish this objective, the FDIC has 32 individuals available to participate in foreign anti-money laundering and counter-terrorist financing (AML/CTF) missions. Periodically, FDIC management and staff meet with supervisory and law enforcement representatives from various countries to discuss AML issues, including examination policies and procedures, the USA PATRIOT Act requirements, suspicious activity reporting

requirements, and interagency information sharing mechanisms. In 2007, the FDIC gave such presentations to representatives from Japan, Korea, Lebanon, Morocco and Uruguay.

In 2007, in partnership with the Department of State, the FDIC hosted three sessions on AML/CTF to 57 individuals from Algeria, Bosnia and Herzegovina, Egypt, Indonesia, Jordan, Kuwait, Morocco, Pakistan, Paraguay, Philippines, Tanzania, and Turkey. The sessions included the AML examination process, customer due diligence, and foreign correspondent banking. In February and November 2007, the FDIC participated in interagency Financial Systems Assessment Teams (FSAT) to Yemen and Senegal, respectively. The FSAT reviewed the countries' AML laws and provided information in the areas of customer identification programs, financial intelligence units and the monitoring of nonbank financial institutions.

In December 2007, the FDIC participated in the third annual U.S.-Middle East/North Africa Private Sector Dialogue in Dubai, United Arab Emirates. The focus of the conference was to raise awareness of terrorist financing and money laundering risks, facilitate a better understanding of effective practices and programs to combat such risks, and strengthen implementation of effective AML/CTF controls.

Financial Crimes Enforcement Network (FinCEN), Department of Treasury

FinCEN, a bureau of the U.S. Department of the Treasury and the U.S. financial intelligence unit (FIU), coordinates and provides training and technical assistance to foreign nations seeking to improve their capabilities to combat money laundering, terrorist financing, and other financial crimes. A specific focus of FinCEN is the creation and strengthening of FIUs, a valuable component of a country's anti-money laundering/counter-terrorist financing (AML/CTF) regime. FinCEN's international training program has two primary focuses: (1) instruction and presentations to a broad range of government officials, financial regulators, law enforcement officers, and others on the subjects of money laundering, terrorist financing, financial crime, and on FinCEN's mission and operation; and (2) individualized training to FIU counterparts regarding FIU operations and analysis training via personnel exchanges and FIU development seminars. Much of FinCEN's work involves strengthening existing FIUs and the channels of communication used to share information to support anti-money laundering investigations. Participation in personnel exchanges (from the foreign FIU to FinCEN and vice versa), delegation visits to/from foreign FIUs, and coordinating regional workshops are just a few examples of FinCEN activities designed to assist and support FIUs.

In 2007, FinCEN hosted representatives from approximately 29 countries. These visits, typically lasting one to three days, focused on topics such as money laundering trends and patterns, the Bank Secrecy Act, USA PATRIOT ACT, communications systems and databases, case processing, and the goals and mission of FinCEN. Representatives from foreign financial and law enforcement sectors generally spend one to two days at FinCEN learning about money laundering, the U.S. AML regime and reporting requirements, the national and international roles of a financial intelligence unit, and various other topics.

FinCEN gives assistance to new or developing FIUs that are not yet members of the Egmont Group of FIUs. Comprised of FIUs that cooperatively agree to share financial intelligence, Egmont has become the standard-setting body for FIUs. FinCEN hosts FIU orientation visits and provides training and mentoring on FIU development. In 2007, FinCEN hosted a representative from Namibia's nascent FIU for an orientation visit that included an overview on various aspects of developing a newly formed FIU. Also, at the invitation of FinCEN's Director, a delegation from Saudi Arabia's FIU was hosted by FinCEN for a weeklong seminar that included an overview of FinCEN's operations and programs,

as well as briefings from other U.S. agencies selected by FinCEN (OCC, IRS, ICE, FBI and DOJ) to discuss their part in the U.S. AML/CTF regime.

For those FIUs that are fully operational, FinCEN's goal is to assist the unit in increasing effectiveness, improving information sharing capabilities, and better understanding the phenomena of money laundering and terrorist financing. As a member of the Egmont Group, FinCEN works closely with other member FIUs to provide training and technical assistance to countries and jurisdictions interested in establishing their own FIUs and obtaining candidacy for membership in the Egmont Group. Additionally, FinCEN works multilaterally through its representative on the Egmont Training Working Group to design, implement, and co-teach Egmont-sponsored regional training programs to both Egmont member and Egmont candidate FIUs.

In addition to hosting delegations for training on FinCEN premises, FinCEN conducts training courses and seminars abroad, both independently and in conjunction with other domestic and foreign agencies, counterpart FIUs, and international organizations. Occasionally, FinCEN's training and technical assistance programming is developed jointly with these other agencies to address specific needs of the jurisdiction/country receiving assistance. Topics such as FIU primary and secondary functions; regulatory issues; international case processing procedures; technology infrastructure and security; and terrorist financing and money laundering trends and typologies provide trainees with broader knowledge and a better understanding of the topics of money laundering and terrorist financing. In 2007, FinCEN collaborated with the Canadian FIU (FINTRAC) and the World Bank to conduct a training workshop for 12 Caribbean FIUs. The workshop focused on enhancing the capacity and cooperation of Caribbean FIUs to combat money laundering and the financing of terrorism. Over a five day training course, participants engaged in discussions and practical exercises relating to various topics such as terrorist financing, nonprofit organizations, protection of information, alternative remittance systems, international and domestic cooperation, and strengthening the analysis of financial reports.

FinCEN conducts core analytical training to counterpart FIUs both at FinCEN and abroad, often in conjunction with other U.S. agencies. FinCEN's analytical training program, typically delivered over the course of one to two weeks, provides foreign analysts with basic skills in critical thinking and analysis; data collection; database research; suspicious transactions analysis; the intelligence cycle; charting; data mining; and case presentation. In 2007, FinCEN provided training on basic analytical skills to FIUs and other agencies from the intelligence, regulatory and enforcement communities in Bangladesh, Saudi Arabia, Afghanistan Egypt and Bosnia. Over the last twelve months, in an effort to reinforce the sharing of information among established Egmont-member FIUs, FinCEN conducted personnel exchanges with Egmont Group members Chile, Canada, Mexico and Japan. These exchanges offer the opportunity for FIU personnel to see first-hand how another FIU operates; develop joint analytical projects and other strategic initiatives; and also to work jointly on on-going financial crimes cases. The participants in these exchanges share ideas, innovations, and insights that lead to improvements in such areas as analysis, information flow, and information security at their home FIUs, in addition to deeper and more sustained operational collaboration.

Immigration and Customs Enforcement, Department of Homeland Security (DHS)

During 2007, U.S. Immigration and Customs Enforcement (ICE), Financial, Narcotics and Public Safety Division, in conjunction with the Office of International Affairs, delivered money laundering/terrorist financing, bulk cash smuggling, and financial investigations training to law enforcement, regulatory, banking and trade officials from more than 50 foreign countries. The training was conducted in both bilateral and multilateral engagements. ICE money laundering and financial

investigations training is based on the broad experience and expertise achieved by leading U.S. efforts in investigating international money laundering and financial crimes as part of the former U.S. Customs Service.

Using primarily State Department/INL funding, ICE provided bilateral and multilateral training and technical assistance on the interdiction and investigation of bulk cash smuggling for 340 officials representing a total of 36 countries. ICE conducted basic bulk cash smuggling training in the Philippines, South Africa, Malaysia, Indonesia, Morocco, Bosnia, and Algeria. ICE also provided an operational training seminar on advanced bulk cash smuggling in the Philippines. Bulk cash smuggling training was also delivered to two regional Financial Action Task Force-style regional bodies (FATF/FSRBs): the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) and the Inter-Government Action Group Against Money Laundering and Terrorist Financing (GIABA.) All ICE training was conducted in furtherance of the FATF Special Recommendation IX on Cash Couriers.

ICE also conducted financial investigation/money laundering training programs for more than 600 participants at the State Department sponsored International Law Enforcement Academy (ILEA) locations in El Salvador, Thailand, Hungary and Botswana. A specialized advanced financial training program was given three times at the ILEA in Thailand.

Trade Transparency Units (TTUs)

Trade Transparency Units (TTUs) identify anomalies related to cross-border trade that are indicative of international trade-based money laundering. TTUs generate, initiate and support investigations and prosecutions related to trade-based money laundering, the illegal movement of criminal proceeds across international borders, alternative money remittance systems, and other financial crimes. By sharing trade data, ICE and participating foreign governments are able to see both sides of import and export transactions for commodities entering or exiting their countries, thus assisting in the investigation of international money laundering organizations

With funding from the Department of State's Bureau of International Narcotics and Law Enforcement (INL), ICE worked to expand the network of operational foreign Trade Transparency Units (TTU's) beyond Colombia, Brazil, and Argentina by providing IT equipment and training to the newly established TTU in Paraguay. ICE also initiated the process of establishing a TTU in Mexico City, Mexico and is conducting suitability surveys in preparation of establishing a TTU in Southeast Asia.

In 2007, ICE updated the technical capabilities of existing TTUs and trained new TTU personnel in Colombia, Argentina, and Paraguay as well as members of their financial intelligence units. Additionally, ICE strengthened its relationship with its TTUs by deploying temporary personnel overseas to work onsite and provide hands on training to all four TTUs in the hemisphere. This action resulted in immediate information sharing between the U.S. and the foreign TTUs in furtherance of ongoing joint criminal investigations.

Other ICE Programs

Additionally, in 2007, ICE expanded Operation Firewall, a joint strategic bulk cash smuggling initiative with U.S. Customs and Border Protection (CBP) to provide hands on training and capacity building to Mexican law enforcement officials. Operation Firewall was initiated to address the threat of bulk cash smuggling via commercial and private passenger vehicles, commercial airline shipments, commercial airline passengers, and pedestrians transiting into Mexico and Canada, as well as other foreign locations. In 2007, Operation Firewall had 845 seizures totaling more than $4.3 million in U.S. currency and negotiable instruments.

Under the ICE Cornerstone initiative, training was developed and designed to provide the financial and trade sectors with the necessary skills to identify and develop methodologies to detect suspicious transactions indicative of money laundering and criminal activity. In furtherance of Cornerstone, ICE has appointed field and headquarters agents who are dedicated to providing training to the financial and trade communities on identifying and preventing exploitation by criminal and terrorist organizations. In 2007, ICE Cornerstone liaisons conducted 1,390 outreach meetings with more than 23,000 industry professionals in the U.S. and abroad.

Internal Revenue Service (IRS), Criminal Investigative Division (CID) Department of Treasury

In calendar year 2007, the IRS Criminal Investigative Division (IRS-CID) continued their involvement in international training and technical assistance efforts designed to assist international law enforcement officers in detecting tax, money laundering and terrorist financing crimes. With funding provided by the Department of State, IRS-CID delivered training through agency and multi-agency technical assistance programs to international law enforcement agencies. Training consisted of both basic and advanced financial investigative techniques. IRS-CID provided instructor and course delivery support to the four International Law Enforcement Academies (ILEAs) in Bangkok, Thailand; Budapest, Hungary; Gaborone, Botswana; and San Salvador, El Salvador.

At ILEA Bangkok, IRS-CID participated in one Supervisory Criminal Investigator course #24 (SCIC) and was the coordinating agency of the Complex Financial Investigations #9 (CFI) course. These courses are provided to senior, mid-level, and first-line law enforcement supervisors and officers from the countries of Cambodia, Hong Kong, Indonesia, Macau, Malaysia, Republic of China, Philippines, Singapore, Thailand, East Timor, and Vietnam.

At ILEA Budapest, IRS-CID participated in five sessions, ILEA 59-63, delivering financial investigative techniques training. The countries that participated in these classes are Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Georgia, Hungary, Kazakhstan, Macedonia, Moldova, Romania, Russia, Serbia, and Ukraine.

At ILEA Gaborone, IRS-CID participated in four Law Enforcement Executive Development programs (LEED 22-25), delivering financial investigative techniques training. IRS-CID also provided a class coordinator for LEED 22, covering a six-week period, with the responsibilities of coordinating and supervising the participant's daily duties and activities. Countries that participated in these classes are Angola, Botswana, Lesotho, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, Tanzania, Zambia, Djibouti, Ethiopia, Kenya, Seychelles, Uganda, Nigeria, Cameroon, Comoros, Republic of the Congo, Gabon, and Madagascar.

At ILEA-San Salvador, IRS-CID participated in four of the America's Law Enforcement Development programs (LEMDP 004-LEMDP 007), delivering financial investigative techniques training. Countries that participated in these classes are Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Chile, El Salvador, Grenada, Guatemala, Jamaica, Mexico, Paraguay, Peru, St. Kitts and Nevis, and Suriname. LEMDP stresses the importance of conducting a financial investigation to further develop a large scale, criminal investigation.

IRS-CID participated in a conference to raise public awareness of asset forfeiture as an effective law enforcement tool in Belgrade, Serbia. The conference was co-sponsored by the OPDAT and the Organization for Security and Co-Operation in Europe (OSCE). The conference was attended by English, Serbian, and Italian speaking participants.

IRS-CID delivered a Forensic Accounting course for Investigators of the Bank of Negara held in Kuala Lumpur, Malaysia. The Internal Revenue Service Tax Advisory Administrative Services (TAAS) funded the program.

IRS-CID participated in delivering a Terrorism Financing/Money Laundering course hosted by the Federal Bureau of Investigation (FBI) in Doha, Qatar.

IRS-CID delivered an International Financial Fraud Training (IFFT) at FLETC, Glynco, Georgia. The class, sponsored by Tax Advisory Administrative Services (TAAS), was attended by 25 foreign dignitaries from Albania, Bangladesh, Bosnia, China, Guatemala, Republic of Korea, Romania, Taiwan, and Trinidad and Tobago.

IRS-CID participated in a conference hosted by The Department of Justice Office of Overseas Prosecutorial Development Assistance and Training (OPDAT) in Kuala Lumpur, Malaysia. The conference focused on Terrorism Financing through Charities.

IRS-CID participated in delivering the Bulgarian Prosecutor Training course focusing on Following the Money and Dismantling the Criminal Organization in Velinko Tarnovo, Bulgaria, and Plovdiv, Bulgaria. The Department of Justice Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) hosted the program.

IRS-CID participated in delivering an Anti-Money Laundering and Anti-Terrorism Financing Training course in Sarajevo, Bosnia and Herzegovina, for 30 law enforcement agents and prosecuting attorneys. The program was sponsored by The Department of State.

IRS-CID, with the FBI, delivered a Financial Investigative Techniques along with a Terrorism Financing Training course in Cebu, Philippines.

IRS-CID delivered two Financial Investigative Techniques courses, hosted by Overseas Prosecutorial Development Training and Assistance (OPDAT), in Dhaka, Bangladesh.

IRS-CID delivered two Advanced Tax Fraud Investigative Techniques courses, hosted by the U.S. Agency of International Development (USAID), in Manila, Philippines.

IRS-CID delivered a Financial Investigative Techniques Training program in Managua, Nicaragua, with 26 participants. The Department of Justice, Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) hosted the program.

IRS-CID participated in delivering a Financial Fraud Training course in Lagos, Nigeria, with 55 participants from the Economic and Financial Crimes Commission. The Department of State and the FBI hosted the course.

IRS-CID delivered a Financial Investigative Techniques Training in Seoul, South Korea. Thirty participants from several Regional Tax Offices attended. Tax Administration Advisory Services and the National Tax Service of Korea hosted the training.

IRS-CID assisted the FBI in delivering a Terrorism Financing and Money Laundering course in Johannesburg, South Africa. The course was attended by 31 participants; 25 from the Johannesburg Metropolitan Police Department (JMPD) and 6 from the South African National Police.

IRS-CID participated with the FBI in delivering an Investigative Techniques and Anti-Terrorism course in Riga, Latvia. Law enforcement agents and prosecuting attorneys attended the program. The Department of State and the Embassy of the United States Riga, Latvia hosted the training.

IRS-CID assisted delivering a Parallel Financial Investigations Training course with 23 participants from the Ministry of Interior, the Kyrgyz Republic Prosecutor's office, and Kyrgyz Republic State Border Guard Service, in Kyrgyzstan, Russia. The training was hosted by the FLETC International Programs Division.

During FY 2007, the IRS-CI Attache for the Caribbean assisted with the coordination and served as a liaison between the Treasury, Office of Technical Assistance (OTA), and OPDAT, along with the State Department and the Attorney Generals' Financial Investigations Units of Antigua and Grenada to provide a workshop to both countries on financial investigations. The workshops were to assist those countries in formulating methodologies of how to work criminal financial investigations, as well as setting up a handbook for each FIU on policies and procedures when working financial investigations. In both countries, the workshops were a success and in Grenada, the workshop was attended by police officers, as well as prosecutors.

In 2007, IRS-CI Attache for Bogota conducted four classes in Colombia and one class in Costa Rica of advanced money laundering training. In total over 300 host nation law enforcement officers and government attorneys were trained with the financial assistance of OPDAT and ICITAP of U.S. Embassy Bogota.

Office of the Comptroller of the Currency (OCC), Department of Treasury

The Office of the Comptroller of the Currency (OCC) provides Bank Secrecy Act (BSA) and anti-money laundering (AML) guidance to national banks and federal branches of foreign banking organizations and performs on-site examinations of compliance with BSA/AML laws and regulations. The OCC also develops and provides, in conjunction with other federal banking regulators, BSA/AML guidance and training to examiners and foreign banking supervisors. The on-site examinations include reviewing compliance with BSA/AML laws and regulations at some of the largest financial institutions in the world. Working with the other federal banking regulators through the Federal Financial Institution Examination Council (FFIEC), the OCC assisted in revising the FFIEC BSA/AML Examination Manual and provided instructors for the FFIEC Advanced BSA/AML Compliance Conference.

The OCC supported U.S. efforts on Financial Action Task Force (FATF) initiatives and provided AML assistance on projects to regional supervisory bodies, U.S. interagency programs, and projects initiated by the International Monetary Fund (IMF) and World Bank. In February and December, the OCC participated on interagency Financial Systems Assessment Teams (FSAT) to Algeria and Northern Iraq.

Various OCC officials participated in international conferences on combating money laundering. In February and March of 2007, OCC officials were part of a body of U.S. regulators presenting to the international audiences at the Florida International Bankers Association and the Money Laundering Alert's International Conference on Combating Money Laundering. The OCC's senior compliance official was a guest speaker at the Inaugural United States/Latin American Private Sector Dialogue Money Laundering and Counter Terrorist Financing held in Bogotá, Columbia. This official was also a roundtable panelist at the third United States / Middle East North Africa Private Sector Dialogue on Implementing Effective Anti-Money Laundering/Counterterrorist Financing Controls held in Dubai, United Arab Emirates.

The OCC conducted and sponsored a number of anti-money laundering initiatives for foreign banking supervisors during 2007. In May, the OCC sponsored its Anti-Money Laundering/Countering the Financing of Terrorism School in Washington, D.C. The school was designed specifically for foreign banking supervisors to increase their knowledge of money laundering and terrorist financing activities and how these acts are perpetrated. The course provided a basic overview of AML examination techniques, tools, and case studies. Twenty-nine banking supervisors from 17 countries attended. The OCC also provided AML technical assistance to banking supervisors from South Korea, Lebanon, and Russia.

During March, the OCC provided an instructor to the IMF-sponsored Anti-Money Laundering/Combating Terrorist Financing Workshop in the United Arab Emirates. The workshop was tailored for banking supervisors from the Middle East and Northern Africa to provide a basic overview of AML examination techniques, tools and case studies. Thirty-four banking supervisors from the Middle East North Africa region attended the workshop at the Arab Monetary Fund in Abu Dhabi, United Arab Emirates.

Office of Overseas Prosecutorial Development, Assistance and Training, the Asset Forfeiture and Money Laundering Section, & Counterterrorism Section (OPDAT, AFMLS, and CTS), Department of Justice

Training and Technical Assistance

The Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) section is the office within the U.S. Department of Justice (DOJ) that assesses, designs and implements training and technical assistance programs for our criminal justice sector counterparts overseas. OPDAT draws upon the subject matter expertise components within the Department, such as the Asset Forfeiture and Money Laundering Section (AFMLS), the Counterterrorism Section (CTS), and the United States Attorney's Offices across the country to provide expert training and advice to enhance the capacities of our foreign partners. Much of the assistance provided by OPDAT and AFMLS is provided with funding from the Department of State.

In addition to training programs that are targeted to each country's needs, OPDAT also provides long term, in-country assistance through Resident Legal Advisors (RLAs). RLAs are federal prosecutors who provide in-country technical assistance to improve capacity, efficiency and professionalism within foreign criminal justice systems. RLAs are posted to the U.S. Embassy in a country for a period of one or two years to work directly with counterparts in legal and law enforcement agencies, such as the ministry of justice, prosecutor's office and the judiciary. To promote reforms within the criminal justice sector, RLAs provide assistance in legislative drafting, modernizing institutional structures, policies and practices, and training law enforcement personnel including prosecutors, judges, police and other investigative or court officials. For all of its programs, OPDAT draws upon the expertise of the Department of Justice's Criminal Division, the National Security Division, and other DOJ components as needed. OPDAT works closely with AFMLS, the lead DOJ unit in providing countries with technical assistance in the drafting of money laundering and asset forfeiture statutes compliant with international standards.

Money Laundering/Asset Forfeiture

During 2007, DOJ/OPDAT and AFMLS continued to provide training to foreign judges, prosecutors and other law enforcement officials, and assistance in the drafting of anti-money laundering statutes compliant with international standards. The assistance furnished by OPDAT and AFMLS enhances the ability of participating countries to prevent, detect, investigate and prosecute money laundering, and to make appropriate and effective use of asset forfeiture. The content of individual technical assistance programs varies depending on the specific needs of the participants, but topics addressed in 2007 included developing money laundering legislation and conducting investigations, complying with international standards in the anti-money laundering/counterterrorist financing (AML/CTF) area: techniques and methods used for effective investigations and prosecution of money laundering, including the role of prosecutors; criminal and civil forfeiture systems; and the importance of both

international and inter-agency cooperation and communication. AFMLS provides direct technical assistance in connection with legislative drafting on all matters involving money laundering, asset forfeiture and the financing of terrorism. During 2007, AFMLS provided such assistance to 11 countries and continued to participate in meetings of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group on Money Laundering to develop and promote best practices in money laundering and asset forfeiture. AFMLS continued to participate in the Group of Eight (G-8) working groups on corruption and asset sharing and the CARIN Group on asset recovery.

AFMLS provided training to government officials concerned with money laundering issues in Algeria, Azerbaijan, China, Indonesia, Jordan, Kyrgyzstan, Lithuania, Qatar, Saudi Arabia, Turkey and Turkey. Additionally, in 2007, AFMLS provided technical assistance to Algeria, Azerbaijan, the Cayman Islands, Indonesia, Jordan, Kenya, Mexico, Moldova, Pakistan, Vietnam and Yemen.

In an effort to improve international cooperation, AFMLS, in conjunction with the Swiss Federal Office of Justice and the Liechtenstein Ministry of Justice, hosted a conference in Davos, Switzerland, from April 17-20, 2007, on International Forfeiture Cooperation for prosecutors and investigators to discuss nonconviction based forfeiture. This conference brought practitioners, investigators, and international experts together to discuss experiences and provide practical tools to further global cooperation concerning nonconviction based forfeitures. Officials from Austria, Bulgaria, Denmark, Guernsey, Hong Kong, Israel, Jersey, Latvia, Liechtenstein, Luxembourg, the Philippines, South Africa, Switzerland, Turkey, the United Kingdom and the United States participated.

With the assistance of Department of State funding, in 2007 OPDAT provided training to government officials on money laundering and financial crime-related issues to officials from more than 23 countries, including Algeria, Antigua, Azerbaijan, Bangladesh, Bulgaria, Brunei, East Timor, Estonia, Grenada, Indonesia, Jordan, Kyrgyzstan, Latvia, Lithuania, Malaysia, Nicaragua, Pakistan, Paraguay, Philippines, Singapore, South Africa, Turkey, and the United Arab Emirates.

OPDAT conducted the second phase of a mentoring program for financial investigators, intelligence analysts, and attorneys in St. George, Antigua. The program was designed to enhance the ability of Antiguan law enforcement officials to investigate and prosecute financial crimes. During the first phase, held in October 2006, the participants developed a draft of a best-practices handbook for financial investigations and prosecutions. The second phase focused on practical exercises.

OPDAT conducted workshops for prosecutors, investigators, and police in four of the five appellate regions of Bulgaria on financial profiling and financial investigations in dismantling trafficking enterprises. These were part of a series of regional workshops encouraging law enforcement to focus on dismantling human trafficking rings by targeting money and assets.

In June, OPDAT, in conjunction with OTA, conducted two financial crimes seminars for Bulgarian prosecutors, in Veliko Tarnovo, and Plovdiv, Bulgaria. The purpose of the programs was to share experiences and lessons learned when investigating and prosecuting financial crime and money laundering cases.

OPDAT conducted a program on money laundering and organized crime in Johannesburg, South Africa, for approximately 115 participants from the South African Police Service and National Prosecuting Authority. Topics included coordination between police and prosecutors; witness protection; crime participants as witnesses; international cooperation; and a review of the South African money laundering statute in terms of subpoena authority, bank reporting requirements, and roles of estate agents and transferring attorneys.

In St. George's, Grenada, OPDAT conducted the first phase of a program designed to enhance the ability of Grenada's law enforcement to investigate and prosecute financial crimes. During the

workshop, 25 participants, including financial investigators and prosecutors, developed a draft of a best practices handbook for financial investigations and prosecutions.

Resident Legal Advisors

The OPDAT RLA to Azerbaijan, with participation from AFMLS, organized a seminar on "Investigating and Prosecuting Money Laundering and Financial Crimes" in Baku, Azerbaijan. The program was geared toward providing technical assistance on Azerbaijan's draft anti-money laundering/counterterrorist financing legislation.

In late November and early December, the OPDAT RLA to Bulgaria, in conjunction with the Bulgarian Association of Prosecutors, conducted three two-day regional workshops on financial crimes for Bulgarian prosecutors. Topics included the legislative framework in Bulgaria and the European Union for combating financial crimes, evidentiary standards for financial crime cases, procedure in financial crimes cases, and the enterprise theory.

Terrorism/Terrorist Financing

Since 2001 OPDAT, CTS, and AFMLS have intensified their efforts to assist countries in developing their legal infrastructure to combat terrorism and terrorist financing. OPDAT, CTS, and AFMLS, with the assistance of other DOJ components, play a central role in providing technical assistance to foreign counterparts both to attack the financial underpinnings of terrorism and to build legal infrastructures to combat it. In this effort, OPDAT, CTS, and AFMLS work as integral parts of the U.S. Interagency Terrorist Financing Working Group (TFWG) in partnership with the Departments of State, Treasury, Homeland Security's Immigration and Customs Enforcement (ICE), and several other DOJ components.

TFWG, co-chaired by State INL and the Coordinator for Counterterrorism (S/CT) currently supports seven RLAs assigned overseas. The RLAs are located in Bangladesh, Indonesia, Kenya, Pakistan, Paraguay, Turkey, and the United Arab Emirates (UAE). Working in countries where governments are vulnerable to terrorist financing, RLAs focus on money laundering and financial crimes and developing counterterrorism legislation that criminalizes terrorist acts, terrorist financing, and the provision of material support or resources to terrorist organizations. The RLAs also develop technical assistance programs for prosecutors, judges and, in collaboration with DOJ's International Criminal Investigative Training Assistance Program (ICITAP), police investigators to assist in the implementation of new money laundering and terrorist financing procedures.

In March 2005, OPDAT placed its first RLA in South Asia at Embassy Dhaka with the goal of assisting the Government of Bangladesh in strengthening its anti-money laundering/terrorist financing regime, and improving the capability of Bangladeshi law enforcement to investigate and prosecute complex financial and organized crimes. During 2007, despite an often unpredictable political climate, the RLA continued to provide assistance to Bangladeshi officials in their efforts to establish an effective anti-money laundering and terrorist financing regime.

In January 2007, the RLA conducted programs designed to support the development of procedures for Bangladesh Bank (BB) and police investigators (CID) to follow when reviewing suspicious transaction reports (STRs) for possible investigation.

At the request of the Bangladeshi government, the RLA organized two courses on Financial Investigations. Three instructors from the Internal Revenue Service (IRS) Criminal Investigation Division (CID) presented two week-long courses on Financial Document Analysis to a total of 60 participants from the police, Attorney General's Office, Central Bank's Anti-Money Laundering Unit, the National Board of Revenue (Bangladesh IRS), and the Anti-Corruption Commission. OPDAT has

provided drafting assistance to the Government of Bangladesh (GOB) on the Anti-Money Laundering Law, most recently in August 2007.

OPDAT and the U.K. Charity Commission jointly sponsored a three-day workshop entitled "Protecting Charities from Financial Abuse" in Dhaka, Bangladesh. The focus on the workshop was to ensure that nongovernmental organizations (NGOs) and charities are not abused by terrorist groups. Participants learned about technical analysis for preparing investigations, assessing threats to NGOs including why they are uniquely vulnerable to abuse due to the areas in which they work and the methods of working, ways of gathering information about NGOs, and analyzing data and suspicious transaction reports.

OPDAT provides regular assistance to the Government of Bangladesh to enable it to become the first South Asian nation admitted to the Egmont Group.

The OPDAT RLA program in Indonesia began in June 2005. In 2007, the RLA continued to engage the Attorney General's Terrorism and Transnational Crime Task Force (SATGAS), which OPDAT helped establish as an operational unit in 2006. The task force is responsible for prosecuting significant pro-active cases involving four key areas: terrorism, money laundering, trafficking in persons and cyber crime. The SATGAS unit has nationwide jurisdiction for such prosecutions, but also works with the local offices to promote such prosecutions. Over the course of 2007, the RLA conducted a number of regional training programs for SATGAS. All the programs focused on providing substantive knowledge to local prosecutors concerning the task force's four priorities while building relationships between the members of the task force and the prosecutors in the field. The RLA engaged the experienced members of the SATGAS as fellow presenters in the trainings. The use of experienced Indonesian SATGAS prosecutors as instructors elicited a high level of engagement on the part of the local prosecutors. Due to the size of Indonesia and SATGAS' national mandate, regional training and outreach is a key element in USG support for SATGAS.

The RLA brought each of the members of SATGAS to the U.S. in two groups for ten-day study programs in April and November 2007. The RLA designed the program to give the SATGAS prosecutors a detailed look at how terrorism and transnational crimes are investigated and prosecuted in the U.S. The visit involved a combination of substantive presentations by DOJ experts, informal discussions with prosecutors, judges, and defense attorneys, courtroom observations, and law enforcement visits. Major themes included specialization of functions within the DOJ, police/prosecutor coordination, terrorist financing, and witness/victim security.

The OPDAT RLA program in Kenya began in 2004. In 2007, the RLA, on detail from the DOJ's Counterterrorism section, continued to engage Government of Kenya (GOK) partners, such as the Department of Public Prosecutions (DPP), Kenya Anti-Corruption Commission (KACC), Law Society of Kenya (LSK), and others in a program that focuses on counter-terrorist financing, anti-corruption, and procedural reform. The RLA participated as one of the chief speakers in the first joint OPDAT-United Nations Office on Drug Control (UNODC) counterterrorism program in Nairobi in November 2007. The RLA made presentations on the handling of counterterrorism cases, and dealing with legal and evidentiary issues peculiar to these cases to an audience that included the Kenya National Counterterrorism Center (prosecutors, analysts, and investigators) and select members of the Anti-Terrorism police.

Despite the difficult political climate in Pakistan, OPDAT launched its RLA program at Embassy Islamabad in September 2006. The RLA, to the extent possible, has concentrated on assisting Pakistan in combating terrorist financing and money laundering, judicial reform, judicial security and intellectual property rights violations.

On August 8, 2007, Pakistan adopted a criminal money laundering law in the form of a presidential ordinance. The ordinance adopted the draft legislation that had been pending before the National

Assembly since 2005, and was in response to increasing international pressure on Pakistan to pass an effective AML Bill. The RLA will continue to monitor and report on efforts to implement the legislation.

The OPDAT RLA program in Paraguay began in 2003, when OPDAT dispatched the first counterterrorism RLA to Asuncion. This position now carries regional responsibilities in the Tri-Border Area (TBA), which encompasses Paraguay, Argentina, and Brazil.

In August 2007, the RLA organized a Penal Code Retreat, during which the Senate Committee charged with amending the Penal Code worked on final revisions. Subsequently later in August, the Paraguayan Senate passed the amendments, which contain a revised money laundering statute. The statute will bring Paraguay into general compliance with international standards relevant to prosecuting money laundering cases. This statute will greatly assist Paraguay in its fight against money laundering in all types of cases including narcotics and public corruption.

Also in August, OPDAT organized a Tri-Border Terror Financing/Money Laundering conference in Asuncion, Paraguay, featuring participants from Paraguay, Argentina, and Brazil. The speakers consisted primarily of U.S. Counter Terrorism Prosecutors and representatives from law enforcement and intelligence agencies. The focus of the conference was money laundering and terrorist financing in the Tri-Border Area.

The OPDAT program in Ankara, Turkey, began in September 2006 and includes three prongs: anti-money laundering, terrorist financing and PKK issues, but the latter colors every substantive issue in which the RLA has been involved. In January 2007, the RLA hosted a legislative roundtable on methods to investigate and prosecute terrorist organizations, particularly the PKK. In this meeting, terrorism prosecutors from Turkey met with their counterparts from several European countries to discuss strategic applications of their respective laws in fighting terrorism. Significantly, the European participants described their laws and expressed their desire to work with the Turkish prosecutors to build better international cases. The two-day workshop was filled with candid discussions on expediting flows of information and the possibilities and caveats in using classified information in prosecutions and specific cases.

In September 2007, the RLA, a trial attorney on detail from AFMLS, conducted a program on anti-money laundering in Algiers, Algeria, for approximately 40 prosecutors, police and judges from the Algerian government. The seminar provided the first opportunity for Algerian and French prosecutors to discuss matters of common interest. Topics covered an overview of international anti-money-laundering standards and best practices, Algerian anti-money laundering laws, financial institutions as defendants, maximizing the financial intelligence unit, taking the profit out of crime through asset forfeiture and international sharing, and money laundering and terrorist financing case studies from the U.S., Algeria, and France. It was a successful first step and OPDAT plans to conduct a follow up workshop.

From October 31-November 1, 2007, OPDAT held an anti-money laundering course, with participation by AFMLS, for Turkish prosecutors, judges, and police in Istanbul, Turkey. The course focused on financial crimes involving banks and other financial institutions and the need to involve such institutions if a country's anti-money laundering regime is to succeed.

OPDAT initiated the United Arab Emirates (UAE) RLA program in 2005. In 2006, OPDAT expanded the UAE RLA portfolio to include assistance to other states in the Gulf Region in combating money laundering and terrorist financing. Throughout 2007, the RLA continued to work on financial crimes, terrorist financing, and money laundering issues. The RLA traveled to Jordan, Kuwait, and Qatar to meet with the key players in the Anti-Money Laundering/Counterterrorist Financing (AML/CTF) field in the host governments. The RLA carried out AML/CTF training in Amman, Jordan, in February-March 2007, in collaboration with Treasury's Office of Technical Assistance (OTA) and in

conjunction with AFMLS. The seminar was designed to bring together key personnel from all government agencies that would participate in Jordan's financial intelligence unit (FIU), once AML legislation was passed. The week-long course included practical exercises and familiarized analysts, investigators and prosecutors with AML/CTF strategies and best practices. The Jordanian Parliament was later reconvened for the specific purpose of considering AML legislation, which was passed and went into effect in June 2007. The RLA is currently in the process of planning an assistance program in Kuwait, set to take place in the spring of 2008.

On December 10-11, 2007, OPDAT organized a "Prosecuting Financial Crimes Seminar," held in Dubai, UAE. The seminar is the first of its kind to be sponsored by both the UAE Institute of Training and Judicial Studies and the Dubai Institute of Advanced Legal and Judicial Studies. The seminar featured case studies designed to promote AML/CTF best practices, and included an overview of anti-money laundering enforcement initiatives to combat bulk cash smuggling.

In addition to the programs organized by the seven counterterrorism RLAs, in 2007, OPDAT conducted several bilateral and regional counterterrorism training programs. In May 2007, OPDAT organized a regional program on money laundering and terrorist financing through charities and new technology that took place in Kuala Lumpur, Malaysia. Representatives from Bangladesh, Pakistan, Singapore, Malaysia, Indonesia, Philippines, Brunei, and East Timor participated in this four-day program of lectures, table top exercises, and panel discussions. The program covered the use and abuse of charities and use of new technology in financing terrorism, the investigation and prosecution of such crimes, and the seizure, freezing, forfeiture and management of assets. Representatives from the eight participating countries had opportunities to work on practical problems and share best practices. The participants from Pakistan have asked for a similar training to be conducted in Pakistan for a broader range of Pakistani participants.

On December 4-6, 2007, OPDAT and the DOJ Office of International Affairs (OIA) conducted a workshop in Manila, Philippines, on investigations and prosecutions in cases involving terrorism and terrorist financing, including the use of electronic surveillance. The need for such a program arose due to the fact that earlier in the year, the Philippines adopted the Human Security Act (HSA) of 2007 (Republic Act No. 9372). This law for the first time allows the use of electronic surveillance in court in cases involving terrorism. The workshop was geared toward policy level officials with the Philippines Department of Justice who are working on guidelines for implementation of the HSA and upper level officials from the agencies that make up the "Anti-Terrorism Council," which is charged to implement the HSA.

During the course of 2007, OPDAT and CTS met with and provided presentations to international visitors from more than 25 countries on counterterrorism topics. The presentations covered the way the United States addresses terrorism in the post 9-11 world. Topics covered include legislation passed and pending at the time of the presentations, and issues raised in implementing new legislative tools and the changing relationship of criminal and intelligence investigations. The USA PATRIOT Act, PATRIOT Improvement and Reauthorization Act, Intelligence Reform and Terrorism Prevention Act, Foreign Intelligence Surveillance Act, terrorist financing and material support statutes, and the Classified Information Procedures Act are among the significant pieces of legislation addressed. Of great interest to visitors is the balancing of civil liberties and national security issues, which is also addressed. When possible, CTS and U.S. Attorney Offices have Trial Attorneys or Assistant United States Attorneys who have case or investigation experience with the visitors' countries, participate in the programs.

Organized Crime

During 2007, OPDAT organized a number of programs for foreign officials on organized crime, which included such topics as corruption, money laundering, implementing complex financial investigations

and special investigative techniques within a task force environment, international standards, legislation, mutual legal assistance, and effective investigation techniques.

OPDAT RLAs continued to support Bosnia's Organized Crime Anti-Human Trafficking Strike Force and the Strike Force's working relationship with officials in Albania, Bulgaria, Kosovo, Macedonia, and Serbia and Montenegro, through mentoring and training programs on investigating and developing organized crime case strategies.

OPDAT conducted a regional program on combating transnational organized crime in Eurasia at the International Law Enforcement Academy (ILEA) in Budapest, Hungary, for prosecutors and investigators from Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, and Ukraine. The program addressed the increasing capacity of criminal organizations to operate in multiple jurisdictions and across national borders, and the legal challenges this presents for law enforcement. Particular attention was given to the increasing use of "shell" corporations by organized crime groups and the need to provide law enforcement with adequate tools to track such information across borders.

OPDAT hosted a U.S. study for six Macedonian prosecutors, four Macedonian judges, and one Macedonian police officer on combating organized crime. The objectives of the study tour were for the Macedonian prosecutors to improve their skills in working with the police to develop organized crime cases, and the ability to present the cases effectively in court. The study tour provided for both the Macedonian prosecutors and judges to become more familiar with methods, techniques, and resources that can be utilized when adjudicating organized crime cases involving narcotics, money laundering, and corruption, and the connection of such cases to trafficking in persons (TIP) cases.

Then in August 2007, OPDAT conducted an anti-organized crime program for 25 judges in George, South Africa. It focused on the application of South Africa's anti-racketeering law, which has been a key ingredient of the DOJ assistance program in South Africa for the past four years. With the use of the anti-racketeering law (similar to the U.S. Racketeer Influenced and Corrupt Organizations Act or "RICO" statute) on the rise among South African prosecutors, South African judges now appreciate the need to understand the nuances of this important prosecutorial tool.

From October 7-20, 2007, the OPDAT Resident Legal Advisor to Kosovo escorted five organized crime prosecutors from the Kosovo Special Prosecutors' Office (KSPO) and three of their legal officers on a study tour of U.S. Attorneys' Offices in Detroit and Cleveland during October 2007. The tour included discussions of border security, counterterrorism, public corruption, computer evidence, physical evidence, financial crime and human trafficking and organized crime from Eastern Europe. The members of the KPSO observed the opening statements and initial witnesses in a complex financial crime and corruption case and discussed how to incorporate questioning and evidentiary techniques under the Kosovo criminal procedures code.

During November 2007, OPDAT and the Public Affairs Office at the U.S. Embassy in Sofia, Bulgaria, conducted programs in three cities in Bulgaria—Veliko Tarnovo, Blagoevgrad, and Sofia—to raise awareness of the importance of combating organized crime. The programs were designed to build political and public will against organized crime in Bulgaria through a series of discussions with widely varying audiences, including but not limited to prosecutors and judges, on how the U.S. and Bulgaria have fought organized crime.

Fraud/Anticorruption

In 2007, OPDAT continued to provide global technical assistance for prosecutors and investigators to improve their prosecutorial and investigative abilities to combat public corruption.

In March 2007, the OPDAT RLA to Nicaragua organized a workshop for Nicaraguan law enforcement officials responsible for investigating and prosecuting corruption-related crimes. The goal of the

workshop was to help the participants draft a handbook of best practices for investigating and prosecuting corruption and related crimes and thereby enhance the participants' willingness and ability to work together on investigations and prosecutions. A select group of 22 members of Nicaragua's law enforcement community participated in the workshop, including members of the Attorney General's Office investigators from the Nicaraguan National Police (NNP) Financial Crimes Division, attorneys for the Superintendence of Banks, and one legislative assistant to the National Assembly working in the area of justice sector reforms.

From February 27-March 1, 2007, OPDAT organized a seminar on election fraud and related corruption in Yerevan, Armenia, for Armenian police, prosecutors, and election officials. Subsequently, on March 10-17, OPDAT conducted a U.S.-based study tour in Washington, DC, and Charleston, WV, for an Armenian delegation of six prosecutors and two Central Election Committee officials. The program focused on demonstrating the U.S. approach to preventing, detecting, investigating and prosecuting election fraud and related corruption via a series of case studies. Then, in April in Yerevan, the Armenian Prosecutor General's office hosted a roundtable discussion of potential amendments to the CPC and electoral code, as well as a training conducted by the participants of the study tour to other police, investigators and prosecutors.

In June 2007, OPDAT, in close collaboration with AFMLS, conducted a program on anti-corruption, financial crimes, and organized crime for 25 Lithuanian prosecutors and representatives from the Ministry of Justice in Vilnius, Lithuania. This was last of three programs presented in the Baltics focusing on lessons learned and best practices when investigating and prosecuting corruption, organized crime and financial crime cases.

On May 22, 2007, the Government of Albania announced the establishment of a Joint Investigative Unit (JIU) to Fight Economic Crime and Corruption. The JIU, which was established in September 2007, brings together prosecutors, police officers, tax and customs officials to investigate and prosecute financial crime and corruption in the district of Tirana. The establishment of the JIU is due in large part to the efforts of the OPDAT RLA to Albania, who continues to provide technical assistance to the investigative unit through training, support, and mentoring. In December 2007, the RLA organized a one-day training session for JIU staff on investigation and prosecution of corruption cases. The training focused on discussion of actual case studies, shared by both U.S. and Albanian prosecutors.

OPDAT conducted an anti-corruption program for Azeri prosecutors, investigators and judges in Baku, Azerbaijan. The conference focused on Azerbaijan's draft National Anti-Corruption Strategy and its compliance with UN and GRECO obligations. The program also had a capacity building component to enhance the attendees' skills in detecting, investigating, prosecuting and adjudicating corruption cases.

In June 2007, OPDAT organized an Anti-Corruption Technical Workshop in Baku, Azerbaijan. This workshop brought together about 30 participants, including a dozen key members of the Anti-Corruption working group, a media representative, members of civil society and nongovernmental organizations (NGOs), U.S. Agency for International Development (USAID), COE and DOJ where they engaged in a working dialogue and produced many specific recommendations for the new Anti-Corruption National Strategy.

In September, OPDAT organized another anti-corruption workshop in Baku, Azerbaijan, titled "Prosecuting Corruption Crimes: Gathering Evidence and Detecting, Freezing and Confiscating Criminal Proceeds." The was the first in a series of workshops on prosecuting corruption crimes in Azerbaijan held at the Prosecutor General's Training Center in Baku for an audience of investigators and prosecutors. The workshop focused on how to gather evidence of corruption crimes and how to detect, freeze and confiscate criminal proceeds.

Also in September 2007, OPDAT organized an anti-corruption training in Bishkek, Kyrgyzstan. The training focused on the investigation and prosecution of anti-corruption cases, and coincided with the OPDAT RLA's effort to assist the Kyrgyz in implementing pending changes and reforms to their criminal law system. Specifically, the Kyrgyz Parliament has enacted new laws that shift warrant power from prosecutors to judges; the Kyrgyz are also in the process of drafting a new jury trial law. The OPDAT training program provided Kyrgyz investigators, prosecutors, and judges with the knowledge, skills, and abilities to better investigate and prosecute corruption cases, while ensuring the investigation will be successful when tried before a trial by jury.

The RLA to Serbia conducted an anti-corruption program for approximately 50 Montenegrin prosecutors and investigators (police, tax and customs) in Przno, Montenegro. Because of the lack of corruption cases actually investigated or prosecuted in Montenegro, the training focused on some of the initial steps in developing corruption cases, including developing informants, developing cases through financial investigations, and conducting simple special investigative techniques (primarily recorded conversations) to obtain evidence in these cases.

Following the program in Montenegro, in December the RLA to Serbia conducted a regional conference on anti-corruption for prosecutors and investigators from western and central Serbia, in Zlatibor, Serbia. Entitled "Challenges and Successes in Combating Corruption in Serbia," the program covered theories, best practices, and highlighted a successful prosecution of a Supreme Court Judge for bribery by the Organized Crime Prosecutor's Office in Belgrade. The conference also served to initiate a series of regularly scheduled, one day round tables for prosecutors and police to discuss problems and solutions relating to corruption cases.

Also in December, the RLA to Georgia organized a series of practical seminars on preventing and prosecuting election fraud and misconduct in anticipation of Georgia's January 5th Presidential election. The focus of the seminar were best practices in investigating and prosecuting a variety of election crimes, the ethical obligations of prosecutors during election time, and appropriate intake procedures for complaints regarding alleged irregularities and illegalities during the campaign.

Justice Sector Reform

In 2007, DOJ's Justice Sector Reform Program in Colombia focused on four specific areas: (1) continued assistance in the implementation of the accusatory system, (2) assistance in specialized areas of criminal law, (3) implementation of justice and peace law, and (4) security and protection programs. In 2007, DOJ trained over 1,000 prosecutors, 13,000 police, 300 judges, and 200 forensic scientists in the accusatory system and implementation of the new Colombian Criminal Procedure Code—all of whom will be implementing the new Code in their respective judicial districts in 2008 as implementation of the new law takes effect in every region of the country. This training involved intensive, practical training in the concepts and legal underpinnings of an accusatory system and the new Code, as well as the technical skills and practical application necessary for implementation—crime scene management, forensic development and presentation of forensic evidence, witness interview, trial preparation, chain of custody and presentation of evidence at trial, trial techniques, investigation and prosecution strategy, police/prosecutor cooperation. DOJ also provided equipment to facilitate the implementation of the new Code. DOJ's assistance in specialized areas of criminal law included training for prosecutors, investigators, and forensic scientists in money laundering, anti-kidnapping, sex crimes, anti-corruption, forensic anthropology, intellectual property, and human rights. DOJ initiated training and technical assistance as well as providing equipment, office and court facilities development, and operational funds for the Prosecutor General's Justice and Peace Unit tasked with the investigation, interviewing and prosecution of demobilized paramilitary members under the Justice and Peace law. DOJ also provided similar assistance to the Colombian magistrates who will be involved in the court proceedings under this law. In the area of protection, DOJ continued

to provide judicial protection training to Colombian protection details and began a shift in this protection training and assistance to courtroom and courthouse security. Over 200 protection personnel were trained in 2007. With the placement of a USMS official in the Embassy in Bogota, DOJ is effectively assisting the Colombian Prosecutor General's Office develops a viable witness protection program.

OPDAT currently has seven Resident Legal Advisors (RLAs) in Iraq assisting the Iraqi justice sector in enhancing sustainable institutions built on the rule of law, with plans to expand the program in 2008. Presently, two RLAs are stationed in Baghdad, four RLAs are deployed to Provincial Reconstruction Teams (PRTs) in Iraqi provinces, (Ninewa, Salah ad Din, Kirkuk and Baghdad), and one RLA is stationed at the Law and Order Task Force (LAOTF) in the Rusafa section of Baghdad. As members of an interdisciplinary reconstruction effort, OPDAT RLAs work with local police and judges to identify and overcome obstacles to effective, fair prosecutions. The RLAs stationed in Baghdad advise the U.S. Embassy, the Iraqi Higher Juridical Council, the Central Criminal Court of Iraq, and other Baghdad-area courts on criminal justice, judicial independence, and the rule of law in coordination with the Rule of Law Coordinator's Office in the Embassy. In the PRTs, RLAs actively pursue projects to establish lasting mechanisms for handling serious crimes, including terrorism, kidnapping, and murder. In 2007, under the leadership of OPDAT RLAs, major crimes prosecutions began in provinces outside of Baghdad for the first time since the fall of the former regime in 2003. RLAs also develop and implement training programs for Iraqi Police and investigators with input and direction from local judges. They also work with NGOs, law schools and other USG and international agencies to advance the rule of law in Iraq.

Office of Technical Assistance (OTA), Treasury Department

The Treasury Department's Office of Technical Assistance is located within the Office of the Assistant Secretary for International Affairs. OTA has five training and technical assistance programs: tax reform, government debt issuance and management, budget policy and management, financial institution reform, and, more recently, financial enforcement related to money laundering, terrorist financing, and other financial crimes.

Fifty-six highly experienced intermittent and resident advisors comprise the Financial Enforcement Team. These advisors provide diverse expertise in the development of anti-money laundering/ccounter-terrorist financing (AML/CTF) regimes, and the investigation and prosecution of complex financial crimes. The Financial Enforcement Team is divided into three regional areas: Europe and Asia, Africa and the Middle East, and the Americas. Each region is managed by a full-time regional advisor.

OTA receives funding from USAID country missions and direct appropriations from the U.S. Congress. OTA has been designated as the recipient of Millennium Challenge Corporation (MCC) funding to provide assistance to a number of Threshold Countries to enhance their capacity to address corruption and related financial crimes.

Assessing Training and Technical Assistance Needs

The goal of OTA's Financial Enforcement program is to build the capacity of host countries to prevent, detect, investigate, and prosecute complex international financial crimes by providing technical assistance in three primary areas: money laundering, terrorist financing, and other financial crimes; organized crime and corruption; and capacity building for financial law enforcement entities.

Before initiating any training or technical assistance to a host government, the OTA Enforcement team conducts a comprehensive assessment to identify needs and to formulate a responsive assistance program. These needs assessments address the legislative, regulatory, law enforcement, and judicial

components of the various regimes, and include the development of technical assistance work plans to enhance a country's efforts to fight money laundering, terrorist financing, organized crime, and corruption. In 2007, such assessments were carried out in Ecuador, Honduras, Argentina, Sao Tome and Principe, Tunisia, Kosovo, Pakistan, and Vietnam.

Anti-Money Laundering and Counter-Terrorist Financing Training

OTA specialists delivered anti-money laundering and counter-terrorist financing courses to government and private sector stakeholders in a number of countries. Course topics included money laundering and financial crimes investigations; identification and development of local and international sources of information; operations and regulation of banks and nonbank financial institutions, including record keeping; investigative techniques, including electronic surveillance and undercover operations; forensic evidence; computer assistance; interviewing; case development, planning, and organization; report writing; and, with the assistance of local legal experts, rules of evidence, search, and seizure, as well as asset seizure and forfeiture procedures.

In Africa and the Middle East, OTA delivered the Financial Investigative Techniques (FIT) course in Botswana, Ethiopia, Jordan, Lesotho, Malawi, Mauritius, Namibia, Seychelles, and South Africa. OTA collaborated with the Department of Homeland Security (DHS), Immigration and Customs Enforcement, and Customs Border Protection to deliver bulk cash smuggling training to the 14 member countries of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) in Livingstone, Zambia and the 15 member countries of the Interagency Action Group Against Money Laundering and Terrorist Financing in West Africa (GIABA) in Dakar, Senegal. Separately, OTA funded DHS presenters in delivering bulk cash smuggling training to law enforcement and regulatory officials following the training in Livingstone.

OTA sponsored officials from several African countries to attend the Office of the Comptroller of the Currency (OCC) annual anti-money laundering and counterterrorist financing training in Washington, D.C. Officials from Namibia, Ethiopia, Zambia, and Malawi were sponsored to attend this advanced training. In addition, OTA funded officials from the FIUs of Seychelles and Malawi for a study and orientation tour of the Mauritius FIU. OTA also funded the Director of the Mauritius FIU to participate in an AML workshop in Malawi, sponsored by the Bank of Malawi, and for a round table discussion with the FIU Director and staff members of the FIU.

In Asia, OTA conducted financial investigative techniques training in Sri Lanka and Vietnam. OTA also conducted several training sessions for Philippine border control agencies on bulk cash smuggling. In Central Asia, OTA provided training and mentoring assistance to law enforcement agencies and banking institutions in Kyrgyzstan and Kazakhstan.

In Europe, OTA teams delivered a variety of technical assistance products, including financial investigation training programs in Croatia, Serbia, Montenegro and Poland; anti-money laundering and antifraud training for the insurance industry in Slovenia; a "train-the-trainer" program on auditing techniques for concerned officials in Armenia; courses in criminal intelligence analysis in Bulgaria; investigative training for the financial police in Georgia; and counterfeiting and anti-money laundering/counterterrorist financing seminars for investigative agencies in Serbia and Montenegro. The seminars in Serbia and Montenegro covered bulk cash smuggling, alternative remittance systems, trade-based money laundering, corruption, using local crime to fund terrorist activities, and investigative techniques. Additionally, OTA funded a study tour for personnel from the Montenegro prosecutor's office, police, and FIU to FinCEN and various interagency investigative task forces.

In the Americas, financial investigative techniques training was provided in the Dominican Republic, El Salvador, Peru, and Chile. In the Dominican Republic, advisors conducted an AML/CTF training seminar for the Superintendent of Banking. In El Salvador, a two-week FIT course was delivered to

tax and customs investigators. In Chile, OTA and OPDAT delivered a combined FIT/Mock Trial course to prosecutors within the Attorney General's Office, the Ministerio Publico, the Consejo de Defensa del Estado, and elements of Chile's investigative police, and to participants from Peru and Bolivia. In Peru, OTA provided Regional FIT training for Argentina, Brazil, Chile, Colombia, Ecuador, Peru and Uruguay. In Montserrat, OTA assisted the Financial Services Commission with the development and delivery of an AML/CTF seminar.

Support for Financial Intelligence Units

In Afghanistan, OTA continued to assist in the development of an FIU as a semi-autonomous unit within Da Afghanistan Bank. In Sri Lanka, OTA's resident advisor helped to stand up an operational FIU. Resident advisors in Albania, Bulgaria, Montenegro, and Serbia, and intermittent advisors in Armenia and Georgia, continued to deliver technical assistance to streamline and enhance host governments' FIUs. In Georgia, this assistance included information technology (IT) development.

In Namibia, Ethiopia, Seychelles and Jordan, advisors were engaged with the respective Central Banks. In Malawi, OTA continued its project under the Millennium Challenge Corporation Threshold Program, following the unexpected accidental death of the resident Enforcement advisor, by assigning an FIU development expert and other advisors to continue working with the Malawi FIU that had recently been established, and to work on improving the capacity of the government to combat financial crimes.

In Paraguay, OTA Advisors made an assessment trip to determine the analytical and IT operational capacity within the FIU (SEPRELAD), as a basis for providing technical assistance in these areas.

Casino Gaming

In the Casino Gaming Group, OTA combines experts from its Tax and Financial Enforcement Teams and has been providing technical assistance to the international community in the areas of Gaming Industry Regulation since 2000. The program provides assistance in the drafting of gaming legislation, and in drafting the regulations required to implement the laws. The program also includes the provision of technical training to gaming industry regulators, including FIU personnel, to provide the capacity for auditing and inspecting casino operations and all games of chance. In addition, advanced technical workshops have been conducted in Las Vegas involving regulators from participating countries. The program has been well received by host country officials who see it as both a valuable revenue-producing project and an anticorruption measure. They also view the assistance as very beneficial in fostering the host country's compliance efforts with the Financial Action Task Force (FATF) 40 Recommendations as they relate to casinos. In 2007, the OTA Casino Gaming Group conducted technical assistance and training, as described above, in Bulgaria, Bosnia-Herzegovina, Philippines (training sessions for the Philippine Gaming Commission), and Chile. Several South American countries participated in the training programs in Chile. Also during 2007, the Casino Gaming Group conducted an assessment of the gaming regulatory system and anti-money laundering programs for casinos in Latvia. The Group participated in a conference in Trinidad to highlight the importance of strong gaming regulatory oversight and the money laundering vulnerabilities within the casino gaming industry.

Money Services Businesses

Money services businesses (MSBs) offer several types of services, including check cashing, money transmissions, currency exchange, and more. Because of the high volume of their cash transactions, and because account relationships with related customer identification procedures are absent (resulting in an uncertain audit trail), MSBs are vulnerable to abuse for the purpose of money laundering and

terrorist financing. For this reason, the FATF Recommendations call upon governments to regulate MSBs.

In April and May 2007, OTA collaborated with the Financial Action Task Force on Money Laundering in South America (GAFISUD) in the organization and presentation of two regional workshops on the oversight, regulation, and examination of MSBs. Thirty-seven regulators, analysts, and financial investigators from seven of its member countries gathered in Lima, Peru for this training. OTA advisors also participated in conferences in the Dominican Republic, and in Trinidad and Tobago, to highlight the vulnerabilities of MSBs relative to money laundering and terrorist financing, and the need for strong regulatory/supervisory regimes.

Insurance

OTA continued its program to provide technical assistance relating to insurance enforcement, begun in 2006. Compromise of an insurance system weakens an economy and provides avenues for money laundering. Since inception of the program, insurance assistance has been provided in all three OTA geographic regions.

In 2007, insurance assistance was provided in a number of countries and included two long-term projects in Paraguay and Jordan. A study of the insurance system in Argentina was also completed as part of a comprehensive study of the financial services for possible OTA assistance in 2008, relating to money laundering.

The assistance in Paraguay centered on insurance company compliance with AML requirements. Information was provided for a new insurance AML compliance regulation; new inspection procedures were completed for regulators that included on-site testing; and training was provided to the inspectors. In Jordan, assistance was provided to establish an insurance anti-fraud effort, including a regulatory framework, AML compliance by the insurance industry, and an antifraud investigation unit with electronic reporting and case management systems. Training in Jordan included participation in a Middle East regional conference, workshop training for regulatory inspectors to detect insider criminal activity, and training for the newly established FIU.

Two AML conferences in Bulgaria provided insurance training for the financial services sector, with one directed toward regional regulators and the other focusing on the industries. OTA also participated in conferences held in Slovenia, with regional attendance, and in Jamaica.

Regional and Resident Advisors

OTA resident advisors continued international support in the areas of money laundering and terrorist financing. In February 2008, OTA will move its Africa and Middle East Regional Advisor, previously based in Pretoria, to Cairo, Egypt to gain a more favorable logistical position to develop and support programs in the Middle East and North Africa. In September 2007, OTA posted an advisor to the Africa Development Bank in Tunis, Tunisia, replacing the incumbent advisor, to provide assistance in the development and implementation of an anticorruption strategy for the Bank and its member countries. In September 2007, a full time resident advisor was posted in Namibia to continue efforts there to establish an FIU. OTA was selected as the MCC implementing agency for the reform of tax and customs agencies in Sao Tome and Principe, and initiated this two-year project in November 2007 with the deployment of long-term TDY advisors. OTA continued its assistance in Jordan by extending the presence of a resident advisor to work with Jordan law enforcement, regulatory, and customs authorities, and with the Central Bank of Jordan in establishing its FIU. The resident advisor in Jordan will also provide assistance to other countries in the region as needed. In Zambia, a resident advisor continued to support national efforts against financial crimes.

OTA's regional advisor for Europe and Asia participated in observer status as part of a nascent European Commission effort to provide AML technical assistance to the northern part of Cyprus. As previously noted, the resident advisors in Albania and Bulgaria continued efforts to streamline and enhance host governments' FIUs. OTA continued its support to the Secretariat of the Eurasian Group to Combat Money Laundering and Terrorist Financing (EAG) through its resident advisor in Moscow. Supporting national efforts against financial crimes was the focus of the resident advisors in Albania, Montenegro, Serbia, and Zambia. The OTA resident advisor in Armenia provided technical assistance on internal audit. OTA placed a new resident advisor in Kabul, Afghanistan, in February 2007, and continued to assist in the development of an operational FIU within the Da Afghanistan Bank (Central Bank). OTA was also instrumental in helping to establish a licensing regime for hawala dealers in Afghanistan. OTA's resident advisor in Colombo, Sri Lanka has been assisting in the development of an effective anti-money laundering and counter-terrorist financing regime, to include the establishment of an FIU that meets international standards.

In Argentina, OTA's resident advisor worked closely with the GAFISUD secretariat to coordinate AML/CTF Technical Assistance Needs Assessments for GAFISUD member countries; to support GAFISUD Working Group regional programs for the development of policies, procedures and the use of technology by FIUs; and to complete a calendar of regional training initiatives, including Financial Investigative Techniques courses, Casino and Gaming workshops, and Money Services Businesses courses. In Chile, OTA continued to provide technical assistance and training to the Superintendent of Casinos, and investigative training to police and prosecutors.

Under the auspices of the Millennium Challenge Corporation Threshold Program established for Paraguay, OTA's resident advisor there continued to provide technical assistance to develop the internal affairs unit within the Ministry of Finance, and criminal investigation units in the Customs and Tax Administrations. OTA continued to work with counterparts in the Ministry of Finance towards the development of these units; the identification, vetting, and training of personnel; and the provision of workplaces. Each of these units has made significant progress in identifying and investigating matters under its jurisdiction.

In Central America and the Caribbean, OTA provided assistance and mentoring to the tax and customs investigation units recently established in Guatemala and Honduras, and to the tax investigation unit in El Salvador. This assistance focused on developing policy, procedures, and administrative and operational manuals; on developing capacity within each unit to conduct investigations; and on implementing case management systems. In Haiti, technical assistance was initiated to develop a financial crimes unit and train its personnel, in addition to training prosecutors and judges. In Montserrat, assistance was provided to the Financial Services Commission to develop and deliver a one-day training seminar on AML/CTF.

In Mexico, technical assistance was initiated to build AML capacity, including enhancing exchanges of information with Mexico's Financial Intelligence Unit, and training in data analysis and forensic accounting for the Unit's analysts.

Treaties and Agreements

Treaties

Mutual Legal Assistance Treaties (MLATs) allow generally for the exchange of evidence and information in criminal and ancillary matters. In money laundering cases, they can be extremely useful as a means of obtaining banking and other financial records from our treaty partners. MLATs, which are negotiated by the Department of State in cooperation with the Department of Justice to facilitate

cooperation in criminal matters, including money laundering and asset forfeiture, are in force with the following countries: Antigua and Barbuda, Argentina, Australia, Austria, the Bahamas, Barbados, Belgium, Belize, Brazil, Canada, Cyprus, Czech Republic, Dominica, Egypt, Estonia, France, Grenada, Greece, Hong Kong (SAR), Hungary, India, Israel, Italy, Jamaica, Latvia, Liechtenstein, Lithuania, Luxembourg, Mexico, Morocco, the Netherlands, the Netherlands with respect to its Caribbean overseas territories (Aruba and the Netherlands Antilles), Nigeria, Panama, the Philippines, Poland, Romania, Russia, South Africa, South Korea, Spain, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Switzerland, Thailand, Trinidad and Tobago, Turkey, Ukraine, the United Kingdom, the United Kingdom with respect to its Caribbean overseas territories (Anguilla, the British Virgin Islands, the Cayman Islands, Montserrat, and the Turks and Caicos Islands), and Uruguay. MLATs have been signed by the United States, but not yet brought into force, with the European Union and the following countries: Colombia, Ireland, Japan, Sweden, and Venezuela. The United States has also signed and ratified the Inter-American Convention on Mutual Legal Assistance of the Organization of American States and the United Nations Convention against Corruption. The United States is actively engaged in negotiating additional MLATs with countries around the world. The United States has also signed executive agreements for cooperation in criminal matters with the Peoples Republic of China (PRC).

Agreements

In addition to MLATs, the United States has entered into executive agreements on forfeiture cooperation, including: (1) an agreement with the United Kingdom providing for forfeiture assistance and asset sharing in narcotics cases; (2) a forfeiture cooperation and asset sharing agreement with the Kingdom of the Netherlands; and (3) a drug forfeiture agreement with Singapore. The United States has asset sharing agreements with Canada, the Cayman Islands (which was extended to Anguilla, British Virgin Islands, Montserrat, and the Turks and Caicos Islands), Colombia, Ecuador, Jamaica, and Mexico.

Treasury's Financial Crimes Enforcement Network (FinCEN) has a Memorandum of Understanding (MOU) or an exchange of letters in place with other financial intelligence units (FIUs) to facilitate the exchange of information between FinCEN and the respective country's FIU. FinCEN has an MOU or an exchange of letters with the FIUs in Argentina, Aruba, Australia, Belgium, Canada, Cayman Islands, Chile, Cyprus, France, Guatemala, Italy, Japan, Macedonia, Malaysia, Mexico, the Netherlands, Netherlands Antilles, Panama, Paraguay, Philippines, Poland, Romania, Russia, Singapore, Slovenia, South Korea, Spain, and the United Kingdom.

Asset Sharing

Pursuant to the provisions of U.S. law, including 18 U.S.C. § 981(i), 21 U.S.C. § 881(e)(1)(E), and 31 U.S.C. § 9703(h)(2), the Departments of Justice, State, and Treasury have aggressively sought to encourage foreign governments to cooperate in joint investigations of narcotics trafficking and money laundering, offering the possibility of sharing in forfeited assets. A parallel goal has been to encourage spending of these assets to improve narcotics-related law enforcement. The long-term goal has been to encourage governments to improve asset forfeiture laws and procedures so they will be able to conduct investigations and prosecutions of narcotics trafficking and money laundering, which include asset forfeiture. The United States and its partners in the G-8 are currently pursuing a program to strengthen asset forfeiture and sharing regimes. To date, Canada, Cayman Islands, Hong Kong, Jersey, Liechtenstein, Luxembourg, Switzerland, and the United Kingdom have shared forfeited assets with the United States.

From 1989 through December 2007, the international asset sharing program, administered by the Department of Justice, shared $229,080,004.79 with foreign governments that cooperated and assisted

in the investigations. In 2007, the Department of Justice transferred $595,539.76 in forfeited proceeds to Canada ($34,513.42), the Cayman Islands ($49,690.09), Germany ($11,336.25) and Honduras ($500,000.00). Prior recipients of shared assets include: Anguilla, Antigua and Barbuda, Argentina, the Bahamas, Barbados, British Virgin Islands, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, Egypt, Greece, Guatemala, Guernsey, Hong Kong (SAR), Hungary, Indonesia, Isle of Man, Israel, Jordan, Liechtenstein, Luxembourg, Netherlands Antilles, Paraguay, Peru, Romania, South Africa, Switzerland, Thailand, Turkey, the United Kingdom, and Venezuela.

From Fiscal Year (FY) 1994 through FY 2007, the international asset-sharing program administered by the Department of Treasury shared $27,807,012.00 with foreign governments that cooperated and assisted in successful forfeiture investigations. In FY 2007, the Department of Treasury transferred $313,085.00 in forfeited proceeds to Canada ($99,872), China ($10,200), Guernsey ($9,865), and the Isle of Man ($193,148). Prior recipients of shared assets include: Aruba, Australia, the Bahamas, Cayman Islands, Canada, China, Dominican Republic, Egypt, Guernsey, Honduras, Isle of Man, Jersey, Mexico, Netherlands, Nicaragua, Panama, Portugal, Qatar, St. Vincent & the Grenadines, Switzerland, and the United Kingdom.

Multi-Lateral Organizations & Programs

The Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRBs)

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF was created in 1989 and works to generate legislative and regulatory reforms in these areas. The FATF currently has 34 members, comprised of 32 member countries and territories and two regional organizations, as follows: Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, the Peoples Republic of China, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, the United States, the European Commission, and the Gulf Cooperation Council. The FATF admitted the People's Republic of China in June 2007.

There are also a number of FATF-style regional bodies that, in conjunction with the FATF, constitute an affiliated global network to combat money laundering and the financing of terrorism.

The Asia Pacific Group (APG) was officially established in February 1997 at the Fourth (and last) Asia/Pacific Money Laundering Symposium in Bangkok as an autonomous regional anti-money laundering body. The 36 APG members are as follows: Afghanistan, Australia, Bangladesh, Brunei Darussalam, Burma, Cambodia, Canada Chinese Taipei, Cook Islands, Fiji, Hong Kong, India, Indonesia, Japan, Laos, Macau Malaysia, Marshall Islands, Mongolia, Nauru, Nepal, New Zealand, Niue, Pakistan, Republic of Korea, Palau, Philippines, Samoa, Singapore, Solomon Islands, Sri Lanka, Thailand, Tonga, United States, Vietnam, and Vanuatu. Laos became a member at the APG July 2007 plenary in Perth, Australia.

The Caribbean Financial Action Task Force (CFATF) was established in 1992. CFATF has thirty members: Anguilla, Antigua & Barbuda, Aruba, The Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Costa Rica, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Montserrat, Netherlands Antilles, Nicaragua, Panama,

St. Kitts & Nevis, St. Lucia, St. Vincent & the Grenadines, Suriname, Trinidad & Tobago, Turks & Caicos Islands, and Venezuela.

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) was established in 1997 under the acronym PC-R-EV. MONEYVAL is comprised of twenty-eight permanent members; two temporary, rotating members; and one active observer. The permanent members are Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia, Hungary, Latvia, Liechtenstein, Lithuania, Moldova, Malta, Monaco, Montenegro, Poland, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, the Former Yugoslav Republic of Macedonia, and Ukraine. The active observer is Israel. Temporary members, designated by the FATF for a two-year membership, are France and the Netherlands.

The Eastern and South African Anti Money Laundering Group (ESAAMLG) was established in 1999. Fourteen countries comprise its membership: Botswana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Uganda, Zambia, and Zimbabwe.

The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) was established on October 6, 2004 and has seven members: Belarus, China, Kazakhstan, Kyrgyzstan, the Russian Federation, Uzbekistan, and Tajikistan.

The Financial Action Task Force on Money Laundering in South America (GAFISUD) was formally established on December 8, 2000. GAFISUD has ten member states: Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Mexico, Paraguay, Peru, and Uruguay.

The Groupe Inter-gouvernemental d'Action contre le Blanchiment en Afrique (GIABA) consists of 15 countries: Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea Bissau, Guinea Conakry, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo.

The Middle East and North Africa Financial Action Task Force (MENAFATF) consists of 16 members: Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Mauritania, Morocco, Oman, Qatar, Saudi Arabia, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen.

The Egmont Group of Financial Intelligence Units

The Egmont Group began in 1995 as a collection of a small handful of entities, today referred to as financial intelligence units (FIUs), seeking to explore ways of cooperation among themselves. The FIU concept has grown over the years and is now an important component of the international community's approach to combating money laundering and terrorist financing. To meet the standards of Egmont membership, an FIU must be a centralized unit within a nation or jurisdiction to detect criminal financial activity and ensure adherence to laws against financial crimes, including terrorist financing and money laundering. Since its inception in 1995, the Egmont Group has grown dramatically from 14 units to a recognized membership of 106 FIUs. The Egmont Group now has passed its first decade, and it is evolving toward a structure of independent units working closely together to strengthen not only their own countries' AML/CTF regime, but to strengthen the global firewall of economic resistance to money launderers and terrorist financiers.

The Egmont Group is an international network designed to improve interaction among FIUs in the areas of communications, information sharing, and training coordination. The goal of the Egmont Group is to provide a forum for FIUs around the world to improve support to their respective governments in the fight against money laundering, terrorist financing, and other financial crimes. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel employed by such organizations, and fostering better

and more secure communication among FIUs through the application of technology. The Egmont Group's secure Internet system permits members to communicate with one another via secure e-mail, requesting and sharing case information as well as posting and assessing information on typologies, analytical tools and technological developments. FinCEN, on behalf of the Egmont Group, maintains the Egmont Secure Web (ESW). Currently, there are 104 Egmont FIUs connected to the ESW.

The Egmont Group is organizationally structured to meet the challenges of the volume of membership and its workload. The Egmont Committee, a group of 14 members, is an intermediary group between the 106 Heads of member FIUs and the five Egmont Working Groups. This Committee addresses the administrative and operational issues facing Egmont and is comprised of seven permanent members and seven regional representatives based on continental groupings (i.e., Asia, Europe, the Americas, Africa and Oceania). In addition to the Committee, there are five Working Groups: Legal, Operational, Training, Information Technology, and Outreach. The Legal Working Group reviews the candidacy of potential members and handles all legal aspects and matters of principle within the Egmont Group. The Training Working Group looks at ways to communicate more effectively, identifies training opportunities for FIU personnel and examines new software applications that might facilitate analytical work. The Outreach Working Group concentrates on expanding and developing the FIU global network by identifying countries that have established or are establishing FIUs. Outreach is responsible for making initial contact with potential candidate FIUs, and conducts assessments to determine if an FIU is ready for Egmont membership. The Operational Working Group is designed to foster increased cooperation among the operational divisions of the member FIUs and coordinate the development of studies and typologies-using data collected by the FIUs-on a variety of subjects useful to law enforcement. The Information Technology (IT) Working Group promotes collaboration and information sharing on IT matters among the Egmont membership, in particular looking to increase the efficiency in the allocation of resources and technical assistance regarding IT systems. The Committee and the Working Groups meet at a minimum three times per year, including the annual plenary session.

To meet an ever-growing demand in terms of volume and complexity, the Egmont Group has established a Secretariat office. With Egmont's input and expertise in increasing demand by other players on the global stage, the creation of the Secretariat will allow for consistent and active collaboration with other international organizations, and will help to ensure that Egmont preserves its reputation in both the public and private sectors by emphasizing the importance of meeting and maintaining uniform standards of quality by all FIUs. The new Egmont Secretariat is now established in Toronto, Canada, with an initial staff of four.

As of June 2007, the 106 members of the Egmont Group are Albania, Andorra, Anguilla, Antigua and Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Bahamas, Bahrain, Barbados, Belarus, Belgium, Belize, Bermuda, Bolivia, Bosnia and Herzegovina, Brazil, British Virgin Islands, Bulgaria, Canada, Cayman Islands, Chile, Colombia, Cook Islands, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominica, Egypt, El Salvador, Estonia, Finland, France, Georgia, Germany, Gibraltar, Greece, Grenada, Guatemala, Guernsey, Honduras, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Latvia, Lebanon, Liechtenstein, Lithuania, Luxembourg, Macedonia, Malaysia, Malta, Marshall Islands, Mauritius, Mexico, Monaco, Montenegro, Netherlands, Netherlands Antilles, New Zealand, Nigeria, Niue, Norway, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, San Marino, Serbia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, St. Kitts & Nevis, St. Vincent & the Grenadines, Sweden, Switzerland, Syria, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Vanuatu, and Venezuela.

The Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering

The Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) is responsible for combating illicit drugs and related crimes, including money laundering. In 2007, CICAD continued to successfully carry out its anti-money laundering and counter-terrorist financing activities throughout Latin America. CICAD's training programs on combating money laundering and terrorist financing have improved and enhanced the knowledge and capabilities of judges, prosecutors, public defenders, law enforcement agents, and financial intelligence unit (FIU) analysts. The Department of State Bureau of International Narcotics and Law Enforcement provided full or partial funding for many of the CICAD training programs conducted in 2007.

CICAD's Group of Experts to Control Money Laundering met twice this year, in Washington, DC, in April, and Santiago, Chile, in November. The first meeting was held only for the Forfeiture and International Cooperation sub-groups to discuss specific themes in these areas. The second meeting focused on the new project in asset forfeiture, which was initiated in October. This project aims at offering technical assistance to OAS member states that are interested in developing and improving their abilities to administer forfeited assets.

In 2007, CICAD also introduced several new programs. CICAD is developing a database, which will catalogue and update information on money laundering and terrorist financing typologies to assist member countries in detecting money laundering, gathering intelligence, conducting investigations, and prosecuting such cases. The database developed through this project will allow authorized users to search for cases similar to those they are currently investigating, to look for patterns, and to have-with the use of the database-the necessary tools to investigate these cases. This Internet-based database will be the first of its kind in this field. In addition, the coherent use of the database in member states' investigations will help facilitate the exchange and sharing of information amongst the specialists who deal with money laundering and terrorist financing.

Training and Technical Assistance

Mock trials were held in 2007 in Bolivia, Honduras, Mexico, and Peru. These trials were conducted with the participation of the United Nations Office on Drugs and Crime (UNODC), and provided training based on money laundering cases to specialists in these specific countries. This program focuses on the resolution of a real money laundering case, during which judges, prosecutors, public defenders, FIU analysts, and the police work together by preparing the given case for trial. In addition to the trials, workshops for judges and prosecutors were carried out in Peru and Mexico, as introductory events for the mock trials.

In a joint initiative with the Inter-American Committee against Terrorism (CICTE), CICAD's Anti-Money Laundering Unit organized two workshops on terrorist financing. The first event was conducted in Bogota, Colombia, and the participating countries' FIUs, police, and prosecutors' office each provided three participants. The beneficiaries of this workshop included Central American countries, Mexico, and the Dominican Republic. Due to the outstanding results obtained with the first event, a second workshop on terrorist financing was held in August in Lima, Peru. The second program's objective was to train specialists from South America.

The events that were held in Peru (the mock trials, the workshop for judges and prosecutors, and the workshop on terrorist financing) took place thanks to a joint initiative with the U.S. Embassy's Narcotics Affairs Section. The NAS helped organize and coordinate these programs. As an outcome of

the success of the three events, the Banking Superintendent of Peru offered the Anti-Money Laundering Unit the use of a building, at no cost, for CICAD's regional training center.

A mock investigation was also held in 2007 with the assistance of the Government of Spain and the participation of UNODC. The event focused on the investigation of a money laundering case and took place in Antigua, Guatemala. The objective of the project was strengthening the cooperation between law enforcement agents, prosecutors, and FIU analysts during case investigations. Participating countries included Bolivia, Costa Rica, El Salvador, Guatemala, Honduras, Panama, Mexico, and Venezuela.

In cooperation with Spain's University of Salamanca, CICAD will offer an online degree in money laundering to law enforcement agents, prosecutors, judges, FIU analysts, and bankers. The signature of the agreement held between CICAD and the University of Salamanca occurred in October in Washington, DC. This project will be conducted by prestigious Spanish experts on money laundering, and will be taught in three modules, at the basic, intermediary, and advanced levels.

CICAD acquired computer hardware and projectors as a follow-up to the train-the-trainers program. CICAD purchased three laptops and three projectors for El Salvador, Costa Rica, and Honduras this year to advance the program in each of these countries.

CICAD also facilitated bilateral cooperation between prosecutors in Peru and Colombia in 2007. As a result of the expertise Colombia has in extinción de dominio (extinction of dominion over assets), two Colombian prosecutors with ample experience in this area participated in an anti-money laundering workshop in Peru in September and shared their experiences and views in this field with the local specialists.

Pacific Anti-Money Laundering Program (PALP)

The Pacific Anti-Money Laundering Program (PALP) was launched in September 2006 under the Pacific Islands Forum Secretariat (PIFS) in Fiji. PALP is a joint initiative between the PIFS, the United Nations Office on Drugs and Crime (UNODC), and the United States Department of State, which designed and funds the PALP. The PALP is a four-year regional technical assistance and training program designed to assist the 14 members of the Pacific Islands Forum that are not also members of the Financial Action Task Force (FATF) in establishing, enhancing, and implementing their anti-money laundering and counter-terrorist financing (AML/CTF) regimes. The 14 members of the Pacific Islands Forum that receive PALP assistance are the Cook Islands, the Federated States of Micronesia, Fiji, Kiribati, the Marshall Islands, Nauru, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu.

The goal of PALP training and technical assistance is to assist participating jurisdictions in complying with international standards of the FATF and relevant United Nations Conventions and Security Council Resolutions. The PALP is essentially an outreach program, utilizing mentors based in host countries to assist with legal, law enforcement, regulatory, and financial intelligence unit (FIU) development throughout the region. In 2007, the PALP provided assistance on a wide range of AML/CTF issues, including legislative drafting, capacity building, case support, and preparation for and follow-up to mutual evaluations.

Mentoring

The PALP uses resident and intermittent mentors to deliver regional and bilateral training in all elements required to establish viable AML/CTF regimes. The PALP currently has mentors in the legal and law enforcement fields based in Tonga and Vanuatu respectively, as well as an intermittent mentor for FIUs. In 2008, a second law enforcement mentor will be based in Palau and a regulatory mentor is

expected to be based in Samoa. Although the PALP mentors are based in their host countries, they are able to respond to requests for assistance from any of 14 participating countries and travel to those jurisdictions for periods of up to one month at a time.

The PALP mentoring program involves a number of different elements. Due to their experience, PALP mentors are able to adapt international standards to local situations. PALP mentors provide on-the-job training and work alongside local officials to ensure that they have sufficient capacity to implement the member country's AML/CTF regime. Unlike consultants, the PALP mentors will stay in-country for as long as four to six weeks at any given time. The amount of time spent in-country also offers a useful opportunity for the mentors to assess the situation on the ground with regard to AML/CTF issues, and compliance with international standards, as well as to determine areas where further work is needed. The ability of PALP mentors to respond quickly to urgent requests from jurisdictions in the region has made PALP's assistance highly sought after.

Throughout 2007, PALP engaged intermittent FIU mentors to conduct reviews in the Marshall Islands, Palau, Tonga, and Vanuatu. These reviews were conducted in preparation for upcoming mutual evaluations, and/or to gauge compliance with international standards. Follow-up action plans are being developed to implement the recommendations derived from these reviews. Because many of these countries do not have sufficient resources to implement the recommendations on their own, a more vigorous follow-up approach has been adopted by the PALP that includes the identification of resources to ensure effective follow-up and implementation of the recommendations derived from the FIU reviews.

Part of the PALP strategy aimed at building national capacity in AML/CTF matters entails efforts to strengthen the role of national AML/CTF committees at the policy level. In 2007, the PALP mentors played vital roles in providing support and advice to the national AML/CTF committees of several jurisdictions in the region, including Fiji, Palau, and Vanuatu.

Legislative Drafting

Through the work of the PALP legal mentor, the PALP has assisted the Cook Islands, Palau, the Republic of the Marshall Islands, Tonga, and Vanuatu in assessing and enhancing their AML/CTF regimes, and drafting the necessary legislation to bring these regimes into greater compliance with international standards.

In 2007, the PALP provided a range of legislative assistance to the Cook Islands to improve the effectiveness of its AML/CTF laws. The PALP legal mentor reviewed the Cook Islands current AML legislation, the Proceeds of Crime Act (POCA) and the Financial Transaction Reporting Act (FTRA), in October 2007. As a result of the review, the PALP assisted the Cook Islands in developing draft legislation regarding the FIU, civil forfeiture, and cross-border currency declarations. Although the FIU of the Cook Islands has been operating since 2001, its authority was limited. The draft Financial Intelligence Unit Act will provide it with broader powers, including the ability to conduct investigations and supervision of financial institutions. The draft civil forfeiture legislation will provide additional options for Cook Islands authorities to confiscate assets beyond the provisions of the POCA. The draft currency declaration bill will assist the Cook Islands in combating currency smuggling, which is a growing problem. The PALP mentor also assisted in drafting amendments to the POCA, FTRA, and the Terrorism Act.

Following a review of Palau's AML/CTF regime, the PALP legal mentor drafted amendments to the Money Laundering and Proceeds of Crime Act. The amendments are aimed at enhancing the effectiveness of AML/CTF prosecutions. The PALP mentor also developed a draft civil forfeiture law, which, when passed, will also allow the Government of Palau to confiscate or forfeit assets independent of criminal proceedings. In addition, the PALP mentor developed regulations aimed at

tightening the regulation of banks to prevent money laundering and fraud. The lack of such measures was highlighted following the collapse of a local bank in December 2006, resulting in the loss of approximately $40 million in stolen funds (equivalent to 40 percent of all bank deposits in Palau).

In December 2007, the President of Palau signed into law some of the amendments to the Money Laundering and Proceeds of Crime Act. It is expected that the other pieces of legislation developed by PALP will be approved in 2008. The PALP legal mentor has had several sessions with members of the Palau Senate and the House of Representatives in 2007 on the importance of enacting the AML/CTF legislation.

PALP legislative assistance to the Marshall Islands in 2007 consisted of drafting regulations for financial institutions and a currency declaration bill, as well as amendments to the Terrorism Act, Banking Act, and Proceeds of Crime Act. The amendments to the Terrorism Act helped avert the threat of membership sanctions by the Egmont Group. As is the case in other Pacific jurisdictions, cash smuggling has become an increasing problem and the draft Border Currency Reporting Act is designed to deal with this. The Oceania Customs Organization (OCO) is considering using the draft Border Currency Reporting Act as model legislation for the region.

In Tonga, the PALP legal mentor provided legislative assistance by drafting amendments to the Money Laundering and Proceeds of Crime Act 2000 (MLPCA), a currency declaration bill, and an FIU bill. The amendments to the MLPCA will include serious offenses designated by the FATF 40 Recommendations as predicate offenses for money laundering. The currency declaration bill, when passed, will assist in detecting bulk cash smuggling. The FIU bill will provide the Tongan FIU with more extensive powers to investigate suspicious transaction reports received from financial institutions.

Following a review of Vanuatu's AML/CTF regime, the PALP mentor developed draft regulations for financial institutions, as well as amendments to Proceeds of Crime Act on cross-border currency reporting. The draft regulations will provide a legal framework for Vanuatu's FIU to develop guidelines for financial institutions. The draft provisions on cross-border reporting will enhance the capacity of Vanuatu authorities to respond more effectively to currency smuggling.

Capacity Building Initiatives

The PALP provides technical assistance and training workshops at the regional, sub-regional, and national levels for law enforcement and customs officials, prosecutors, judges, and regulatory authorities. In 2007, the PALP conducted several capacity building training initiatives at both the regional and national levels. Approximately 310 individuals from all 14 jurisdictions received capacity building assistance from the PALP.

On May 9-12, 2007, the PALP hosted a judicial workshop on money laundering, and terrorist financing in Palau. Eleven judges from the Marshall Islands, Micronesia, Palau, Papua New Guinea, Solomon Islands, and Tuvalu participated in this training. The workshop was jointly funded by PALP and Australia's Anti-Money Laundering Assistance Team (AMLAT), although the training itself was conducted by PALP. The Chief Justice of Tuvalu, acting as the President of the Fiji Court of Appeals in August, 2007, later praised this training program for helping with his judgment in upholding the Fiji High Court's conviction of an Australian national who was running an advanced fee scheme. This was Fiji's first money laundering conviction

The PALP hosted a regional workshop for AML/CTF investigators in Samoa on July 9-13, 2007. Thirty-five law enforcement officials from Cook Islands, Fiji, Kiribati, Micronesia, Niue, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu attended the training. The workshop was jointly funded and conducted by the PALP and AMLAT.

On September 27-28, 2007, the PALP hosted a national workshop on civil forfeiture for 19 prosecutors and law enforcement officials from Fiji. The objective of the workshop was to assist prosecutors and law enforcement in the use and application of the new civil forfeiture provisions. The workshop was funded by PALP and conducted jointly by the PALP and judges from the Fiji High Court.

The PALP hosted a regional workshop for supervisors and regulators of nonbank financial institutions in Vanuatu, December 3-7, 2007. A total of 26 supervisors and regulators from nine countries attended the workshop, including the Cook Islands, Fiji, Micronesia, Marshall Islands, Niue, Papua New Guinea, Samoa, Solomon Islands, and Vanuatu. The workshop examined the challenges faced by supervisors and regulators in ensuring compliance with AML/CTF regulations by nonbank entities, such as lawyers, accountants, insurance companies, real estate agents, trust companies, and service providers. This workshop was the first of its kind undertaken by the PALP and highlighted the need for follow-up work in 2008. The workshop was jointly funded by PALP and the Commonwealth Secretariat, and the training was conducted by the PALP, the International Monetary Fund, Australia's FIU, and private sector experts from the Cook Islands.

In December 2007, the PALP conducted training on cross-border currency reporting in Fiji. Six countries attended this training, including Fiji, Kiribati, Nauru, Solomon Islands, Tuvalu, and Vanuatu. Approximately 210 staff from Fiji Customs and Airport Authority, Police, and the Immigration and Quarantine agency, as well as officials from the other participating countries, attended the training. A key outcome of this training was the development of a tool kit, which establishes procedures and policies for customs and other border officials regarding the detection and seizure of unreported cross-border cash movements. The tool kit was developed by the three agencies for Fiji, and is now being considered for use by other jurisdictions. The training was conducted jointly by PALP, AMLAT, and the OCO, with funding from AMLAT.

Case support

One of the key areas of the PALP's work is case support for jurisdictions in the region on high-profile money laundering and terrorist financing cases. In 2007, the PALP provided case support to the Cook Islands, Palau, and Tonga.

The Government of Palau requested PALP assistance in the investigation of money laundering and fraud offences emanating from the collapse of a local bank, which affected 40 percent of all depositors in Palau. The case highlighted the lack of effective internal controls, regulations, or legislation, as well as a lack of investigative capacity to deal with such a large case. The key contribution made by the PALP was the instigation of criminal charges, which had not been considered by the Palau authorities at the start of the investigation. In addition, the PALP developed an investigative strategy for the criminal investigation, which was accepted by the Special Prosecutor in charge of the case and now forms the basis of the investigation. The PALP law enforcement mentor continues to provide advice and investigative support to the Special Prosecutor, and the legal mentor has also provided advice to the Special Prosecutor. The PALP also assisted the United States Internal Revenue Service in its own criminal investigation into the bank by providing information about the defendants and assisting with mutual legal assistance requests to New Zealand. In early 2008, PALP's second law enforcement mentor will be based in Palau.

Since June 2007, the PALP has provided legal and investigative advice to the Cook Islands FIU, the Financial Supervisory Commission, and the Cook Islands Police on a money laundering and terrorist financing case involving an international bank. As in Palau, the PALP assisted the FIU and the Police in developing an investigative strategy. The case potentially involves seven other jurisdictions, and several mutual legal assistance requests have been presented to India, New Zealand, and Pakistan with the assistance and advice of the PALP. The PALP law enforcement contacts in some of these countries

have also provided useful information and assistance to law enforcement officials in the Cook Islands. The information obtained from these mutual legal assistance requests has helped the Cook Islands Police and FIU to make headway in their investigations. The authorities now believe that they have sufficient information to shut down an international bank that is registered in the Cook Islands and believed to be involved in money laundering and providing financial support for terrorism. This is the first time the Cook Islands Police and FIU have dealt with a high profile case

In 2007, the PALP legal mentor responded to a request from Tongan authorities regarding the theft of precursor chemicals that were believed to be used for the manufacture of methamphetamine. The advice provided by the legal mentor included opinions on the use of the Tongan legislation and the appropriate charges to be filed.

Mutual evaluations

The PALP has also extended its assistance to jurisdictions when preparing for mutual evaluations or when implementing reforms suggested by the mutual evaluation team. The goal of the assistance provided by the PALP is to ensure that the jurisdiction is prepared for the mutual evaluation process and that, to the greatest extent possible, their AML/CTF regimes comport with international standards. The review of their AML/CTF regimes by the PALP helps these countries to take stock of where they are in terms of compliance with international standards, and to identify areas where technical assistance may be required. Furthermore, the reviews undertaken by the PALP are an important preparatory step as the jurisdictions prepare themselves for mutual evaluations by the Asia Pacific Group (APG), World Bank, or International Monetary Fund (IMF). In 2007, the PALP provided assistance to Palau and Tonga in preparation for their upcoming mutual evaluations. The PALP also assisted Fiji in implementing recommendations made by the evaluation team as a result of their mutual evaluation in 2006.

In Palau, the PALP reviewed its Money Laundering and Proceeds of Crime Act, assisted officials with the completion of the mutual evaluation questionnaire, and carried out a review of Palau's FIU in November 2007. Palau will undergo a mutual evaluation by the IMF in February 2008.

PALP's legal mentor provided assistance to the government of Tonga's review of its Money Laundering and Proceeds of Crime Act 2001. A review of Tonga's FIU was conducted in March 2007 by a PALP intermittent mentor. The mutual evaluation of Tonga will occur in 2008.

In the Cook Islands, the PALP reviewed their existing AML/CTF legislation and developed several draft laws, including FIU, civil forfeiture and currency declaration bills. The passage of this legislation would place the Cook Islands in a greater level of compliance with international standards. The Cook Islands will be evaluated in the third quarter of 2008.

Following its mutual evaluation, the PALP assisted Fiji in implementing the recommendations made in the 2006 World Bank mutual evaluation report. The PALP provided legal advice to the Fiji's FIU as to how the FIU-related recommendations could best be implemented. A national workshop will be held for Fiji officials in March 2008 on developing a risk-based approach to combating money laundering and terrorist financing.

United Nations Global Programme Against Money Laundering

The United Nations is one of the most experienced global providers of anti-money laundering (AML) training and technical assistance and, since 9-11, counter-terrorist financing (CTF) training and technical assistance. The United Nations Global Program against Money Laundering (GPML), part of

the United Nations Office on Drugs and Crime (UNODC), was established in 1997 to assist Member States to comply with the UN Conventions and other instruments that deal with money laundering and terrorist financing. These now include the United Nations Convention against Traffic in Narcotic Drugs and Psychotropic Substances (the 1988 Vienna Convention), the United Nations International Convention for the Suppression of the Financing of Terrorism (the 1999 Convention), the United Nations Convention against Transnational Organized Crime (the 2000 Palermo Convention), and the United Nations Convention against Corruption (the 2003 Merida Convention).

In September 2006, the UN General Assembly adopted the United Nations Global Counter-Terrorism Strategy. The Plan of Action contained in the Strategy encourages UNODC to help countries comply with international norms and standards, and to enhance international cooperation in these areas. GPML is the focal point for anti-money laundering policy and activities within the UN System and a key player in strengthening efforts to counter the financing of terrorism. GPML provides technical assistance and training in the development of related legislation, infrastructure and skills, directly assisting member states in the detection, seizure, and confiscation of illicit proceeds. Since 2001, GPML's technical assistance work on countering the financing of terrorism has also received priority. As part of the implementation of the UN Global Counter-Terrorism Strategy, GPML is one of the lead entities of the working group of the UN Counter-Terrorism Implementation Task Force (CTITF), an information-sharing and coordinating body aimed at developing policy recommendations in tackling the financing of terrorism. GPML now incorporates a focus on counterterrorist financing in all its technical assistance work.

In 2007, GPML provided training and long-term assistance in the development of viable AML/CTF regimes to more than fifty countries. In September 2007, UNODC and the World Bank launched the Stolen Asset Recovery (StAR) Initiative aimed at assisting developing countries to recover stolen assets that have been sent abroad by corrupt leaders. Given the close links between money laundering and corruption, and the fact that building an anti-money laundering system forms an integral part of good governance policy and asset recovery strategy, GPML is actively involved in this initiative and in the implementation of the UN Convention against Corruption, in force since December 2005.

The Mentoring Program

GPML's Mentor Program is one of the most successful and well-known activities of international AML/CTF technical assistance and training, and is increasingly serving as a model for other organizations' initiatives. It is one of the core activities of the GPML technical assistance program and is highly regarded by the AML/CTF community. GPML's Mentor Program has key advantages over more traditional forms of technical assistance. First, mentors serve as residential advisors in a country or region for as long as one to four years, and offer sustained skills and knowledge transfer. Second, mentoring constitutes a unique form of flexible, ongoing needs assessment, where the mentor can pinpoint specific needs over a period of months, and adjust his/her work plan to target assistance that responds to those needs. Third, the member state has access to an "on-call" resource to provide advice on real cases and problems as they arise. Fourth, a mentor can facilitate access to foreign counterparts for international cooperation and mutual legal assistance at the operational level by using his/her contacts to act as a bridge to the international community.

The GPML Mentoring Program provides targeted on-the-job training that adapts international standards to specific local/national situations, rather than the traditional training seminar. The concept originated in response to repeated requests from member states for longer-term international assistance in this technically demanding and rapidly evolving field. GPML provides experienced prosecutors and law enforcement personnel who work side-by-side with their counterparts in a target country for several months at a time on daily operational matters to help develop capacity. Some advise governments on legislation and policy, while others focus on operating procedures, either with law

enforcement or with issues relating to a country's financial intelligence unit (FIU). By giving in-depth support upon request, the mentors have gained the confidence of the recipient institutions, which enables the achievement of concrete and significant outputs. In many countries, GPML mentors are the only locally placed AML/CTF experts, hence they are heavily relied upon by local offices of donor countries and organizations for advice in the process of creation and delivery of other donor AML/CTF projects. The GPML prosecutorial mentor based in the Prosecutor General's Office of Namibia provides assistance for the development of asset forfeiture mechanisms in Botswana, Namibia, Zambia, and Zimbabwe. The mentor provided legal inputs to amend relevant legislation in each country, specifically the Financial Intelligence Act of Namibia, which was passed in June 2007, and initiated and monitored the Prosecutor Placement Program, an initiative aimed at placing prosecutors from the region for a certain period of time within the Asset Forfeiture Unit of the National Prosecuting Authority (NPA) in South Africa.

The UN mentor based in Tanzania with the Secretariat of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) delivered training to 14 member countries and assisted the ESAAMLG Secretariat in conducting its two mutual evaluations in 2007 and one on-site visit. The mentor completed his term at the end of December 2007. Under the monitoring of the UN mentor, GPML developed in 2007 a "train the trainers" course, which is an ongoing certification program on financial investigation in Namibia. In collaboration with the U.S. Department of State and the World Bank, GPML extended the appointment of the regional mentor for Central Asia in Almaty, Kazakhstan, focusing on legislative assistance and FIU development, as well as an AML/CTF mentor in Hanoi, Vietnam, to provide assistance to Vietnam, Lao PDR, and Cambodia to establish comprehensive AML/CTF regimes, including the establishment and enhancement of FIUs. In addition, GPML assisted in legislative drafting for many other countries, including Yemen, Djibouti, and member countries of the West African Economic and Monetary Union, and implemented a comprehensive "train the trainers" program for FIU, law enforcement agencies and prosecutors in Armenia, as well as an FIU development project in Kyrgyzstan. Both initiatives are ongoing.

Mentoring & Financial Intelligence Units

GPML was among the first technical assistance providers to recognize the importance of countries' creating a financial intelligence capacity, and GPML mentors worked extensively on the development and the implementation phases of FIUs in several countries in the Eastern Caribbean, the Pacific, and most recently in South East Asia. The development of FIUs in the Eastern Caribbean played a key role in the removal of many of the jurisdictions from the FATF Non-Cooperative Countries and Territories (NCCT) list.

A major initiative that could have global implications for many FIUs is the development by the UNODC Information Technology Service (ITS), with substantive inputs from GPML, of an analytical and integrated database and intelligence analysis system for operational deployment in FIUs, called goAML (http://goaml.unodc.org). It is an IT solution for FIUs to manage their activities, particularly data collection, analysis, and dissemination. The goAML program is now operational in Nigeria and several countries have contacted UNODC to explore the feasibility of future IT partnerships with goAML. The system provides a uniform and standard AML platform to fight money laundering and the financing of terrorism and was introduced and praised at the Egmont Group Plenary meeting in June 2007.

Computer-Based Training

Other highlights of GPML's work in 2007 included the ongoing development of its global computer-based training (CBT) initiative. The program provides 12 hours of interactive basic AML training consisting of thirteen modules for global delivery. Delivery continued in the Pacific, Central

American, and Western Africa regions. CBT training classrooms were established in Niamey, Niger, at the financial intelligence unit (CENTIF), two training centers in Morocco (Central Bank and the Royal Institute of Police), one at the Egyptian Banking Institute in Cairo, and one at the Colombian National Police in Bogotá. GPML also installed its mobile CBT training centre throughout West Africa to train key officials of National AML Inter-Ministerial Committees. In 2007, GPML initiated the development of new CBT modules on asset forfeiture.

The training program has flexibility in terms of language, level of expertise, target audience, and theme. Computer-based training is particularly applicable in countries and regions with limited resources and law enforcement skills, as it can be used for a sustained period of time. As an approach, CBT, translated into several languages, lends itself well to GPML's global technical assistance operations.

Other GPML Initiatives

GPML contributed to the delivery of mock trials in Central and South America. This tailor-made activity was developed in response to repeated requests from member states for practical realistic AML training. It combines training and practical aspects of the judicial work into one capacity building exercise. Five mock trials were organized and delivered in 2007 in Bolivia, Honduras, Mexico, Peru, and Venezuela.

GPML assisted West African countries in the development of their AML/CTF national strategies, and developed financial investigations courses in South Asia, Ethiopia, and West Africa in partnership with the Commonwealth Secretariat and the Office of Technical Assistance of the U.S. Department of Treasury (OTA). In 2007, GPML, in a collaborative effort with the International Monetary Fund (IMF), initiated the revision of a model law on AML/CTF and proceeds of crime for common law countries, encompassing worldwide AML/CTF standards and taking into account best legal practices. GPML continued to work closely with partners, including among others the U.S. Department of Justice, OTA, the Organization for Security and Cooperation in Europe (OSCE), the Commonwealth Secretariat, the IMF, and the World Bank to deliver CTF training, particularly in the regions of Central Asia, Southern Europe, and Africa.

GPML administers the Anti-Money Laundering International Database (AMLID) on the International Money Laundering Information Network (IMoLIN), an online, password-restricted, analytical database of national AML/CTF legislation that is available only to public officials. GPML also maintains an online AML/CTF legal library and issues a Central Asia Newsletter monthly in English and quarterly in Russian. IMoLIN (www.imolin.org) is a practical tool in daily use by government officials, law enforcement, and lawyers. GPML manages and constantly updates this database on behalf of the UN and 11 major international partners in the field of AML/CTF: the Asia/Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), the Commonwealth Secretariat, the Council of Europe-MONEYVAL, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the Eurasian Group (EAG), the Financial Action Task Force (FATF), the Financial Action Task Force of South America (GAFISUD), the Inter-Governmental Action Group against Money Laundering and Terrorist Financing in West Africa (GIABA), Interpol, and the Organization of American States (OAS). In July 2007, GPML launched the French language version of IMoLIN. GPML continued its second round of legal analysis using the revised AMLID questionnaire. In this regard, the database currently contains fifty-seven revised questionnaires under the second round of legal analysis. The updated AMLID questionnaire reflects new money laundering trends and standards, and takes provisions related to terrorist financing and other new developments into account, including the revised FATF recommendations.

Law Enforcement Cases

Operation TNT—Contract Fraud

In November 2004, U.S. Immigration and Customs Enforcement (ICE) initiated an investigation based on a Bank Secrecy Act report filed by a financial institution. The investigation identified South Florida companies whose corporate officers and directors were part of an international conspiracy to perpetrate a bid-rigging scheme against the government of Trinidad and Tobago. The scheme involved the awarding of a contract involving the construction of the Piarco International Airport in Trinidad. In one instance, the conspirators used a related company to intentionally submit a higher competitive bid to help them win a multi-million dollar contract to equip the airport in Trinidad with items such as x-ray machines, passenger boarding bridges, and elevators. This was done to give the appearance that the conspirators' bid of $30 million was reasonable by comparison to the $35 million bid that they prepared and submitted on behalf of their supposed competition.

Upon award of the contract, the conspirators laundered the proceeds and paid kickbacks to co-conspirators through an elaborate series of financial transactions executed utilizing offshore shell companies and bank accounts established in the Bahamas and elsewhere. Ultimately, millions of dollars of fraud proceeds were repatriated to the United States and used to purchase items such as artwork, vacations, and jewelry. Additionally, the investigation revealed that some of the conspirators also engaged in a bank fraud scheme that resulted in a loss of approximately $23 million to South Florida financial institutions through default on unsecured loans.

The owner of one of the South Florida companies was recently sentenced to 72 months imprisonment for conspiracy to commit wire and bank fraud. The defendant also agreed to a $22 million restitution order. The Chief Financial Officer of this company was sentenced to four years probation for bank fraud, and was ordered to pay over $400,000 in restitution. Additionally, four co-conspirators were convicted of charges related to bank and/or wire fraud. Sentences ranged from probation to 37 months in prison.

Drug Trafficking Organization—Laundering via Bulk Cash Smuggling and the Purchase of Real Estate and Automobiles

The investigation into the George MARTINEZ Drug Trafficking Organization (DTO) began with a routine traffic stop on November 1, 2000, in West Memphis, Arkansas. A vehicle driven by Marco Gonzalez, a resident of Cudahy, California, was stopped by an officer of the West Memphis Police Department. Following a consent search of the vehicle, officers discovered approximately $854,000 in cash hidden in two false compartments beneath the vehicle. Subsequently, ICE's SAC/Los Angeles office opened an investigation on the seizure based upon Gonzalez's residency in the Los Angeles area and the fact he was driving the cash westbound towards California.

The multi-year wiretap investigation revealed an extensive DTO that laundered its proceeds through the purchase of real estate properties and luxury and vintage vehicles. The MARTINEZ DTO smuggled cocaine and marijuana from Mexico through various ports of entry in California in vehicles purchased from Los Angeles-area automobile auctions. Vehicles were selected for their ability to hold large false compartments beneath the floorboards. The automobiles were outfitted by MARTINEZ DTO drug associates once the vehicles were purchased. The drugs were distributed throughout California, Seattle, Baltimore, New York, Miami, and Canada.

Proceeds from the sale of the narcotics were sent directly to MARTINEZ at his base of operations in Downey, California. Cash was laundered predominantly by MARTINEZ through the purchase of real estate in California; however, MARTINEZ also personally bought numerous luxury and vintage

vehicles in cash. The remainder of the cash was used to improve MARTINEZ' properties and "flip" them for profit in a booming Southern California real estate market. The bulk cash that MARTINEZ did not launder in southern California was driven south into Mexico and laundered through various casas de cambios.

The head of the DTO, along with eight other associates, were arrested; one target is still a fugitive-at-large. The defendants pled to conspiracy to import and distribute controlled substances and received varied sentences. MARTINEZ was the only person who pled to a money laundering charge.

Trade-based Money Laundering/Black Market Exchange

An ICE investigation of an unlicensed money services business (MSB) in Atlanta resulted in the seizure of approximately $714,000 from six bank accounts. The investigation revealed that a black market currency exchanger in Brazil, called a "doleiro," was transferring payments to U.S. bank accounts. The owner of the bank accounts in the U.S. would then facilitate third-party wire transfers to U.S. and Asian exporters for commercial goods that were shipped to the South American Tri-Border area of Argentina, Brazil, and Paraguay. In Brazil, this trade-based money laundering scheme, known as the "paralelo," is designed to avoid high fees and taxes associated with legitimate international wire transactions conducted via the National Bank of Brazil. Criminal organizations utilize trade-based money laundering to transfer value across borders through trade-based transactions (e.g., imports and exports of commercial merchandise) and to disguise the illicit origins of criminal proceeds. ICE analysis and investigation documented the illegal transfer of more than $100 million from the Tri-Border area to the United States that resulted in the subsequent seizure.

Bulk Cash Smuggling, Casas de Cambio, and the Black Market Peso Exchange

In March 2006, in a joint action between the Colombian National Police and the U.S. Drug Enforcement Agency, Ricardo Mauricio Bernal-Palacios, his brother Juan Bernal-Palacios, and Camillo Ortiz-Echeverri were arrested in Bogotá, Colombia. The investigation of the Bernal organization documented amounts in excess of $300 million laundered through the U.S.-based correspondent accounts of Casa de Cambio Ribadeo and another Mexican-based casa de cambio. The international investigation also included the related seizure by the Spanish Guardia Civil of approximately 17 million euros (approximately $20 million), and the seizure of 2,000 kilograms of cocaine.

The investigation specifically targeted Mauricio Bernal's concealed ownership interest in Casa de Cambio Ribadeo in Mexico City, which he used to receive and launder "bulk currency" narcotics proceeds generated in the United States and Europe. Bernal used U.S.-based bank accounts maintained in the name of Casa de Cambio Ribadeo to transfer these proceeds to Colombia or to free trade zones for the purchase of commodities destined for Colombia using the Black Market Peso Exchange.

Recent Terrorist Financing Prosecutions

Terrorist financing prosecutions continue to be a particular focus of the Department of Justice National Security Division's (NSD) Counterterrorism Section. Terrorists cannot carry out their acts without money to buy weapons, explosives and equipment. The NSD's Counterterrorism Section has taken steps to identify and eliminate terrorist financing disguised as charitable giving. Such activity is not protected by the First Amendment; rather, it seeks to pervert and undermine it.

What is at issue here is not anything close to pure speech. It is, rather, material support to foreign organizations that the United States has deemed, through a process defined by federal statute and including judicial review by the D.C. Circuit, a threat to our national security. The fact that the support takes the form of money does not make the support the equivalent of speech. In this context, the

donation of money could properly be viewed by the government as more like the donation of bombs and ammunition than speech.

Terrorists exploit the charitable efforts of others to divert money meant for the poor and disenfranchised. NSD utilizes the traditional investigative tools and techniques used in white collar crime cases to further terrorist financing investigations. These are often difficult cases with unique issues, which frequently involve classified Foreign Intelligence Surveillance Act (FISA) electronic surveillance which extended over a period of years, providing additional challenges in presenting the evidence to the jury.

Holy Land Foundation

Holy Land Foundation. On October 22, 2007, in the Northern District of Texas a mistrial was declared after the jury was unable to reach a verdict in the trial of the leaders of the Holy Land Foundation for Relief & Development (HLF) for providing material support to Hamas, a foreign terrorist organization, and related charges. One of the defendants, Mohammed El-Mezain, was found not guilty on all counts with which he was charged except Count 1, the material support conspiracy count. All other defendants at trial—Shukri Abu Baker, Ghassan Elashi, Mufid Abdulqader, and Abdulraham Odeh—and all counts resulted in a mistrial. The case has been re-assigned for retrial in 2008. HLF received start-up assistance from Mousa Abu Marzook, a leader of Hamas. It was the largest Muslim charity in the United States until it was declared a Specially Designated Terrorist Organization in 2001 and shut down. HLF raised millions of dollars for Hamas over a 13-year period.

Chiquita Brands Pays Terrorist Group AUC

Chiquita Brands International. On March 19, 2007, Chiquita Brands International Inc., a multinational corporation incorporated in New Jersey and headquartered in Cincinnati, Ohio, pled guilty in the District of Columbia to one count of engaging in transactions with a Specially Designated Global Terrorist. Under the terms of the plea agreement, Chiquita was sentenced to a $25 million criminal fine, required to implement and maintain an effective compliance and ethics program, and five years of probation. The plea agreement arose from significant payments that Chiquita made for years to the violent, right-wing terrorist organization United Self-Defense Forces of Colombia (AUC). From 1997 through February 4, 2004, Chiquita paid money to the AUC in two regions of Colombia where Chiquita had fruit operations: Urabá and Santa Marta. Chiquita made these payments through its wholly-owned Colombian subsidiary known as "Banadex." By 2003, Banadex was Chiquita's most profitable operation. Chiquita, through Banadex, paid the AUC nearly every month. In total, Chiquita made over 100 payments to the AUC amounting to over $1.7 million. The U.S. government designated the AUC as a Foreign Terrorist Organization (FTO) on Sept. 10, 2001, and that designation was well-publicized in the American public media. The AUC's designation was even more widely reported in the public media in Colombia, where Chiquita had its substantial banana-producing operations. Chiquita also had specific information about the AUC's designation as an FTO through an Internet-based, password-protected subscription service that Chiquita paid money to receive. Nevertheless, from Sept. 10, 2001, through Feb. 4, 2004, Chiquita made 50 payments to the AUC totaling over $825,000.

Money Laundering to Support Terrorism

Yassin Aref. On October 10, 2006, a jury in the Northern District of New York found Yassin Aref guilty of conspiracy to commit money laundering, conspiracy to provide material support to terrorists, and conspiracy to provide material support to a designated foreign terrorist organization, as well as two counts of money laundering. He was also found guilty of one count of making false statements.

His co-defendant, Mohammed Hossain, was also found guilty, and both defendants were sentenced to 15 years in prison. Aref was initially identified when his name and telephone number were discovered in documents found in 2003 at three separate Ansar-al-Islam locations in Iraq. In addition, investigation disclosed that numerous telephone calls were placed from his home telephone to a telephone number in Damascus, Syria, connected to al Qaeda. The case involved a sting operation in which an FBI informant represented to the defendants that the informant needed to conceal the proceeds of the importation of a surface-to-air missile (SAM). The informant further represented that the SAM was to be used by terrorists in New York City in an operation targeting a Pakistani government official. Hossain agreed to launder the money through his business, and Aref, the imam of a local mosque, agreed to witness and guarantee the transactions to ensure that they were conducted according to the laws of Allah.

Material Support to Hamas

Mohamed Shorbagi. On August 28, 2006, Mohamed Shorbagi pled guilty in the Northern District of Georgia to providing material support to Hamas, a designated foreign terrorist organization. Shorbagi provided financial support to Hamas through donations to the Holy Land Foundation for Relief and Development, and conspired with others to provide such material support, knowing that Hamas had been designated as a foreign terrorist organization and that Hamas engaged in terrorist activity. Shorbagi also hosted high-level Hamas officials at a Georgia mosque, where he served as the imam. He was sentenced to 92 months in prison. Shorbagi also testified in the trial of Abdelhaleem Ashqar and Muhammad Salah in the Northern District of Illinois, who were charged along with others with participation in a 15-year racketeering conspiracy in the U.S. and abroad, using bank accounts in the United States to launder millions of dollars to illegally finance Hamas' terrorist activities in Israel, the West Bank, and Gaza Strip. On February 1, 2007, Salah and Ashqar were convicted on obstruction and contempt charges but acquitted of racketeering conspiracy charges. Salah was sentenced on July 11, 2007, to 21 months imprisonment. Ashqar was sentenced on November 21, 2007, to 135 months imprisonment.

Rendering Assistance to a Khalistan Commando Force

Khalistan Commando Force. On December 20, 2006, a jury in the Eastern District of New York returned a verdict convicting Khalid Awan of providing money and financial services to the Khalistan Commando Force (KCF), a terrorist organization (although not on a UN Security Council Resolution or U.S. Government list) responsible for thousands of deaths in India since its founding in 1986. Awan was sentenced to 14 years in prison on September 12, 2007. KCF was formed in 1986 and is comprised of Sikh militants who seek to establish a separate Sikh state in the Punjab region of India. The organization has engaged in numerous assassinations of prominent Indian government officials—including the murder of Chief Minister Beant Singh of Punjab in 1995—and hundreds of bombings, acts of sabotage and kidnappings. The government's evidence at trial included recordings of Awan's prison telephone calls to Panjwar in Pakistan, in which Awan introduced the inmate as a potential recruit for the KCF; statements by Awan admitting that he sent hundreds of thousands of dollars to KCF; testimony by two New York-area fund raisers for the KCF who stated that they delivered money to Awan's residence in Garden City; and testimony by the Assistant Inspector General of the Punjab Police Intelligence Division that the KCF was responsible for the deaths of thousands of innocent victims in India.

Major Money Laundering Countries

Every year, U.S. officials from agencies with anti-money laundering responsibilities meet to assess the money laundering situations in 200 jurisdictions. The review includes an assessment of the significance of financial transactions in the country's financial institutions that involve proceeds of serious crime, steps taken or not taken to address financial crime and money laundering, each jurisdiction's vulnerability to money laundering, the conformance of its laws and policies to international standards, the effectiveness with which the government has acted, and the government's political will to take needed actions.

The 2008 INCSR assigned priorities to jurisdictions using a classification system consisting of three differential categories titled Jurisdictions of Primary Concern, Jurisdictions of Concern, and Other Jurisdictions Monitored.

The "Jurisdictions of Primary Concern" are those jurisdictions that are identified pursuant to the INCSR reporting requirements as "major money laundering countries." A major money laundering country is defined by statute as one "whose financial institutions engage in currency transactions involving significant amounts of proceeds from international narcotics trafficking." However, the complex nature of money laundering transactions today makes it difficult in many cases to distinguish the proceeds of narcotics trafficking from the proceeds of other serious crime. Moreover, financial institutions engaging in transactions involving significant amounts of proceeds of other serious crime are vulnerable to narcotics-related money laundering. The category "Jurisdiction of Primary Concern" recognizes this relationship by including all countries and other jurisdictions whose financial institutions engage in transactions involving significant amounts of proceeds from all serious crime. Thus, the focus of analysis in considering whether a country or jurisdiction should be included in this category is on the significance of the amount of proceeds laundered, not of the anti-money laundering measures taken. This is a different approach taken than that of the FATF Non-Cooperative Countries and Territories (NCCT) exercise, which focuses on a jurisdiction's compliance with stated criteria regarding its legal and regulatory framework, international cooperation, and resource allocations.

All other countries and jurisdictions evaluated in the INCSR are separated into the two remaining groups, "Jurisdictions of Concern" and "Other Jurisdictions Monitored," on the basis of a number of factors that may include: (1) whether the country's financial institutions engage in transactions involving significant amounts of proceeds from serious crime; (2) the extent to which the jurisdiction is or remains vulnerable to money laundering, notwithstanding its money laundering countermeasures, if any (an illustrative list of factors that may indicate vulnerability is provided below); (3) the nature and extent of the money laundering situation in each jurisdiction (for example, whether it involves drugs or other contraband); (4) the ways in which the United States regards the situation as having international ramifications; (5) the situation's impact on U.S. interests; (6) whether the jurisdiction has taken appropriate legislative actions to address specific problems; (7) whether there is a lack of licensing and oversight of offshore financial centers and businesses; (8) whether the jurisdiction's laws are being effectively implemented; and (9) where U.S. interests are involved, the degree of cooperation between the foreign government and U.S. government agencies. Additionally, given concerns about the increasing interrelationship between inadequate money laundering legislation and terrorist financing, terrorist financing is an additional factor considered in making a determination as to whether a country should be considered an "Other Jurisdiction Monitored " or a "Jurisdiction of Concern." A government (e.g., the United States or the United Kingdom) can have comprehensive anti-money laundering laws on its books and conduct aggressive anti-money laundering enforcement efforts but still be classified a "Primary Concern" jurisdiction. In some cases, this classification may simply or largely be a function of the size of the jurisdiction's economy. In such jurisdictions quick, continuous, and effective anti-money laundering efforts by the government are critical. While the actual money laundering problem in jurisdictions classified "Concern" is not as acute, they too must

undertake efforts to develop or enhance their anti-money laundering regimes. Finally, while jurisdictions in the "Other" category do not pose an immediate concern, it will nevertheless be important to monitor their money laundering situations because, under certain circumstances, virtually any jurisdiction of any size can develop into a significant money laundering center.

Vulnerability Factors

The current ability of money launderers to penetrate virtually any financial system makes every jurisdiction a potential money laundering center. There is no precise measure of vulnerability for any financial system, and not every vulnerable financial system will, in fact, be host to large volumes of laundered proceeds, but a checklist of what drug money managers reportedly look for provides a basic guide. The checklist includes:

- Failure to criminalize money laundering for all serious crimes or limiting the offense to narrow predicates.
- Rigid bank secrecy rules that obstruct law enforcement investigations or that prohibit or inhibit large value and/or suspicious or unusual transaction reporting by both banks and nonbank financial institutions.
- Lack of or inadequate "know-your-client" requirements to open accounts or conduct financial transactions, including the permitted use of anonymous, nominee, numbered, or trustee accounts.
- No requirement to disclose the beneficial owner of an account or the true beneficiary of a transaction.
- Lack of effective monitoring of cross-border currency movements.
- No reporting requirements for large cash transactions.
- No requirement to maintain financial records over a specific period of time.
- No mandatory requirement to report suspicious transactions or a pattern of inconsistent reporting under a voluntary system; lack of uniform guidelines for identifying suspicious transactions.
- Use of bearer monetary instruments.
- Well-established nonbank financial systems, especially where regulation, supervision, and monitoring are absent or lax.
- Patterns of evasion of exchange controls by legitimate businesses.
- Ease of incorporation, in particular where ownership can be held through nominees or bearer shares, or where off-the-shelf corporations can be acquired.
- No central reporting unit for receiving, analyzing, and disseminating to the competent authorities information on large value or suspicious or unusual financial transactions that might identify possible money laundering activity.
- Lack of or weak bank regulatory controls, or failure to adopt or adhere to Basel Committee's "Core Principles for Effective Banking Supervision," especially in jurisdictions where the monetary or bank supervisory authority is understaffed, under skilled, or uncommitted.

- Well-established offshore financial centers or tax-haven banking systems, especially jurisdictions where such banks and accounts can be readily established with minimal background investigations.
- Extensive foreign banking operations, especially where there is significant wire transfer activity or multiple branches of foreign banks, or limited audit authority over foreign-owned banks or institutions.
- Jurisdictions where charitable organizations or alternate remittance systems, because of their unregulated and unsupervised nature, are used as avenues for money laundering or terrorist financing.
- Limited asset seizure or confiscation authority.
- Limited narcotics, money laundering and financial crime enforcement, and lack of trained investigators or regulators.
- Jurisdictions with free trade zones where there is little government presence or other supervisory authority.
- Patterns of official corruption or a laissez-faire attitude toward the business and banking communities.
- Jurisdictions where the U.S. dollar is readily accepted, especially jurisdictions where banks and other financial institutions allow dollar deposits.
- Well-established access to international bullion trading centers in New York, Istanbul, Zurich, Dubai and Mumbai.
- Jurisdictions where there is significant trade in or export of gold, diamonds, and other gems.
- Jurisdictions with large parallel or black market economies.
- Limited or no ability to share financial information with foreign law enforcement authorities.

Changes in INCSR Priorities for 2007

Jurisdictions moving from the Primary Concern column to the Concern column: Bosnia and Herzegovina and St. Kitts & Nevis.

Jurisdictions moving from the Other/Monitored column to the Concern column: Ghana, Guinea-Bissau, and Suriname.

In the Country/Jurisdiction Table on the following page, “major money laundering countries” that are in the “Jurisdictions of Primary Concern” column are identified for purposes of statutory INCSR reporting requirements. Identification as a “major money laundering country” is based on whether the country or jurisdiction’s financial institutions engage in transactions involving significant amounts of proceeds from serious crime. It is not based on an assessment of the country or jurisdiction’s legal framework to combat money laundering; its role in the terrorist financing problem; or the degree of its cooperation in the international fight against money laundering, including terrorist financing. These factors, however, are included among the vulnerability factors when deciding whether to place a country in the “concern” or “other” column. This year, the movement of Bosnia and Herzegovina from the Primary Concern Column to the Concern Column was based on the absence of significant money laundering, not on its continued vulnerability to terrorist financing.

Note: Country reports are provided for only those countries listed in Primary Concern column and the Concern column.

Country/Jurisdiction Table

Countries/Jurisdictions of Primary Concern

Afghanistan
Antigua and Barbuda
Australia
Austria
Bahamas
Belize
Brazil
Burma
Cambodia
Canada
Cayman Islands
China, People Rep
Colombia
Costa Rica
Cyprus
Dominican Republic
France
Germany
Greece
Guatemala
Guernsey
Haiti
Hong Kong
India
Indonesia
Iran
Isle of Man
Israel
Italy
Japan
Jersey
Kenya
Latvia
Lebanon
Liechtenstein
Luxembourg
Macau
Mexico
Netherlands
Nigeria
Pakistan
Panama
Paraguay
Philippines
Russia
Singapore
Spain
Switzerland
Taiwan
Thailand
Turkey
Ukraine
United Arab Emirates
United Kingdom
United States
Uruguay
Venezuela

Countries/Jurisdictions of Concern

Albania
Algeria
Angola
Argentina
Aruba
Bahrain
Bangladesh
Barbados
Belarus
Belgium
Bolivia
Bosnia and Herzegovina
British Virgin Islands
Bulgaria
Chile
Comoros
Cook Islands
Cote d'Ivoire
Czech Rep
Dominica
Ecuador
Egypt
El Salvador
Ghana
Gibraltar
Grenada
Guinea-Bissau
Guyana
Honduras
Hungary
Iraq
Ireland
Jamaica
Jordan
Korea, North
Korea, South
Kuwait
Laos
Malaysia
Moldova
Monaco
Morocco
Netherlands Antilles
Nicaragua
Palau
Peru
Poland
Portugal
Qatar
Romania
Samoa
Saudi Arabia
Senegal
Serbia
Seychelles
Sierra Leone
Slovakia
South Africa
St. Kitts & Nevis
St. Lucia
St. Vincent
Suriname
Syria
Tanzania
Turks and Caicos
Uzbekistan
Vanuatu
Vietnam
Yemen
Zimbabwe

Other Countries/Jurisdictions Monitored

Andorra
Anguilla
Armenia
Azerbaijan
Benin
Bermuda
Botswana
Brunei
Burkina Faso
Burundi
Cameroon
Cape Verde
Central African Republic
Chad
Congo, Dem Rep of
Congo, Rep of
Croatia
Cuba
Denmark
Djibouti
East Timor
Equatorial Guinea
Eritrea
Estonia
Ethiopia
Fiji
Finland
Gabon
Gambia
Georgia
Guinea
Iceland
Kazakhstan
Kyrgyz Republic
Lesotho
Liberia
Lithuania
Macedonia
Madagascar
Malawi
Maldives
Mali
Malta
Marshall Islands
Mauritania
Mauritius
Micronesia FS
Mongolia
Montenegro
Montserrat
Mozambique
Namibia
Nauru
Nepal
New Zealand
Niger
Niue
Norway
Oman
Papua New Guinea
Rwanda
San Marino
Sao Tome & Principe
Slovenia
Solomon Islands
Sri Lanka
Swaziland
Sweden
Tajikistan
Togo
Tonga
Trinida and Tobago
Tunisia
Turkmenistan
Uganda
Zambia

Introduction to Comparative Table

The comparative table that follows the Glossary of Terms below identifies the broad range of actions, effective as of December 31, 2007 that jurisdictions have, or have not, taken to combat money laundering. This reference table provides a comparison of elements that define legislative activity and identify other characteristics that can have a relationship to money laundering vulnerability.

Glossary of Terms

1. "Criminalized Drug Money Laundering": The jurisdiction has enacted laws criminalizing the offense of money laundering related to drug trafficking.
2. "Criminalized Beyond Drugs": The jurisdiction has extended anti-money laundering statutes and regulations to include nondrug-related money laundering.
3. "Record Large Transactions": By law or regulation, banks are required to maintain records of large transactions in currency or other monetary instruments.
4. "Maintain Records Over Time": By law or regulation, banks are required to keep records, especially of large or unusual transactions, for a specified period of time, e.g., five years.
5. "Report Suspicious Transactions": By law or regulation, banks are required to record and report suspicious or unusual transactions to designated authorities. On the Comparative Table the letter "M" signifies mandatory reporting; "P" signifies permissible reporting.
6. "Financial Intelligence Unit": The jurisdiction has established an operative central, national agency responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to the competent authorities disclosures of financial information concerning suspected proceeds of crime, or required by national legislation or regulation, to counter money laundering. These reflect those jurisdictions that are members of the Egmont Group.
7. "System for Identifying and Forfeiting Assets": The jurisdiction has enacted laws authorizing the tracing, freezing, seizure and forfeiture of assets identified as relating to or generated by money laundering activities.
8. "Arrangements for Asset Sharing": By law, regulation, or bilateral agreement, the jurisdiction permits sharing of seized assets with third party jurisdictions which assisted in the conduct of the underlying investigation.
9. "Cooperates w/International Law Enforcement": By law or regulation, banks are permitted/required to cooperate with authorized investigations involving or initiated by third party jurisdictions, including sharing of records or other financial data.
10. "International Transportation of Currency": By law or regulation, the jurisdiction, in cooperation with banks, controls or monitors the flow of currency and monetary instruments crossing its borders. Of critical weight here are the presence or absence of wire transfer regulations and use of reports completed by each person transiting the jurisdiction and reports of monetary instrument transmitters.
11. "Mutual Legal Assistance": By law or through treaty, the jurisdiction has agreed to provide and receive mutual legal assistance, including the sharing of records and data.
12. "Nonbank Financial Institutions": By law or regulation, the jurisdiction requires nonbank financial institutions to meet the same customer identification standards and adhere to the same reporting requirements that it imposes on banks.

13. "Disclosure Protection Safe Harbor": By law, the jurisdiction provides a "safe harbor" defense to banks or other financial institutions and their employees who provide otherwise confidential banking data to authorities in pursuit of authorized investigations.
14. "Criminalized the Financing of Terrorism." The jurisdiction has criminalized the provision of material support to terrorists and/or terrorist organizations.
15. "States Parties to 1988 UN Drug Convention": As of December 31, 2007, a party to the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, or a territorial entity to which the application of the Convention has been extended by a party to the Convention.[1]
16. "States Party to the UN International Convention for the Suppression of the Financing of Terrorism." As of December 31, 2007, a party to the International Convention for the Suppression of the Financing of Terrorism, or a territorial entity to which the application of the Convention has been extended by a party to the Convention.

[1] The United Kingdom extended its application of the 1988 Convention and the United Kingdom Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Gibraltar, Montserrat, Turks and Caicos, Isle of Man, Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

Comparative Table

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	Int'l. Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Internat'l Terrorism Financing Convention
Government/Jurisdiction																
Afghanistan	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Albania	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Algeria	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Andorra	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	N	Y	N
Angola	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	N
Anguilla[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Antigua & Barbuda	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Argentina	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Armenia	Y	Y	N	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Aruba	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Australia	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Austria	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Azerbaijan	Y	N	N	Y	N	N	N	N	N	Y	Y	N	N	Y	Y	Y
Bahamas	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Bahrain	Y	Y	N	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Bangladesh	Y	Y	N	Y	M	N	N	N	N	Y	Y	N	N	N	Y	Y
Barbados	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Belarus	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Belgium	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Belize	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Benin	Y	Y	N	Y	M	N	Y	N	Y	Y	N	N	Y	N	Y	Y

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	Int'l. Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Internat'l Terrorism Financing Convention
Bermuda[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Bolivia[2]	Y	Y	N	Y	M	N	Y	N	N	N	Y	N	Y	N	Y	Y
Bosnia & Herzegovina	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Botswana	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	N	Y	N	Y	Y
Brazil	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
British Virgin Islands[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N
Brunei Darussalam	Y	Y	N	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Bulgaria	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Burkina Faso	N	N	Y	N	M	N	N	N	N	N	N	N	N	N	Y	Y
Burma	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	N	Y	Y
Burundi	N	N	N	Y	N	N	Y	N	Y	Y	N	N	N	N	Y	N
Cambodia	Y	N	Y	Y	M	N	N	N	Y	Y	N	N	N	Y	Y	Y
Cameroon	Y	Y	Y	Y	M	N	Y	N	N	N	N	N	N	N	Y	Y
Canada	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cape Verde	Y	Y		Y	M	N	Y	N			Y			N	Y	Y
Cayman Islands[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Chad	Y	Y	Y	Y	M	N	Y	N	N	Y	N	N	N	N	Y	N
Chile	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
China (PRC)	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	N	Y	Y	Y
Colombia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Comoros	Y	Y	N	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

[2] Bolivia's FIU was suspended from membership in the Egmont Group on July 31, 2007

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	Int'l. Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Internat'l Terrorism Financing Convention
Congo (Dem. Republic)	Y	Y	Y	Y	M	N	Y	N	N	N	N	Y	Y	Y	Y	Y
Congo (Republic)	Y	Y	Y	Y	M	N	N	N	N	N	Y	Y	Y	Y	Y	Y
Cook Islands	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Costa Rica	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y
Cote D'Ivoire	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Croatia	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cuba	Y	Y	N	N	P	N	Y	N	N	Y	N	N	N	Y	Y	Y
Cyprus (ROC)	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cyprus ("TRNC")	Y	Y	Y	Y	M	N	N	N	N	Y	N	N			NA	NA
Czech Republic	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Denmark	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Djibouti	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Dominica	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Dominican Republic	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	N
East Timor	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Ecuador	Y	Y	Y	Y	M	N	Y	Y	N	Y	Y	Y	N	N	Y	Y
Egypt	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
El Salvador	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Equatorial Guinea	Y	Y	Y	Y	M	N	N	N	N	N	N	N	N	N	N	Y
Eritrea	N	N	Y	Y	N	N	N	N	Y	Y	N	N	N	N	Y	N
Estonia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Ethiopia	Y	Y	Y	Y	M	N	N	N	N	N	N	N	N	N	Y	N
Fiji	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	N	Y	N	Y	N
Finland	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
France	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Gabon	N	N	Y	Y	M	N	N	N	N	N	N	Y	N	N	Y	Y

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	Int'l. Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Internat'l Terrorism Financing Convention
Gambia	Y	Y	N	Y	M	N	Y	N	N	N	N	N	Y	N	Y	N
Georgia	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Germany	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Ghana	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Gibraltar[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N
Greece	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Grenada	Y	Y	N	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Guatemala	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Guernsey[1]	Y	Y	N	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Guinea	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	Y	Y
Guinea-Bissau	Y	Y	Y	Y	M	N	N	N	N	N	Y	Y	Y	Y	Y	N
Guyana	Y	Y	N	Y	M	N	Y	N	N	Y	Y	N	Y	N	Y	Y
Haiti	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	N
Honduras	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Hong Kong[2]	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Hungary	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Iceland	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
India	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Indonesia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Iran	N	N	N	Y	M	N	N	N	N	N	N	N	N	N	Y	N
Iraq	Y	Y	N	Y	M	N	Y	N	N	Y	N	Y	Y	Y	Y	N
Ireland	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

[2] The People's Republic of China extended the UN Financing of Terrorism Convention to the Special Administrative Regions of Hong Kong and Macau.

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	Int'l. Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Internat'l Terrorism Financing Convention
Isle of Man[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Israel	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Italy	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Jamaica	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Japan	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Jersey[1]	Y	Y	N	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Jordan	Y	Y	N	Y	M	N	Y	Y	N	N	Y	Y	Y	Y	Y	Y
Kazakhstan	Y	N	N	Y	P	N	N	N	N	Y	Y	N	N	Y	Y	Y
Kenya	Y	N	Y	Y	P	N	N	N	Y	Y	Y	N	N	N	Y	Y
Korea (DPRK)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N
Korea (Republic of)	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Kosovo	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	NA	NA
Kuwait	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	N
Kyrgyzstan	N	N	N	N	P	N	Y	N	N	N	N	N	Y	N	Y	Y
Laos	Y	Y	N	N	M	N	N	N	Y	Y	Y	Y	Y	Y	Y	N
Latvia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Lebanon	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	N
Lesotho	N	N	Y	Y	M	N	N	N	Y	N	Y	N	Y	N	Y	Y
Liberia	Y	Y	N	N	P	N	N	N	N	Y	N	N	N	N	Y	Y
Libya	Y	Y	N	Y	M	N	N	N	N	N	N	Y	Y	N	Y	Y
Liechtenstein	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Lithuania	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Luxembourg	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	Int'l. Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Internat'l Terrorism Financing Convention
Macau[1]	Y	Y	N	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Macedonia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Madagascar	Y	Y	N	Y	N	N	Y	N		N	Y	Y	Y	N	Y	Y
Malawi	N	N	Y	Y	P	N	N	N		N	N	N	N	N	Y	Y
Malaysia	Y	Y	N	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Maldives	Y	N	N	N	M	N	Y	N		N		N	N	Y	Y	Y
Mali	Y	Y	N	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Malta	Y	Y	N	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Marshall Islands	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y
Mauritania	Y	Y	Y	Y	P	N	Y	N	Y	N	Y	N	Y	Y	Y	Y
Mauritius	Y	Y	N	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Mexico	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Micronesia	Y	Y	N	Y	N	N	Y	N	Y	N	Y	N	Y	N	Y	Y
Moldova	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Monaco	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Mongolia	N	N	N	N	N	N	Y	N	N	N	N	N	Y	N	Y	Y
Montenegro	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Montserrat[1]	Y	Y	N	Y	M	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Morocco	Y	Y	N	Y	M	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
Mozambique	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Namibia	Y	Y	Y	Y	M	N	N	N	N	Y	Y	Y	N	N	N	N
Nauru	Y	Y	N	Y	M	N	Y	Y	Y	N	Y	Y	Y	Y	N	Y

[1] The People's Republic of China extended the UN Financing of Terrorism Convention to the Special Administrative Regions of Hong Kong and Macau.

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	Int'l. Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Internat'l Terrorism Financing Convention
Nepal	N	N	N	Y	N	N	N	N	Y	N	N	N	N	N	Y	N
Netherlands	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Netherlands Antilles	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N
New Zealand	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Nicaragua	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y
Niger	Y	Y	N	Y	M	N	Y	N	Y	N	N	Y	N	N	Y	Y
Nigeria	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Niue	Y	Y	N	Y	M	Y	Y	N	Y	N	Y	Y	Y	N	NA	NA
Norway	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Oman	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	N
Pakistan	Y	Y	Y	Y	M	N	Y	N	N	N	Y	Y	Y	Y	Y	N
Palau	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Panama	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Papua New Guinea	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y
Paraguay	Y	Y	Y	Y	M	Y	N	N	Y	Y	Y	Y	Y	N	Y	Y
Peru	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Philippines	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Poland	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Portugal	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Qatar	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Romania	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Russia	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Rwanda	N	N	N	N	P	N	N	N	Y	N	N	N	N	N	Y	Y

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

Samoa	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
San Marino	Y	Y	N	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Sao Tome & Principe	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y
Actions by Governments	**Criminalized Drug Money Laundering**	**Criminalized Beyond Drugs**	**Record Large Transactions**	**Maintain Records Over Time**	**Report Suspicious Transactions (NMP)**	**Egmont Financial Intelligence Units**	**System for Identifying/Forfeiting Assets**	**Arrangements for Asset Sharing**	**Cooperates w/International Law Enf.**	**Int'l. Transportation of Currency**	**Mutual Legal Assistance**	**Non-Bank Financial Institutions**	**Disclosure Protection "Safe Harbor"**	**Criminalized Financing of Terrorism**	**States Party to 1988 UN Convention**	**Internat'l Terrorism Financing Convention**
Saudi Arabia	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Senegal	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Serbia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Seychelles	Y	Y	N	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Sierra Leone	Y	Y	Y	Y	M	N	Y	N	N	Y	Y	Y	Y	Y	Y	Y
Singapore	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Slovakia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Slovenia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Solomon Islands	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N
South Africa	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Spain	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Sri Lanka	N	N	N	N	N	N	N	N	N	N	Y	N	Y	Y	Y	Y
St Kitts & Nevis	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
St. Lucia	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	N
St. Vincent/Grenadines	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Suriname	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	N
Swaziland	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	N	Y	Y
Sweden	Y	Y	Y	Y	M	Y	Y		Y	N	Y	Y	Y	Y	Y	Y
Switzerland	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Syria	Y	Y	Y	Y	M	Y	Y	N	N	N	Y	Y	N	N	Y	Y
Taiwan	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	N	NA	NA
Tajikistan	Y	Y	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y
Tanzania	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	Int'l. Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Internat'l Terrorism Financing Convention
Thailand	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Togo	Y	N	Y	Y	N	N	Y	N	Y	N	Y	N	Y	N	Y	Y
Tonga	Y	Y	Y	Y	M	N	Y	N	Y	Y	N	N	N	N	Y	Y
Trinidad & Tobago	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Tunisia	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Turkey	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Turkmenistan	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	N	N	Y	Y	Y
Turks & Caicos[1]	Y	Y	Y	Y	M	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Uganda	Y	N	N	N	N	N	N	N	Y	N	N	N	Y	Y	Y	Y
Ukraine	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
United Arab Emirates	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
United Kingdom	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
United States	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Uruguay	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Uzbekistan	Y	Y	N	Y	N	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y
Vanuatu	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Venezuela	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Vietnam	Y	Y	Y	Y	M	N	Y	N	N	Y	Y	Y	N	N	Y	Y
Yemen	Y	Y	N	Y	M	N	N	N	Y	N	Y	Y	Y	N	Y	N
Zambia	Y	Y	N	Y	M	N	Y	N	Y	N	Y	N		N	Y	N
Zimbabwe	Y	Y	N	Y	M	N	Y	N	N	Y	N	N	N	Y	Y	N

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

Country Reports

Afghanistan

Afghanistan is not a regional financial or banking center, and is not considered an offshore financial center. However, its formal financial system is growing rapidly while its traditional informal financial system remains significant in reach and scale. Afghanistan is a major drug trafficking and drug producing country and the illicit narcotics trade is the primary source of laundered funds. Afghanistan passed anti-money laundering and terrorist financing legislation in October 2005, and efforts are being made to strengthen police and customs forces. However, there remain few resources, limited capacity, little expertise and insufficient political will to combat financial crimes. The most fundamental obstacles continue to be legal, cultural and historical factors that conflict with more Western-style proposed reforms to the financial sector. Public corruption is a significant problem. Afghanistan is ranked 172 out of 180 countries in Transparency International's 2007 Corruption Perception Index.

According to United Nations (UN) statistics, in 2005 and 2006, opium production increased and today Afghanistan accounts for over 90 percent of the world's opium production. Opium gum is sometimes used as a currency—especially by rural farmers—and it is used as a store of value in prime production areas. It is estimated that at least one third of Afghanistan's (licit plus illicit) gross domestic product (GDP) is derived directly from narcotics activities, and proceeds generated from the drug trade have reportedly fueled a growing real estate boom in Kabul, as well as a sharp increase in capital investment in rural poppy growing areas.

Much of the recent rise in opium production comes from Taliban strongholds in the southern part of the country. The Taliban impose taxes on narcotics dealers, which undoubtedly helps finance their terrorist activities. Additional revenue streams for the Taliban and regional warlords come from "protecting" opium shipments, running heroin labs, and from "toll booths" established on transport and smuggling routes.

Afghan opium is refined into heroin by production labs, more of which are being established within Afghanistan's borders. The heroin is then often broken into small shipments and smuggled across porous borders for resale abroad. Payment for the narcotics outside the country is facilitated through a variety of means, including through conventional trade and the traditional hawala system that uses trade as the primary medium to balance accounts. In addition, the narcotics themselves are often used as tradable goods and as a means of exchange for automobiles, construction materials, foodstuffs, vegetable oils, electronics, and other goods between Afghanistan and neighboring Pakistan and Iran. Many of these goods are smuggled into Afghanistan from neighboring countries, particularly Iran and Pakistan, or enter via the Afghan Transit Trade Agreement (ATTA) without payment of customs duties or tariffs. Most of the trade goods imported into Afghanistan originate in Dubai. Invoice fraud, corruption, indigenous smuggling networks, underground finance, and legitimate commerce are all intertwined.

Afghanistan is widely served by the hawala system, which provides a range of financial and nonfinancial business services in local, regional, and international markets. Financial activities include foreign exchange transactions, funds transfers (particularly to and from neighboring countries with weak regulatory regimes for informal remittance systems), micro and trade finance, as well as some deposit-taking activities. While the hawala network may not provide financial intermediation of the same type as the formal banking system (i.e., deposit-taking for lending and investing purposes based on the assessment, underwriting, and pricing of risks), it is a traditional form of finance and deeply entrenched and widely used throughout Afghanistan and the neighboring region.

There are over 300 known hawala dealers in Kabul, with branches or additional dealers in each of the 34 provinces. These dealers are organized into informal provincial unions or guilds whose members maintain a number of agent-principal and partnership relationships with other dealers throughout the country and internationally. Their record keeping and accounting practices are robust, efficient, and take note of currencies traded, international pricing, deposit balances, debits and credits with other dealers, lending, cash on hand, etc. Hawaladars are supposed to be licensed; however the licensing regime that existed from April 2004 until September of 2006 was overly burdensome and resulted in issuance of few licenses. In September of 2006, Da Afghanistan Bank (DAB), Afghanistan's Central Bank, issued a new money service provider regulation that streamlined the licensing process and substantially reduced the licensing and ongoing compliance burden for hawaladars. The focus of the regulation is on anti-money laundering and counter-terrorist financing (AML/CTF). The regulation requires and provides standard mechanisms for record keeping and reporting of large transactions. The DAB provided training sessions on the regulation and has developed a streamlined application process. In Kabul, approximately 100 licenses have been issued under the regulation, which is the result of the DAB outreach, law enforcement actions, and pressure from commercial banks where hawaladars hold accounts. Options for strengthening the hawaladar unions and promoting self-regulation are also being studied. The DAB has begun outreach efforts to money service providers in other large cities, specifically Mazar-e-Sharif and Herat, and hopes to expand the licensing to these cities in 2008. Given how widely used the hawala system is in Afghanistan, financial crimes undoubtedly occur through these entities.

In early 2004, the DAB worked in collaboration with international donors to establish the legislative framework for AML/CTF initiatives. Although Afghanistan was unable to meet its initial commitment to enact both pieces of legislation by September 30, 2004, they were both finalized and signed into law by late October 2004.

The Anti-Money Laundering and Proceeds of Crime and Combating the Financing of Terrorism laws incorporate provisions that are designed to meet the recommendations of the Financial Action Task Force (FATF). These laws address the criminalization of money laundering and the financing of terrorism, customer due diligence, the establishment of a financial intelligence unit (FIU), international cooperation, extradition, and the freezing and confiscation of funds. Under the law, money laundering and terrorist financing are criminal offences. The AML law also includes provisions to address cross-border currency reporting, and establishes authorities to seize and confiscate monies found to be undeclared or falsely declared, or determined to be transferred for illicit purposes.

Under the AML law, the Financial Transactions and Reports Analysis Center of Afghanistan (FinTRACA), Afghanistan's FIU, has been established and is functioning as a semi-autonomous unit within the DAB. The FIU, originally to be established in January 2005, was actually initiated in October 2005—with the assignment of a General Director, office space, and other basic resources.

Banks and other financial and nonfinancial institutions are required to report to the FIU all suspicious transactions and large cash transactions above the equivalent of U.S. $10,000, as prescribed by the DAB. These financial institutions are also required to maintain their records for a minimum of 10 years. Approximately 10,000 large cash transaction reports are currently being received from financial institutions and processed each month. The FIU has over 140,000 large transaction reports currently stored in its database that can be searched using a number of criteria. The FIU has the legal authority to freeze financial assets for up to seven days. FinTRACA also has access to records and databases of other government entities.

The formal banking sector consists of sixteen licensed banks. AML examinations have been conducted for all these banks that have resulted in a growing awareness of AML requirements, deficiencies among the banks, and a need for building the AML capacity of the formal financial sector. Additionally, the Central Bank has worked with the banking community through the Afghan Bankers

Association (ABA) to develop several ongoing topical working groups focused on AML issues. The ABA has recently designed a "know your customer" (KYC) form that has been accepted by the financial industry and has provided on-going education on identifying suspicious transactions. Seven suspicious transaction reports were received in 2007 by the FIU, one of which was referred to law enforcement for investigation.

The Afghanistan Central Bank has circulated a list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list of designated individuals and entities to financial institutions. There is no information currently available regarding the results of these lists being circulated.

The Supervision Department within the DAB was formed at the end of 2003, and is divided into four divisions: Licensing, General Supervision (which includes on-site and off-site supervision), Special Supervision (which deals with special cases of problem banks), and Regulation. The Department is charged with administering the AML/CTF legislation, conducting examinations, licensing new institutions, overseeing money service providers, and outreach to the commercial banking sector. The effectiveness of the Supervision Department in the AML area remains limited due to staffing, organization, and management issues. As a result, FinTRACA has taken on some supervisory responsibilities, yet resources are limited.

The Ministry of Interior (MOI) and the Attorney General's Office are the primary financial enforcement and investigative authorities. They are responsible for tracing, seizing and freezing assets. While MOI generally has adequate police powers, it lacks the resources to trace, seize, and freeze assets. According to FinTRACA, it is not aware of Afghanistan freezing, seizing, or forfeiting related assets in 2007, or of any calls on the banking community for cooperation with enforcement efforts. FinTRACA has an MOU in place with the MOI for cooperation and currently shares information with the Sensitive Investigations Unit (SIU), a law enforcement group within the MOI.

Pursuant to the Central Bank law, a Financial Services Tribunal will be established to review certain decisions and orders of the DAB. Judges and administrative staff will need to significantly increase their technical knowledge before the Tribunal is effective. The Tribunal will review supervisory actions of the DAB, but will not prosecute cases of financial crime. At present, all financial crime cases are being forwarded to the Kabul Provincial Court, where there has been little to no activity in the last three years. The process to prosecute and adjudicate cases is long and cumbersome, significantly underdeveloped, and corruption can play a role at various levels. There was one arrest for alleged terrorist financing in 2007 but the individual was not prosecuted.

Border security continues to be a major issue throughout Afghanistan. At present there are 21 border crossings that have come under central government control, utilizing international donor assistance as well as local and international forces. However, many of the border areas are not policed and therefore susceptible to illicit cross-border trafficking and trade-based money laundering. Many regional warlords also continue to control the international borders in their provincial areas, causing major security risks. Customs authorities, with the help of outside assistance, have made significant strides, but much work remains to be done.

Customs collection has improved, but smuggling and corruption continue to be major concerns, as well as trade fraud, which includes false and over-and under-invoicing. Thorough cargo inspections are not conducted at any gateway. A pilot program for declaring large, cross-border currency transactions has been developed at the Kabul International Airport (KIA). This prototype will serve as the foundation for expansion to other land, air and sea crossings. Currently, KIA requires incoming and outgoing passengers to fill out declarations forms for carrying cash in an amount of 1 million Afghanis (approximately U.S. $20,000) or its equivalent. The DAB is working with Customs authorities to further improve enforcement of airport declarations. However there is very little international air travel outside of Kabul. Although Afghanistan has limited resources to enforce

customs declarations outside of Kabul, the DAB has sent delegations to border crossings in Hairatan and Islam Qala to assess the capacity and describe the provisions of the law to the local authorities. There is no restriction on transporting any amount of declared currency. However, in the case of cash smuggling at the airport, reports are entered into a Customs database and this information is shared with the FIU.

Under the Law on Combating the Financing of Terrorism, any nonprofit organization that wishes to collect, receive, grant, or transfer funds and property must be entered in the registry with the Ministry of Auqaf (Islamic Affairs). All nonprofit organizations are subject to a due diligence process which includes an assessment of accounting, record keeping, and other activities. However, the capacity of the Ministry to conduct such examinations is nearly nonexistent, and the reality is that any organization applying for a registration is granted one. Furthermore, because no adequate enforcement authority exists, many organizations operating under a "tax-exempt" nonprofit status in Afghanistan go completely unregistered, and illicit activities are suspected on the part of a number of organizations.

The Government of Afghanistan (GOA) is a party to 12 of the United Nations (UN) conventions and protocols against terrorism and is a signatory to the International Convention for the Suppression of Acts of Nuclear Terrorism (which is pending ratification). Afghanistan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Afghanistan is also a signatory to the UN Convention against Corruption (UNCAC). Ratification of UNCAC, one of the benchmarks established under the London Compact, as well as amendment of domestic laws to conform to the UNCAC's obligations, remain pending.

In July 2006, Afghanistan became a member in the Asia Pacific Group, a FATF-Style Regional Body (FSRB), and has also obtained observer status in the Eurasian Group, another FSRB. No mutual evaluation has been conducted on the AML/CTF regime of Afghanistan to date; however, the APG is scheduled to assess the financial system in the third quarter of 2009. FinTRACA, Afghanistan's FIU, has active bilateral MOUs for cooperation with the FIU's of the United Kingdom, Russia, the Kyrgyz Republic, and Belarus. Although FinTRACA is not yet a member of the Egmont Group of financial intelligence units, it has taken several steps to build its capacity in efforts to meet international standards.

The Government of Afghanistan has made progress over the past year in developing its overall AML/CTF regime. Improvement has been seen in development of its nascent FIU, the reporting of large cash transactions, participation in international AML bodies, improvement in bank AML compliance awareness, information technology systems, and in efforts to bring money service providers into a legal and regulatory framework. However, much work remains to be done. Afghanistan needs to commit additional resources and find the political will to seriously combat financial crimes, including corruption. Afghanistan should develop secure, reliable, and capable relationships among departments and agencies involved in law enforcement. Afghanistan should develop the investigative capabilities of law enforcement authorities in the various areas of financial crimes, particularly money laundering and terrorist finance. Judicial authorities need to become proficient in understanding the various elements required for money laundering prosecutions. The FIU should become autonomous and increase its staff and resources. Afghan customs authorities should implement cross-border currency reporting and learn to recognize forms of trade-based money laundering. Border enforcement should be a priority, both to enhance scarce revenue and to disrupt narcotics trafficking and illicit value transfer. Afghan authorities should also work to address the widespread corruption in commerce and government.

Albania

Albania is not considered an important regional financial or offshore center. As a transit country for trafficking in narcotics, arms, contraband, and humans, Albania remains at significant risk for money laundering. The major sources of criminal proceeds in the country are trafficking offenses, official corruption and fraud. Corruption and organized crime are likely the most significant sources of money laundering, but the exact extent to which these various illegal activities contribute to overall crime proceeds and money laundering is unknown.

Criminals frequently invest tainted money in real estate and business development projects. Albania has a significant black market for smuggled goods because of its high level of consumer imports and weak customs controls. Organized crime groups use Albania as a base of operations for conducting criminal activities in other countries and often return their illicit gains to Albania. The proceeds from these activities are easily laundered in Albania because of the cash economy and weak government controls on banking.

As a cash-based economy, the Albanian economy is also particularly vulnerable to money laundering activity. Few individuals have bank accounts and check writing is not common. Of the 17 banks in Albania, five of them are considered to have a significant national presence. According to the Bank of Albania (the Central Bank), 25 percent of the money in circulation is outside of the banking system, compared to an average of 10 percent in other Central and Eastern European transitioning economies. A significant portion of remittances enters the country through unofficial channels. It is estimated that only half of total remittances enter Albania through banks or money transfer companies. According to a 2007 United Nations Office on Drugs and Crime (UNODC) report, remittances comprise nearly 14 percent of Albania's annual gross domestic product (GDP.) Black market exchange is still present in the country despite repeated efforts by the Government of Albania (GOA) institutions to impede such exchanges. The Bankers Association estimates that only 20-30 percent of transactions take place through formal banking channels. Similarly, the GOA estimates that proceeds from the informal sector account for approximately 30-60 percent of Albania's GDP. Although current law permits the operation of free trade zones, none are currently in operation.

Electronic and automatic teller machine (ATM) transactions are relatively few in number but are growing as more banks introduce this technology. The number of ATMs expanded following the decision of the GOA to deliver salaries through electronic transfers. All central government institutions have now converted to electronic pay systems, and many private companies have also started to issue salaries electronically. Credit card usage has also increased, but only a small number of people possess them and usage is primarily limited to a few large vendors. Bank fraud still remains largely undetected.

Albania criminalized money laundering with Article 287, Albanian Criminal Code 1995, as amended. Albania's original money laundering law was "On the Prevention of Money Laundering", or Law No. 8610 of 17 May 2000. In June 2003, Parliament approved Law No. 9084, which strengthened the old Law No. 8610, and improved the Criminal Code and the Criminal Procedure Code. The new law redefined the legal concept of money laundering, harmonizing the Albanian definition with that of the European Union (EU) and international conventions. Under the revised Criminal Code, Albania expanded and upgraded many powers. The new law also revises the definition of money laundering, outlaws the establishment of anonymous accounts, and permits the confiscation of accounts. The law also mandates the identification of beneficial owners. Currently, no law criminalizes negligence by financial institutions in money laundering cases. The Bank of Albania has established a task force to confirm banks' compliance with customer verification rules.

Albania's law sets forth an "all crimes" definition for the offense of money laundering. However, the Albanian court system applies a difficult burden of proof. Albanian courts require a prior or simultaneous conviction for the predicate offense before issuing an indictment for money laundering.

Law 9084 places reporting requirements on both financial institutions and individuals. Obliged institutions must report to Albania's financial intelligence unit (FIU) all transactions that exceed approximately U.S. $200,000 as well as those transactions that involve suspicious activity, regardless of the amount. A new draft law, when enacted, will lower the threshold for currency transaction reporting from the current U.S. $200,000 to U.S. $15,000, thereby ensuring compliance with EU standards. Subject transactions must be reported within 72 hours of their occurrence. Individuals and entities reporting transactions are protected by law if they cooperate with and provide financial information to the FIU and law enforcement agencies. Reportedly, however, leaks of financial disclosure information from other agencies compromise the entities' client confidentiality.

Under current Albanian law, financial institutions have no legal obligation to identify customers prior to opening an account. Albania distinguishes between record keeping of client information and record keeping of transaction information, and, in an effort to reduce the record-keeping burden on obligated entities, has a different threshold for each. While most banks have internal rules mandating customer identification, Albania's money laundering law only requires customer identification prior to conducting transactions that exceed approximately U.S. $20,000 or when there is a suspicion of money laundering. For all transactions in excess of U.S. $20,000, entities must maintain customer records. With regard to transactions, obliged entities are not required to maintain records on transactions under a U.S. $200,000 threshold. For every transaction in excess of U.S. $200,000 entities must maintain records that can be used to reconstruct the transaction if necessary. If there is no suspicion, entities must retain customer identification information for all transactions exceeding U.S. $20,000—but could destroy all records of financial transactions below U.S. $200,000. The new draft law, when enacted, will require client identification regardless of the size of the transaction.

It is the responsibility of the licensing authority to supervise intermediaries for compliance. For example, the Ministry of Justice is responsible for oversight of attorneys and notaries, and the Ministry of Finance for accountants. Although regulations also cover nonbank financial institutions, enforcement has been poor in practice. There is an increasing number of suspicious transaction reports (STRs) coming from banks as that sector matures, although the majority continues to come from tax and customs authorities and foreign counterparts.

Individuals must report to customs authorities all cross-border transactions that exceed approximately U.S. $10,000. Albania provides declaration forms at border crossing points, and the law does not distinguish between an Albanian and a foreign visitor. However, customs controls on cross-border transactions lack effectiveness due to a lack of resources, poor training and, reportedly, corruption of customs officials.

Law No. 8610 established an administrative FIU to coordinate the GOA's efforts to detect and prevent money laundering. Under Law No. 9084, the FIU became a quasi-independent agency within the Ministry of Finance, formally known as the General Directorate for the Prevention of Money Laundering (DPPPP). Albania is in the process of preparing a new administrative law on FIU operations. Referred to as the "draft law," it will clarify certain anti-money laundering measures and elaborate on reporting requirements for obliged entities.

As an administrative-type FIU, the DPPPP does not have law enforcement capabilities. The FIU receives reports from obliged entities, analyzes them, and then disseminates the results of its analysis to the prosecutor's office. After nearly six years, the FIU cannot demonstrate any referral that has resulted in a money laundering prosecution. There were only three money laundering referrals to the Prosecutor's Office during 2006 and all three were declined for prosecution. There were no money laundering referrals to the Prosecutor's Office during 2007. In an effort to increase money laundering prosecutions, in May 2007, Albania established the Economic Crimes and Corruption Joint Investigative Unit (ECCJIU) within the Tirana District Prosecution Office. This unit focuses efforts and builds expertise in the investigation and prosecution of financial crimes and corruption cases by

bringing together members of the General Prosecutors Office, the Albanian State Police's Financial Crimes Sector, the Ministry of Finance's Customs Service and Tax Police, and Albanian intelligence services. The ECCJIU will also receive cooperation from the FIU and the National Intelligence Service. The ECCJIU will have responsibility for the prosecution of money laundering cases within the District of Tirana.

To address the criminal aspects of its informal economy, Albania passed comprehensive legislation against organized crime in 2004. Law No. 9284, the "anti-mafia law," enables civil asset sequestration and confiscation provisions in cases involving organized crime and trafficking. The law applies to the assets of suspected persons, their families, and close associates. In cases where the value of the defendant's assets exceeds the income generated by known legal activity, the law places the burden on the defendant to prove a legitimate source of income for the assets. During 2006, the Serious Crimes Prosecution Office filed twenty forfeiture cases pursuant to the anti-mafia law. The properties sequestered include a sports center of 4000 square meters, hotels, apartments, land, vehicles, and approximately U.S. $35,000 in cash. Although the Agency for the Administration of the Sequestration and Confiscation of Assets (AASCA) is charged with the responsibility of administrating confiscated assets, the agency has failed to function in a meaningful fashion. As such, enforcement of the assets law remains reportedly inadequate due to a lack of financial or political support for the agency.

Article 230/a of the Penal Code criminalizes the financing of terrorism. Financing of terrorism or its support of any kind is punishable by a term of imprisonment of at least fifteen years, and carries a fine of U.S. $50,000 to U.S. $100,000. The Penal Code also contains additional provisions dealing with terrorist financing including sections dealing with giving information regarding the investigation or identification to identified persons, and conducting financial transactions with identified persons. There are no known prosecutions under these laws, but the Prosecutor's Office is currently investigating one case with such implications.

In 2004, Albania enacted Law No. 9258, "On Measures against Terrorist Financing". This law provides a mechanism for the sequestration and confiscation of assets belonging to terrorism financiers, particularly as to the United Nations (UN) updated lists of designees. While comprehensive, it lacks implementing regulations and thus is not fully in force. As of October 2007, the Ministry of Finance claimed to maintain asset freezes against six individuals and fourteen foundations and companies from the UN Security Council's 1267 Consolidated lists of identified terrorist entities. In total, assets worth more than U.S. $10 million, belonging to six persons, five foundations and nine companies, remain sequestered. Reportedly, the full extent of sequestered assets and their exact whereabouts are unknown.

The Ministry of Finance is the main entity responsible for issuing freeze orders. After the Minister of Finance executes an order, the FIU circulates it to other government agencies, which then sequester any assets found belonging to the UNSCR 1267 named individual or entity. The sequestration orders remain in force as long as their names remain on the list.

Albania is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the 1988 UN Drug Convention. Albania is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and was most recently evaluated by MONEYVAL in July 2006. Albania's FIU is also a member of the Egmont Group, the international organization of financial intelligence units.

Although there are continuing initiatives to improve Albania's capacity to deal with financial crimes and money laundering, the lack of positive results and apparent inability to adequately address the deficiencies in the programs continue to hamper progress. Despite Albania's efforts, additional improvements are needed. Albania should increase support and training for the FIU, as a majority of its staff is new and lacks experience in the analysis of money laundering and terrorist financing cases.

The FIU should create or obtain a database to allow effective analysis of the large volume of currency transaction reports and suspicious transaction reports received. Albania should ensure that those charged with pursuing financial crime increase their technical knowledge to include modern financial investigation techniques. Albania should provide its police force with a central database. Investigators and prosecutors should implement case management techniques, and prosecutors, and judges need to become more conversant with the nuances of money laundering. The FIU, prosecutors and ECCJIU should enhance their effectiveness through cooperation with one another and outreach to other entities. Albania should remove the requirement of a conviction for the predicate offense before a conviction for money laundering can be obtained. Albania should devise implementing regulations for Law 9258 regarding sequestration and confiscation of assets linked to the financing of terrorism so that it can be fully effective. The Government of Albania should also improve the enforcement and enlarge the scope of its asset seizure and forfeiture regime, including fully funding and supporting the Agency for the Administration of the Sequestration and Confiscation of Assets (AASCA). Albania should also incorporate into anti-money laundering legislation specific provisions regarding negligent money laundering, corporate criminal liability, comprehensive customer identification procedures, and the adequate oversight of money remitters and charities. Albania should enact its draft law and promulgate implementing regulations as soon as possible.

Algeria

Algeria is not a regional financial center or an offshore financial center. The extent of money laundering through formal financial institutions is thought to be minimal due to stringent exchange control regulations and an antiquated banking sector. The partial convertibility of the Algerian dinar enables the Bank of Algeria (Algeria's Central Bank) to monitor all international financial operations carried out by public and private banking institutions. Embezzlement, fraud, and tax evasion are common financial crimes. Algeria has a large informal and cash-based economy. Algeria is a transit country for men and women trafficked from sub-Sahara Africa en route to Europe.

Algeria first criminalized terrorist financing through the adoption of Ordinance 95.11 on February 24, 1994, making the financing of terrorism punishable by five to ten years of imprisonment. On February 5, 2005, Algeria enacted public law 05.01, entitled "The Prevention and Fight against Money Laundering and Financing of Terrorism." The law aims to strengthen the powers of the Cellule du Traitement du Renseignement Financier (CTRF), an independent financial intelligence unit (FIU) within the Ministry of Finance (MOF) created in 2002. This law seeks to bring Algerian law into conformity with international standards and conventions. It offers guidance for the prevention and detection of money laundering and terrorist financing, institutional and judicial cooperation, and penal provisions.

The 2005 legislation extends money laundering controls to specific, nonbank financial professions such as lawyers, accountants, stockbrokers, insurance agents, pension managers, and dealers of precious metals and antiquities. Provided that information is shared with CTRF in good faith, the law offers immunity from administrative or civil penalties for individuals who cooperate with money laundering and terrorist finance investigations. Under the law, assets may be frozen for up to 72 hours on the basis of suspicious activity; such freezes can only be extended with judicial authorization. Financial penalties for noncompliance range from 50,000 to 5 million Algerian dinars (approximately U.S. $760 to U.S. $76,000). In addition to its provisions pertaining to money laundered from illicit activities, the law allows the investigation of terrorist-associated funds derived from "clean" sources.

The law provides significant authority to the Algerian Banking Commission, the independent body established under the authority of the Bank of Algeria to supervise banks and financial institutions, to inform CTRF of suspicious or complex transactions. The law also gives the Algerian Banking Commission, CTRF, and the Algerian judiciary wide latitude to exchange information with their

foreign government counterparts in the course of money laundering and terrorist finance investigations, provided confidentiality for suspected entities is insured. A clause excludes the sharing of information with foreign governments in the event legal proceedings are already underway in Algeria against the suspected entity, or if the information is deemed too sensitive for national security reasons.

On November 14, 2005, the Government of Algeria issued Executive Decree 05-442 establishing a deadline of September 1, 2006 after which all payments in excess of 50,000 Algerian dinars must be made by check, wire transfer, payment card, bill of exchange, promissory note, or other official bank payment. While nonresidents are exempt from this requirement, they must (like all travelers to and from the country) report foreign currency in their possession to the Algerian Customs Authority. The government suspended the deadline in September 2006, however, in response to the slow implementation of a nation-wide electronic check-clearing system that failed to gain the confidence of the Algerian business community.

In 1996 Algeria adopted ordinance 96-22 regarding exchange regulations and currency movements abroad. The law criminalized cash smuggling as well as the failure to respect reporting requirements for the transfer of cash into or out of Algeria. The maximum value of cash that may be carried by an individual at any given time is the equivalent of 7,600 euros (approximately U.S. $11,000). Higher sums may only be legally sent abroad by wire transfer. Given limits on convertibility of the Algerian dinar, even sums less than the 7,600 euros threshold must be accompanied by a bank statement declaring that the holder acquired the foreign currency with the authorization of the central bank. Holders of foreign currency without such a declaration, such as individuals who traded dinars for foreign currencies in one of Algiers' many black markets, risk confiscation. In addition to foreign currency, the ordinance applies to other liquid financial instruments, precious metals and gemstones. Penalties for noncompliance range from three to five years of imprisonment or a fine valued of up to twice the value of the seized property.

Algerian financial institutions, as well as Algerian customs and tax administration agents, are required to report any activities they suspect of being linked to criminal activity, money laundering, or terrorist financing to CTRF and comply with subsequent CTRF inquiries. They are obligated to verify the identity of their customers or their registered agents before opening an account; they must furthermore record the origin and destination of funds they deem suspicious. In addition, these institutions must maintain confidential reports of suspicious transactions and customer records for at least five years after the date of the last transaction or the closing of an account.

In 2006, the Algerian customs service reported 373 cases of cash smuggling with a total value of U.S. $5.6 million. These cases occurred in 11 of the country's 48 wilayas (regional departments). In 2005, customs reported 426 cases with a total value of U.S. $2.7 million. The total fines levied against smugglers were U.S. $41 million in 2006. In 2007, CTRF investigated 103 suspicious transaction reports.

The Ministry of Interior is charged with registering foreign and domestic nongovernmental organizations in Algeria. While the Ministry of Religious Affairs legally controls the collection of funds at mosques for charitable purposes, some of these funds escape the notice of government monitoring efforts.

Algerian customs and law enforcement authorities are increasingly concerned with cases of customs fraud and trade-based money laundering. In response, Algerian authorities are taking steps to coordinate information sharing between concerned agencies.

In November 2004, Algeria became a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). Algeria is a party to the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, the UN

Convention against Corruption, and the 1988 UN Drug Convention. In addition, Algeria is a signatory to various UN, Arab, and African conventions against terrorism, trafficking in persons, and organized crime. The Ministry of Justice is expected to create a pool of judges trained in financial matters.

The Government of Algeria has taken significant steps to enhance its statutory regime against money laundering and terrorist financing. It needs to move forward now to implement those laws and eliminate bureaucratic barriers among various government agencies by empowering CTRF to be the focal point for the AML/CTF investigations. In addition, given the scope of Algeria's informal economy, it should renew its initiative to limit the size of cash transactions. Algerian law enforcement and customs authorities need to enhance their ability to recognize and investigate trade-based money laundering, value transfer, and bulk cash smuggling used for financing terrorism and other illicit financial activities.

Angola

Angola is neither a regional nor an offshore financial center and has not prosecuted any known cases of money laundering. Angola does not produce significant quantities of drugs, although it continues to be a transit point for drug trafficking, particularly cocaine brought in from Brazil or South Africa destined for Europe. The laundering of funds derived from continuous and widespread high-level corruption is a concern, as is the use of diamonds as a vehicle for money laundering. The Government of the Republic of Angola (GRA) has implemented a diamond control system in accordance with the Kimberley Process. However, through the method of "mixing parcels" of licit and illicit diamonds and the fraudulent purchasing of Kimberley Process "certificates of authenticity," the Kimberley process can be compromised. Corruption and Angola's long and porous borders further facilitate smuggling and the laundering of diamonds.

Angola currently has no comprehensive laws, regulations, or other procedures to detect money laundering and financial crimes. Other provisions of the criminal code do address some related crimes. The various ministries with responsibility for detection and enforcement are revising a draft anti-money laundering law drawn up with help from the World Bank. The Central Bank's Supervision Division, which has responsibility for money laundering issues, exercises some authority to detect and suppress illicit banking activities under legislation governing foreign exchange controls. The Central Bank has the authority to freeze assets, but Angola does not presently have an effective system for identifying, tracing, or seizing assets. Instead, such crimes are addressed through other provisions of the criminal code. For example, Angola's counternarcotics laws criminalize money laundering related to narcotics trafficking.

Angola's high rate of cash flow makes its financial system an attractive site for money laundering. With no domestic interbank dollar clearing system, even dollar transfers between domestic Angolan banks are logged as "international" transfers, thus creating an incentive to settle transfers in cash. The local banking system imports approximately U.S. $200-300 million in currency per month, largely in dollars, without a corresponding cash outflow. Local bank representatives have reported that clients have walked into banks with up to U.S. $2 million in a briefcase to make a deposit. No currency transaction reports cover such large cash transactions. These massive cash flows occur in a banking system ill-equipped to detect and report suspicious activity. The Central Bank has no workable data management system and only rudimentary analytic capability. Corruption pervades Angolan society and commerce and extends across all levels of government. Angola is rated 147 out of 180 countries in Transparency International's 2007 International Corruption Perception Index.

Angola is party to the 1988 UN Drug Convention and the UN Convention against Corruption. Angola has signed but has not yet ratified the UN Convention against Transnational Organized Crime. Angola has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Angola should pass its pending legislation to criminalize money laundering beyond drug offenses and terrorist financing. The GRA should establish a system of financial transparency reporting requirements and a corresponding Financial Intelligence Unit through legislation that adheres to world standards. The GRA should then move quickly to implement this legislation and bolster the capacity of law enforcement to investigate financial crimes. Angola's judiciary, including its Audit Court (Tribunal de Contas) should give priority to prosecuting financial crimes, including corruption. The GRA should become a party to both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. The GRA should increase efforts to combat official corruption, by establishing an effective system to identify, trace, seize, and forfeit assets and by empowering investigative magistrates to actively seek out and prosecute high profile cases of corruption.

Antigua and Barbuda

Antigua and Barbuda has comprehensive legislation in place to regulate its financial sector, but remains susceptible to money laundering because of its offshore financial sectors and Internet gaming industry. As with other countries in the region, illicit proceeds from the transshipment of narcotics are laundered in Antigua and Barbuda. Its offshore financial sector exacerbates Antigua and Barbuda's vulnerability to money laundering.

In 2007, Antigua and Barbuda had 17 offshore banks, three offshore trusts, two offshore insurance companies, 3,255 international business corporations (IBCs), and 23 licensed Internet gaming companies. The International Business Corporations Act of 1982 (IBCA), as amended, is the governing legal framework for offshore businesses in Antigua and Barbuda. Bearer shares are permitted for international companies. However, the license application requires disclosure of the names and addresses of directors (who must be natural persons), the activities the corporation intends to conduct, the names of shareholders, and number of shares they will hold. Registered agents or service providers are required by law to know the names of beneficial owners. Failure to provide information or giving false information is punishable by a fine of U.S. $50,000. Offshore financial institutions are exempt from corporate income tax. All licensed institutions are required to have a physical presence, which means presence of at least a full-time senior officer and availability of all files and records. Shell companies are not permitted.

Antigua and Barbuda has five domestic casinos, which are required to incorporate as domestic corporations. Internet gaming companies are required to incorporate as IBCs, and as such are required to have a physical presence. Internet gaming sites are considered to have a physical presence when the primary servers and the key person are resident in Antigua and Barbuda. The Government of Antigua and Barbuda (GOAB) receives approximately U.S. $2.8 million per year from license fees and other charges related to the Internet gaming industry. A nominal free trade zone in the country seeks to attract investment in priority areas of the government. Casinos and sports book-wagering operations in Antigua and Barbuda's free trade zone are supervised by the Office of National Drug Control and Money Laundering Policy (ONDCP), which serves as the GOAB's financial intelligence unit (FIU), and the Directorate of Offshore Gaming (DOG), housed in the Financial Services Regulatory Commission (FSRC). The GOAB has adopted regulations for the licensing of interactive gaming and wagering, to address possible money laundering through client accounts of Internet gambling operations. The FSRC and DOG have also issued Internet gaming technical standards and guidelines. Internet gaming companies are required to submit quarterly and annual audited financial statements, enforce know-your-customer verification procedures, and maintain records relating to all gaming and financial transactions of each customer for six years. Suspicious activity reports from domestic and offshore gaming entities are sent to the ONDCP and FSRC.

The GOAB has not initiated a unified regulatory structure or uniform supervisory practices for its domestic and offshore banking sectors. Currently, the Eastern Caribbean Central Bank (ECCB) supervises Antigua and Barbuda's domestic banking sector. The Registrar of Insurance supervises and examines domestic insurance agencies. The director of the ONDCP—who was designated in 2003 as the Supervisory Authority created under the Money Laundering Prevention Act of 1996 (MLPA)—supervises all financial institutions for compliance with suspicious transaction reporting requirements. The FSRC is responsible for the regulation and supervision of all institutions licensed under the IBCA, including offshore banking and all aspects of offshore gaming. This includes issuing licenses for IBCs, maintaining the register of all corporations, and conducting examinations and reviews of offshore financial institutions as well as some domestic financial entities, such as insurance companies and trusts.

In the offshore sector, the IBCA requires that a corporate entity submit all books, minutes, cash, securities, vouchers, customer identification, and customer account records. Financial institutions are required to maintain records for six years after an account is closed. The IBCA provides for disclosure of confidential information pursuant to a request by the director of the ONDCP, and pursuant to an order of a court of competent jurisdiction in Antigua and Barbuda. In addition, section 25 of the MLPA states that the provisions of this Act shall have effect notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information imposed by any law or otherwise. The MLPA contains provisions for obtaining client and ownership information.

The MLPA, as amended, is the cornerstone of Antigua and Barbuda's anti-money laundering legislation. The MLPA makes it an offense for any person to obtain, conceal, retain, manage, or invest illicit proceeds or bring such proceeds into Antigua and Barbuda if that person knows or has reason to suspect that they are derived directly or indirectly from any unlawful activity. The MLPA covers institutions defined under the Banking Act, IBCA, and the Financial Institutions (NonBanking) Act, which include offshore banks, IBCs, money service businesses, credit unions, building societies, trust businesses, casinos, Internet gaming companies, and sports betting companies. Intermediaries such as lawyers and accountants are not included in the MLPA. The MLPA requires reporting entities to report suspicious activity suspected to be related to money laundering, whether a transaction was completed or not. There is no reporting threshold imposed on banks and financial institutions. Internet gaming companies, however, are required by the Interactive Gaming and Interactive Wagering Regulations to report to the ONDCP all payouts over U.S. $25,000.

The Office of National Drug Control and Money Laundering Policy Act, 2003 establishes the ONDCP as the GOAB's FIU. The ONDCP is an independent organization under the Ministry of National Security and is primarily responsible for the enforcement of the MLPA and for directing the GOAB's anti-money laundering efforts in coordination with the FSRC. The ONDCP assumes the role and fulfills the responsibilities of the Supervisory Authority as described in the MLPA, which includes the supervision of all financial institutions with respect to filing suspicious transaction reports (STRs). Additionally, the ONDCP Act authorizes the director to appoint officers to investigate narcotics trafficking, fraud, money laundering, and terrorist financing offenses. Auditors of financial institutions review their compliance program and submit a report to the ONDCP for analysis and recommendations. The ONDCP has no direct access to databases of financial institutions. Domestically, the ONDCP has a memorandum of understanding with the FSRC and is expected to sign another with the ECCB. Other memoranda of understanding have been drafted to cover all aspects of the ONDCP's relationship with the Royal Antigua and Barbuda Police Force, Customs, Immigration, and the Antigua and Barbuda Defense Force.

As of October 2007, the ONDCP had received 43 STRs (down from 52 in 2006), 11 of which were investigated. No arrests, prosecutions or convictions were reported by the GOAB in 2006 or 2007, although there were two arrests in 2005. Antigua and Barbuda has yet to prosecute a money laundering case.

Under the MLPA, a person entering or leaving the country is required to report to the ONDCP whether he or she is carrying U.S. $10,000 or more in cash or currency. In addition, all travelers are required to fill out a customs declaration form indicating if they are carrying in excess of U.S. $10,000 in cash or currency. If so, they may be subject to further questioning and possible search of their belongings by Customs officers. The GOAB Customs Department maintains statistics on cross-border cash reports and seizures for failure to report. This information is shared with the ONDCP and the police.

The Misuse of Drugs Act empowers the court to forfeit assets related to drug offenses. The ONDCP is responsible for tracing, seizing and freezing assets related to money laundering. The ONDCP has the ability to direct a financial institution to freeze property up to seven days, while it makes an application for a freeze order. If a charge is not filed or an application for civil forfeiture is not made within 30 days, the freeze order lapses. Convictions for a money laundering offense make it likely that an application for forfeiture will succeed unless the defendant can show that the property was acquired by legal means or the defendant's business was legitimate. Forfeited assets are placed into the Forfeiture Fund and can be used by the ONDCP for any other purpose. Approximately 20 percent of forfeited assets go to the Consolidated Fund at the Treasury.

The GOAB is currently working on asset forfeiture agreements with other jurisdictions. The director of ONDCP, with Cabinet approval, may enter into agreements and arrangements with authorities of a foreign State, which covers matters relating to asset sharing. There are asset sharing agreements with certain countries, while others are negotiated on an ad hoc basis. The ONDCP is presently overseeing the drafting of MOUs with a number of countries in Central America to enhance asset tracing, freezing and seizure. An MOU has recently been concluded with Canada. Regardless of its own civil forfeiture laws, currently the GOAB can only provide forfeiture assistance in criminal forfeiture cases.

In the past few years, the GOAB has frozen approximately U.S. $6 million in Antigua and Barbuda financial institutions as a result of U.S. requests and has repatriated approximately U.S. $4 million. The GOAB has frozen, on its own initiative, over U.S. $90 million believed to be connected to money laundering cases still pending in the United States and other countries. The GOAB reported seizing U.S. $420,236 in 2006 and U.S. $14,753 in 2007.

The GOAB enacted the Prevention of Terrorism Act 2001, amended in 2005, to implement the UN conventions on terrorism. The Act empowers the ONDCP to nominate any entity as a "terrorist entity" and to seize and forfeit terrorist funds. The law covers any finances in any way related to terrorism. The Act also provides the authority for the seizure of property used in the commission of a terrorist act; seizure and restraint of property that has been, is being or may be used to commit a terrorism offence; forfeiture of property on conviction of a terrorism offence; and forfeiture of property owned or controlled by terrorists. The Act requires financial institutions to report every three months on whether or not they are in possession of any property owned or controlled by or on behalf of a terrorist group. In addition, financial institutions must report every transaction that is suspected to be related to the financing of terrorism to the ONDCP. The Attorney General may revoke or deny the registration of a charity or nonprofit organization if it is believed funds from the organization are being used for financing terrorism. The GOAB circulates lists of terrorists and terrorist entities to all financial institutions in Antigua and Barbuda. No known evidence of terrorist financing has been discovered in Antigua and Barbuda to date. The GOAB does not believe indigenous alternative remittance systems exist in country, and has not undertaken any specific initiatives focused on the misuse of charities and nonprofit entities

The GOAB continues its bilateral and multilateral cooperation in various criminal and civil investigations and prosecutions. As a result of such cooperation, both the United States and Canada have shared forfeited assets with the GOAB on several occasions. The amended Banking Act 2004 enables the ECCB to share information directly with foreign regulators if a memorandum of understanding is established. In 1999, a Mutual Legal Assistance Treaty (MLAT) and an extradition

treaty with the United States entered into force. An extradition request related to a fraud and money laundering investigation remains pending under the treaty. The GOAB signed a Tax Information Exchange Agreement with the United States in December 2001 that allows the exchange of tax information between the two nations.

Antigua and Barbuda is a member of the Caribbean Financial Action Task Force (CFATF) and will undergo a mutual evaluation in early 2008. Antigua and Barbuda is also a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). The GOAB is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention against Terrorism. The ONDCP is a member of the Egmont Group.

The Government of Antigua and Barbuda has taken steps to combat money laundering and terrorist financing by passing relevant legislation that applies to both domestic and offshore financial institutions, and establishing a thorough regulatory regime. However, the GOAB should implement and enforce all provisions of its anti-money laundering and counter-terrorist financing legislation, including the supervision of its offshore sector and gaming industry. Despite the comprehensive nature of the law, Antigua and Barbuda has yet to prosecute a money laundering case and there are few arrests or prosecutions. The GOAB should conduct more thorough investigations that could lead to higher numbers of arrests, prosecutions, and convictions. Law enforcement and customs authorities should be trained to recognize money laundering typologies that fall outside the formal financial sector. The GOAB should continue its international cooperation, particularly with regard to the timely sharing of statistics, information related to offshore institutions, and seized assets.

Argentina

Argentina is neither an important regional financial center nor an offshore financial center. Money laundering related to narcotics trafficking, corruption, contraband, and tax evasion is believed to occur throughout the financial system, in spite of the efforts of the Government of Argentina (GOA) to stop it. The financial sector's continuing recovery from the 2001-02 financial crisis and post-crisis capital controls may have reduced the incidence of money laundering through the banking system. However, transactions conducted through nonbank sectors and professions, such as the insurance industry, financial advisors, accountants, notaries, trusts, and companies, real or shell, remain viable mechanisms to launder illicit funds. Tax evasion is the predicate crime in the majority of Argentine money laundering investigations. Argentina has a long history of capital flight and tax evasion, and Argentines hold billions of dollars offshore, much of it legitimately earned money that was never taxed.

In 2007, the Argentine Congress passed legislation criminalizing terrorism and terrorist financing. Law 26.268, "Illegal Terrorist Associations and Terrorism Financing", entered into effect in mid-July. The law amends the Penal Code and Argentina's anti-money laundering law, Law No. 25.246, to criminalize acts of terrorism and terrorist financing, and establish terrorist financing as a predicate offense for money laundering. Persons convicted of terrorism are subject to a prison sentence of five to 20 years, and those convicted of financing terrorism are subject to a five to 15 year sentence. The new law provides the legal foundation for Argentina's financial intelligence unit (the Unidad de Información Financiera, or UIF), Central Bank, and other regulatory and law enforcement bodies to investigate and prosecute such crimes. The adoption of counter-terrorist financing legislation effectively removes Argentina from the Financial Action Task Force's (FATF) follow-up process, which began in 2004 to address deficiencies in the GOA's anti-money laundering and counter-terrorist financing (AML/CTF) regime. With the passage of Law 26.268, Argentina also joins Chile, Colombia, and Uruguay as the only countries in South America to have criminalized terrorist financing.

On September 11, 2007, President Nestor Kirchner signed into force the National Anti-Money Laundering and Counter-Terrorism Finance Agenda. The overall goal of the National Agenda is to serve as a roadmap for fine-tuning and implementing existing money laundering and terrorist financing laws and regulations. The Agenda's 20 individual objectives focus on closing legal and regulatory loopholes and improving interagency cooperation. The next challenge is for Argentine law enforcement and regulatory institutions, including the Central Bank and UIF, to implement the National Agenda and aggressively enforce the newly strengthened and expanded legal, regulatory, and administrative measures available to them to combat financial crimes.

Argentina's primary anti-money laundering legislation is Law 25.246 of May 2000. Law 25.246 expands the predicate offenses for money laundering to include all crimes listed in the Penal Code, sets a stricter regulatory framework for the financial sectors, and creates the UIF under the Ministry of Justice and Human Rights. The law requires customer identification, record keeping, and reporting of suspicious transactions by all financial entities and businesses supervised by the Central Bank, the Securities Exchange Commission (Comisión Nacional de Valores, or CNV), and the National Insurance Superintendence (Superintendencia de Seguros de la Nación, or SSN). The law forbids institutions to notify their clients when filing suspicious transaction reports (STRs), and provides a safe harbor from liability for reporting such transactions. Reports that are deemed by the UIF to warrant further investigation are forwarded to the Attorney General's Office.

Law 26.087 of March 2006 amends and modifies Law 25.246 to address many previous deficiencies in Argentina's anti-money laundering regime. It makes substantive improvements to existing law, including lifting bank, stock exchange, and professional secrecy restrictions on filing suspicious activity reports; partially lifting tax secrecy provisions; clarifying which courts can hear requests to lift tax secrecy requests; and requiring court decisions within 30 days. Law 26.087 also lowers the standard of proof required before the UIF can pass cases to prosecutors, and eliminates the so-called "friends and family" exemption contained in Article 277 of the Argentine Criminal Code for cases of money laundering, while narrowing the exemption in cases of concealment. Overall, the law clarifies the relationship, jurisdiction, and responsibilities of the UIF and the Attorney General's Office, and improves information sharing and coordination. The law also reduces restrictions that have prevented the UIF from obtaining information needed for money laundering investigations by granting greater access to STRs filed by banks. However, the law does not lift financial secrecy provisions on records of large cash transactions, which are maintained by banks when customers conduct a cash transaction exceeding 10,000 pesos (approximately U.S. $3,200).

In September 2006, Congress passed Law 26.119, which amends Law 25.246 to modify the composition of the UIF. The law reorganized the UIF's executive structure, changing it from a five-member directorship with rotating presidency to a structure that has a permanent, politically-appointed president and vice-president. Law 26.119 also established a UIF Board of Advisors, comprised of representatives of key government entities, including the Central Bank, AFIP, the Securities Exchange Commission, the national counternarcotics secretariat (SEDRONAR), and the Justice, Economy, and Interior Ministries. The Board of Advisors' opinions on UIF decisions and actions are nonbinding.

The UIF has issued resolutions widening the range of institutions and businesses required to report suspicious or unusual transactions beyond those identified in Law 25.246. Obligated entities include the tax authority (Administración Federal de Ingresos Publicos, or AFIP), Customs, banks, currency exchange houses, casinos, securities dealers, insurance companies, postal money transmitters, accountants, notaries public, and dealers in art, antiques and precious metals. The resolutions issued by the UIF also provide guidelines for identifying suspicious or unusual transactions. All suspicious or unusual transactions, regardless of the amount, must be reported directly to the UIF. Obligated entities are required to maintain a database of information related to client transactions, including suspicious or unusual transaction reports, for at least five years and must respond to requests from the UIF for further information within 48 hours. As of September 30, 2007, the UIF had received 2851 reports of

suspicious or unusual activities since its inception in 2002, forwarded 165 suspected cases of money laundering to prosecutors for review, and assisted prosecutors with 121 cases. There have been only two money laundering convictions in Argentina since money laundering was first criminalized in 1989, and none since the passage of Law 25.246 in 2000.

The Central Bank requires by resolution that all banks maintain a database of all transactions exceeding 10,000 pesos, and periodically submit the data to the Central Bank. Law 25.246 requires banks to make available to the UIF upon request records of transactions involving the transfer of funds (outgoing or incoming), cash deposits, or currency exchanges that are equal to or greater than 10,000 pesos (approximately U.S. $3200). The UIF further receives copies of the declarations to be made by all individuals (foreigners or Argentine citizens) entering or departing Argentina with over U.S. $10,000 in currency or monetary instruments. These declarations are required by Resolutions 1172/2001 and 1176/2001, which were issued by the Argentine Customs Service in December 2001. In 2003, the Argentine Congress passed Law 22.415/25.821, which would have provided for the immediate fine of 25 percent of the undeclared amount, and for the seizure and forfeiture of the remaining undeclared currency and/or monetary instruments. However, the President vetoed the law because it allegedly conflicted with Argentina's commitments to MERCOSUR (Common Market of the Southern Cone).

Although the GOA has passed a number of new laws in recent years to improve its AML/CTF regime, Law 25.246 still limits the UIF's role to investigating only money laundering arising from seven specific crimes. The law also defines money laundering as an aggravation after the fact of the underlying crime. A person who commits a crime cannot be independently prosecuted for laundering money obtained from the crime; only someone who aids the criminal after the fact in hiding the origins of the money can be guilty of money laundering. Another impediment to Argentina's anti-money laundering regime is that only transactions (or a series of related transactions) exceeding 50,000 pesos (approximately U.S. $16,000) can constitute money laundering. Transactions below 50,000 pesos can constitute only concealment, a lesser offense.

In 2006 and 2007, the National Coordination Unit in the Ministry of Justice and Human Rights became fully functional, managing the government's AML/CTF efforts and representing Argentina at the FATF and the Financial Action Task Force for South America (GAFISUD). The Attorney General's special investigative unit set up to handle money laundering and terrorism finance cases began operations in 2007. The proposal by the Argentine Banking Superintendence to create a specialized anti-money laundering and counter-terrorism finance examination program is awaiting authorization and is not yet operational.

Argentina's Narcotics Law of 1989 authorizes the seizure of assets and profits, and provides that these or the proceeds of sales will be used in the fight against illegal narcotics trafficking. Law 25.246 provided that proceeds of assets forfeited under this law can also be used to fund the UIF.

Prior to the passage of terrorist financing legislation in June 2007, the Central Bank was the lead Argentine entity responsible for issuing regulations on combating the financing of terrorism. The Central Bank issued Circular A 4273 in 2005 (titled "Norms on 'Prevention of Terrorist Financing'"), requiring banks to report any detected instances of the financing of terrorism. The Central Bank regularly updates and modifies the original Circular. The Central Bank of Argentina also issued Circular B-6986 in 2004, instructing financial institutions to identify and freeze the funds and financial assets of the individuals and entities listed on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. It modified this circular with Resolution 319 in October 2005, which expands Circular B-6986 to require financial institutions to check transactions against the terrorist lists of the United Nations, United States, European Union, Great Britain, and Canada. No assets have been identified or frozen to date. The GOA and Central Bank assert that they

remain committed to freezing assets of terrorist groups identified by the United Nations if detected in Argentine financial institutions.

In December 2006, the U.S. Department of Treasury designated nine individuals and two entities that have provided financial or logistical support to Hizballah and operate in the territory of neighboring countries that border Argentina. This region is commonly referred to as the Tri-Border Area, between Argentina, Brazil, and Paraguay. According to the designation, the nine individuals have provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was previously designated by the U.S. Treasury in June 2004 for his support to Hizballah leadership. The two entities, Galeria Page and Casa Hamze, are located in Ciudad del Este, Paraguay, and have been used in generating or moving terrorist funds. The GOA joined the Brazilian and Paraguayan governments in publicly disagreeing with the designations, stating that the United States had not provided new information proving terrorist financing activity is occurring in the Tri-Border Area.

Working with the U.S. Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Argentina has established a Trade Transparency Unit (TTU). The TTU examines anomalies in trade data that could be indicative of customs fraud and international trade-based money laundering. The TTU has discovered a major discrepancy in import-export data and is supporting an on-going investigation. One key focus of the TTU, as well as of other TTUs in the region, will be financial crimes occurring in the Tri-Border Area. The creation of the TTU was a positive step towards complying with FATF Special Recommendation VI on terrorist financing via alternative remittance systems. Trade-based systems often use fraudulent trade documents and over and under invoicing schemes to provide counter valuation in value transfer (hawala) and settling accounts.

The GOA remains active in multilateral counternarcotics and international AML/CTF organizations. It is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering, the FATF and GAFISUD. The GOA is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the Inter-American Convention against Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Argentina participates in the "3 Plus 1" Security Group (formerly the Counter-Terrorism Dialogue) between the United States and the Tri-Border Area countries. The UIF has been a member of the Egmont Group since July 2003, and has signed memoranda of understanding regarding the exchange of information with a number of other financial intelligence units. The GOA and the USG have a Mutual Legal Assistance Treaty that entered into force in 1993, and an extradition treaty that entered into force in 2000.

With passage of counter-terrorist financing legislation and strengthened mechanisms available under Laws 26.119, 26.087, and 25.246, Argentina has the legal and regulatory capability to combat and prevent money laundering and terrorist financing. Furthermore, the new national anti-money laundering and counter-terrorist financing agenda provides the structure for the Government of Argentina to improve existing legislation and regulation, and enhance inter-agency coordination. The challenge now is for Argentine law enforcement and regulatory agencies and institutions, including the Ministry of Justice, Central Bank, and UIF, to implement the National Agenda and aggressively enforce the newly strengthened and expanded legal, regulatory, and administrative measures available to them to combat financial crimes. The GOA could further improve its legal and regulatory structure by enacting legislation to expand the UIF's role to enable it to investigate money laundering arising from all crimes, rather than just seven enumerated crimes; establishing money laundering as an autonomous offense; and eliminating the current monetary threshold of 50,000 pesos (approximately U.S. $16,000) required to establish a money laundering offense. To comply with the FATF recommendation on the regulation of bulk money transactions, Argentina should review the legislation vetoed in 2003 to find a way to regulate such transactions consistent with its MERCOSUR obligations. Other continuing priorities are the effective sanctioning of officials and institutions that fail to comply

with the reporting requirements of the law, the pursuit of a training program for all levels of the criminal justice system, and the provision of the necessary resources to the UIF to carry out its mission. There is also a need for increased public awareness of the problem of money laundering and its connection to narcotics, corruption, and terrorism.

Aruba

Aruba is an autonomous and largely self-governing Caribbean island under the sovereignty of the Kingdom of the Netherlands; foreign, defense and some judicial functions are handled at the Kingdom level. Due to its geographic location, casinos, and free trade zones, Aruba is both attractive and vulnerable to narcotics trafficking and money laundering.

Aruba has four commercial and two offshore banks, one mortgage bank, one credit union, an investment bank, a finance company, and eleven casinos. The island also has four registered money transmitters, two exempted U.S. money transmitters (Money Gram and Western Union), eight life insurance companies, 13 general insurance companies, four captive insurance companies, and 11 company pension funds. There are approximately 5,343 limited liability companies (NVs), of which 372 are offshore limited liability companies or offshore NVs, which may operate until 2008. In addition, there are approximately 2,763 Aruba Exempt Companies (AECs), which mainly serve as vehicles for tax minimization, corporate revenue routing, and asset protection and management.

The offshore NVs and the AECs are the primary methods used for international tax planning in Aruba. The offshore NVs pay a small percentage tax and are subject to more regulation than the AECs. The AECs pay an annual U.S. $280 registration fee and must have a minimum of U.S. $6,000 in authorized capital. Both offshore NVs and AECs can issue bearer shares. A local managing director is required for offshore NVs. The AECs must have a local registered agent, which must be a trust company.

In 2001, the Government of Aruba (GOA) made a commitment to the Organization for Economic Cooperation and Development (OECD), in connection with the Harmful Tax Practices initiative, to modernize fiscal legislation in line with OECD standards. In 2003, the GOA introduced a New Fiscal Regime (NFR) containing a dividend tax and imputation payment. As of July 1, 2003, the incorporation of low tax offshore NVs was halted. The NFR contains a specific exemption for the AECs. Nevertheless, as a result of commitments to the OECD, the regime was brought in line with OECD standards as of January 2006. As a result of the NFR, Aruba's offshore regime will cease operations by July 1, 2008.

Aruba currently has three designated free zones: Oranjestad Free Zone, Bushiri Free Zone, and the Barcadera Free Zone. The free zones are managed and operated by Free Zone Aruba (FZA) NV, a government limited liability company. Originally, only companies involved in trade or light industrial activities, including servicing, repairing and maintenance of goods with a foreign destination, could be licensed to operate within the free zones. However, State Ordinance Free Zones 2000 extended licensing to service-oriented companies (excluding financial services). Before being admitted to operate in the free zone, companies must submit a business plan along with personal data of managing directors, shareholders, and ultimate beneficiaries, and must establish a limited liability company founded under Aruban law intended exclusively for free zone operations. Aruba took the initiative in the Caribbean Financial Action Task Force (CFATF) to develop regional standards for free zones in an effort to control trade-based money laundering. The guidelines were adopted at the CFATF Ministerial Council in October 2001. Free Zone Aruba NV is continuing the process of implementing and auditing the standards that have been developed.

The Central Bank of Aruba is the supervisory and regulatory authority for credit institutions, insurance companies, company pension funds, and money transfer companies. The State Ordinance on the Supervision of Insurance Business (SOSIB) brought all insurance companies under the supervision of

the Central Bank. The insurance companies already active before the introduction of this ordinance were also required to obtain a license from the Central Bank. The State Ordinance on the Supervision of Money-Transfer Companies, effective August 2003, places money transfer companies under the supervision of the Central Bank. Quarterly reporting requirements became effective in 2004. A State Ordinance on the supervision of trust companies, which will designate the Central Bank as the supervisory authority, is currently being drafted.

Aruba's State Ordinance on the penalization money laundering of 1993 (AB 1993 no. 70) was repealed in 2006 through amendments to the Penal Code (AB 2006 no. 11). The GOA's anti-money laundering legislation extends to all crimes, and the Penal Code allows for conviction-based forfeiture of assets. All financial and nonfinancial institutions, which include banks, money remitters, brokers, insurance companies, and casinos, are obligated to identify clients that conduct transactions over 20,000 Aruban guilders (approximately U.S. $11,300), and report suspicious transactions to Aruba's financial intelligence unit (FIU), the Meldpunt Ongebruikelijke Transacties (MOT). Obligated entities are protected from liability for reporting suspicious transactions. The GOA's anti-money laundering requirements do not extend to such nonfinancial businesses and professions as lawyers, accountants, the real estate sector, or dealers in precious metals and jewels.

The MOT was established in 1996. The MOT is authorized to inspect all obligated entities for compliance with reporting requirements for suspicious transactions and the identification requirements for all financial transactions. The MOT is currently staffed by 10 employees. In 2007, the MOT received approximately 5,715 suspicious transaction reports (STRs), resulting in 180 investigations conducted and 47 cases transferred to the appropriate authorities. The MOT reports that very few STRs are filed by the gaming and insurance sectors.

In June 2000, Aruba enacted a State Ordinance making it a legal requirement to report the cross-border transportation of currency in excess of 20,000 Aruban guilders to the customs department. The law also applies to express courier mail services. Reports generated are forwarded to the MOT to review, and in 2007, approximately 820 such reports were submitted.

The MOT shares information with other national government departments. In April 2003, the MOT signed an information exchange agreement with the Aruba Tax Office, which is in effect and being implemented. The MOT and the Central Bank have also signed an information exchange memorandum of understanding (MOU), effective January 2006. The MOT is not linked electronically to the police or prosecutor's office. The MOT is a member of the Egmont Group and is authorized by law to share information with members of the Egmont Group through MOUs.

In 2004, the Penal Code of Aruba was modified to criminalize terrorism, the financing of terrorism, and related criminal acts. The GOA has a local committee comprised of officials from different departments of the Aruban Government, under the leadership of the MOT, to oversee the implementation of Financial Action Task Force (FATF) Forty Recommendations and Nine Special Recommendations on terrorist financing. The local committee, FATF Committee Aruba, reviewed the GOA anti-money laundering legislation and proposed, in accordance with the nine FATF Special Recommendations on Terrorist Financing, amendments to existing legislation and introduction of new laws. In 2007, the Parliament of Aruba approved the Ordinance on Sanctions 2006 (AB 2007 no. 24), to enhance the GOA's compliance with the FATF Special Recommendations. The GOA and the Netherlands formed a separate committee in 2004 to ensure cooperation of agencies within the Kingdom of the Netherlands in the fight against cross-border organized crime and international terrorism.

The bilateral agreement between the Netherlands and the United States Government (USG) regarding mutual cooperation in the tracing, freezing, seizure, and forfeiture of proceeds and instrumentalities of crime and the sharing of forfeited assets, which entered into force in 1994, applies to Aruba. The Mutual Legal Assistance Treaty between the Netherlands and the USG also applies to Aruba, though it

is not applicable to requests for assistance relating to fiscal offenses addressed to Aruba. The Tax Information Exchange Agreement with the United States, signed in November 2003, became effective in September 2004.

The Netherlands extended application of the 1988 UN Drug Convention to Aruba in 1999, the UN International Convention for the Suppression of the Financing of Terrorism in 2005, and the UN Convention against Transnational Organized Crime in 2007. The Netherlands has not yet extended application of the UN Convention against Corruption to Aruba. Aruba participates in the FATF and the FATF mutual evaluation program as part of the Kingdom of the Netherlands. The GOA is also a member of CFATF. The MOT became a member of the Egmont Group in 1997. Aruba is also a member of the Offshore Group of Banking Supervisors.

The Government of Aruba has shown a commitment to combating money laundering and terrorist financing by establishing an anti-money laundering and counter-terrorist financing regime that is generally consistent with the recommendations of the FATF and CFATF. Aruba should take additional steps to immobilize bearer shares under its fiscal framework and to enact its long-pending ordinance addressing the supervision of trust companies. The GOA should ensure that all obligated entities are fully complying with their anti-money laundering and counter-terrorist financing reporting requirements, and consider extending these reporting requirements to designated nonfinancial businesses and professions.

Australia

Australia is one of the major centers for capital markets in the Asia-Pacific region. In 2006-07, turnover across Australia's over-the-counter and exchange-traded financial markets was AU $120 trillion (approximately U.S. $108 trillion). Australia's total stock market capitalization is over AU $1.63 trillion (approximately U.S. $1.5 trillion), making it the eighth largest market in the world, and the third largest in the Asia-Pacific region behind Japan and Hong Kong. Australia's foreign exchange market is ranked seventh in the world by turnover, with the U.S. dollar and the Australian dollar the fourth most actively traded currency pair globally. While narcotics offences provide a substantial source of proceeds of crime, the majority of illegal proceeds are derived from fraud-related offences. A 2004 Australian Government estimate suggests that the amount of money laundered in Australia is in the vicinity of AU $4.5 billion (approximately U.S. $4 billion) per year.

The Government of Australia (GOA) has maintained a comprehensive system to detect, prevent, and prosecute money laundering. The last five years have seen a noticeable increase in activities investigated by Australian law enforcement agencies that relate directly to offenses committed overseas. Australia's system has evolved over time to address new money laundering and terrorist financing risks identified through continuous consultation between government agencies and the private sector.

In March 2005, the Financial Action Task Force (FATF) conducted its on-site Mutual Evaluation (FATFME) of Australia's anti-money laundering/counter-terrorist financing (AML/CTF) system. Australia was one of the first member countries to be evaluated under FATF's revised recommendations. The FATF's findings from the mutual evaluation of Australia were published in October 2005; and Australia was found to be compliant or largely complaint with just over half of the FATF Recommendations. The FATFME noted that although Australia "has a comprehensive money laundering offense . . . the low number of prosecutions . . . indicates . . . that the regime is not being effectively implemented."

In response, the GOA has committed to reforming Australia's AML/CTF system to implement the revised FATF Forty plus Nine recommendations. The Attorney General's Department (AGD) is

coordinating this process, now underway, which is significantly reshaping Australia's AML/CTF regime and bringing it into line with current international best practices.

Australia criminalized money laundering related to serious crimes with the enactment of the Proceeds of Crime Act 1987. This legislation also contained provisions to assist investigations and prosecution in the form of production orders, search warrants, and monitoring orders. It was superseded by two acts that came into force on January 1, 2003 (although proceedings that began prior to that date under the 1987 law will continue under that law). The Proceeds of Crime Act 2002 provides for civil forfeiture of proceeds of crime as well as for continuing and strengthening the existing conviction-based forfeiture scheme that was in the Proceeds of Crime Act 1987. The Proceeds of Crime Act 2002 also enables freezing and confiscation of property used in, intended to be used in, or derived from, terrorism offenses. It is intended to implement obligations under the UN International Convention for the Suppression of the Financing of Terrorism and resolutions of the UN Security Council relevant to the seizure of terrorism-related property. The Act also provides for forfeiture of literary proceeds where these have been derived from commercial exploitation of notoriety gained from committing a criminal offense.

The Proceeds of Crime (Consequential Amendments and Transitional Provisions) Act 2002 (POCA 2002), repealed the money laundering offenses that had previously been in the Proceeds of Crime Act 1987 and replaced them with updated offenses that have been inserted into the Criminal Code. The new offenses in Division 400 of the Criminal Code specifically relate to money laundering and are graded according both to the level of knowledge required of the offender and the value of the property involved in the activity constituting the laundering. As a matter of policy all very serious offenses are now gradually being placed in the Criminal Code. POCA 2002 also enables the prosecutor to apply for the restraint and forfeiture of property from proceeds of crime. POCA 2002 further creates a national confiscated assets account from which, among other things, various law enforcement and crime prevention programs may be funded. Recovered proceeds can be transferred to other governments through equitable sharing arrangements.

The Anti-Money Laundering and Counter-Terrorism Financing Act (AML/CTF Act) received Royal Assent on December 12, 2006 and was subsequently amended on April 12, 2007. The Act forms part of a legislative package that implements the first tranche of reforms to Australia's AML/CTF regulatory regime. The AML/CTF Act covers the financial sector, gambling sector, bullion dealers and any other professionals or businesses that provide particular 'designated services'. The Act imposes a number of obligations on entities that provide designated services, including customer due diligence, reporting obligations, record keeping obligations, and the requirement to establish and maintain an AML/CTF program. The AML/CTF Act implements a risk-based approach to regulation and the various obligations under the Act will be implemented over a two-year period (the final components will commence in December 2008). The legislative framework authorizes operational details to be settled in AML/CTF Rules, which will be developed by the Australian Transaction Reports and Analysis Centre (AUSTRAC) in consultation with industry. During 2006-07, AUSTRAC published 16 Rules relating to the AML/CTF Act, all developed in consultation with industry. AUSTRAC has also published a number of guidance notes for entities, including guidance regarding correspondent banking and providers of designated remittance services.

In 2007, the Australian Government began work on a second tranche of AML/CTF reforms, which will extend regulatory obligations to designated services provided by real estate agents, dealers in precious stones and metals, and specified legal, accounting, trust and company services (lawyers and accountants were included in the first tranche, but only where they compete with the financial sector and not for general services). The AGD has actively engaged with a broad cross-section of entities and interest groups regarding the proposed reforms.

The AML/CTF Act will gradually replace the Financial Transaction Reports Act 1988 (FTR Act) which currently operates concurrently to the AML/CTF Act, providing certain AML/CTF obligations until the various provisions of the new act are fully implemented. The FTR Act was enacted to combat tax evasion, money laundering, and serious crimes and it requires banks and nonbanking financial entities (collectively referred to as cash dealers) to verify the identities of all account holders and signatories to accounts, and to retain the identification record, or a copy of it, for seven years after the day on which the relevant account is closed. A cash dealer, or an officer, employee, or agent of a cash dealer, is protected against any action, suit, or proceeding in relation to the reporting process. The FTR Act also establishes reporting requirements for Australia's cash dealers. Required to be reported are: suspicious transactions, cash transactions equal to or in excess of AU $10,000 (approximately U.S. $9,000), and all international funds transfers into or out of Australia, regardless of value. The FTR Act also obliges any person causing an international movement of currency of Australian AU $10,000 (or a foreign currency equivalent) or more, into or out of Australia, either in person, as a passenger, by post or courier to make a report of that transfer. When the reporting obligations of the AML/CTF Act are implemented in December 2008, reporting entities will be required to report suspicious matters (which is broader than the current obligation to report suspect transactions), international funds transfers, and threshold transactions (more than AU $10,000), as well as being obliged to report details of their compliance with the AML/CTF legislation in the form of compliance reports.

FTR Act reporting also applies to nonbank financial institutions such as money exchangers, money remitters, stockbrokers, casinos and other gambling institutions, bookmakers, insurance companies, insurance intermediaries, finance companies, finance intermediaries, trustees or managers of unit trusts, issuers, sellers, and redeemers of travelers checks, bullion sellers, and other financial services licensees. Solicitors (lawyers) are also required to report significant cash transactions. Accountants do not have any FTR Act obligations. However, they do have an obligation under a self-regulatory industry standard not to be involved in money laundering transactions.

AUSTRAC was established under the FTR Act and is continued in existence by the AML/CTF Act. AUSTRAC is Australia's AML/CTF regulator and specialist financial intelligence unit (FIU). AUSTRAC collects, retains, compiles, analyzes, and disseminates financial transaction report (FTR) information. AUSTRAC also provides advice and assistance to revenue collection, social justice, national security, and law enforcement agencies, and issues guidelines to regulated entities regarding their obligations under the FTR Act, AML/CTF Act and the Regulations and Rules. Under the AML/CTF Act, AUSTRAC now has an expanded role as the national AML/CTF regulator with supervisory, monitoring and enforcement functions over a diverse range of business sectors. As such, AUSTRAC plays a central role in Australia's AML system both domestically and internationally. During the 2006-07 Australian financial year, AUSTRAC's FTR information was used in 1,529 operational matters. Results from the Australian Taxation Office (ATO) shows that the FTR information contributed to more than AU $87 million (approximately U.S. $77 million) in ATO assessments during the year. In 2006-07, AUSTRAC received 15,740,744 financial transaction reports, with 99.7 percent of the reports submitted electronically through the EDDS Web reporting system. AUSTRAC received 24,440 suspect transaction reports (SUSTRs), a decline of 1.5 percent following a 44.1 percent increase in the previous year.

During 2006-07, there was a significant increase in the total number of financial transaction reports received by AUSTRAC. Significant cash transactions reports (SCTRs) account for 17 percent of the total number of FTRs reported to AUSTRAC in 2006-07 and are reported by cash dealers and solicitors. In 2006-07, AUSTRAC received 2,675,050 SCTRs, an increase of 10.7 percent from the previous year. Cash dealers are also required to report all international funds transfer instructions (IFTIs) to AUSTRAC. Cash dealers reported 13,017,467 IFTIs to AUSTRAC during the financial year—a 14.0 percent increase from 2005-06. International currency transfer reports (ICTR) are primarily declared to the Australian Customs Service (ACS) by individuals when they enter or depart

from Australia. AUSTRAC received 23,351 ICTRs—a 15.9 percent decrease from the previous financial year. The Infringement Notice Scheme (INS) is a new penalty-based scheme introduced in 2007 under the AML/CTF Act to strengthen Australia's cross border movement procedures. An ACS or Australian Federal Police (AFP) officer can issue infringements at the border, where there is a failure to report a cross border movement of physical currency (CBM-PC) or the cross border movement of a bearer negotiable instrument (CBM-BNI; for example, travelers checks). The issuing of infringements for a failure to report a CBM-BNI is based on disclosure upon request rather than a declaration.

In April 2005, the Minister for Justice and Customs launched AUSTRAC's AML eLearning application. This application has been well received by cash dealers as a tool in providing basic education on the process of money laundering, the financing of terrorism, and the role of AUSTRAC in identifying and assisting investigations of these crimes. In December 2007, the new Minister for Home Affairs launched three new tools to assist industry comply with their AML/CTF obligations, in addition to updating the eLearning application. AUSTRAC Online is a secure Internet-based system which assists entities adhere to their reporting and regulatory obligations, and enables them to access their own information. The AUSTRAC Regulatory Guide is an instructional and 'living' document that assists industry to understand and meet their AML/CTF obligations, which will be updated as further AML/CTF Act provisions are implemented. Lastly, the AUSTRAC Typologies and Case Studies Report 2007 was published to raise industry awareness regarding potential AML/CTF risk factors, methods and typologies.

The Australian Prudential Regulation Authority (APRA) is the prudential supervisor of Australia's financial services sector. AUSTRAC regulates anti-money laundering/counter-terrorist financing (AML/CTF) compliance. The FATFME noted that a comprehensive system for AML/CTF compliance for the entire financial sector needed to be established by the GOA, as does an administrative penalty regime for AML/CTF noncompliance. As a result, the AML/CTF Act has given AUSTRAC a wide range of enhanced enforcement powers to complement the criminal sanctions that were available under the FTR Act. The AML/CTF Act now provides AUSTRAC with a civil penalty framework and other intermediate sanctions, such as enforceable undertakings, remedial directions and external audits for noncompliance. AUSTRAC has conducted very few compliance audits in recent years and places a great deal of emphasis on educating and continuously engaging the private sector regarding the evolution of AML/CTF regime and the attendant reporting requirements. During 2006-07, AUSTRAC conducted 78 educational visits to regulated entities to raise awareness of their obligations under the AML/CTF Act.

In June 2002, Australia passed the Suppression of the Financing of Terrorism Act 2002 (SFT Act). The aim of the SFT Act is to restrict the financial resources available to support the activities of terrorist organizations. This legislation criminalizes terrorist financing and substantially increases the penalties that apply when a person uses or deals with suspected terrorist assets that are subject to freezing. The SFT Act enhances the collection and use of financial intelligence by requiring cash dealers to report suspected terrorist financing transactions to AUSTRAC, and relaxes restrictions on information sharing with relevant authorities regarding the aforementioned transactions. The SFT Act also addresses commitments Australia has made with regard to the UNSCR 1373 and is intended to implement the UN International Convention for the Suppression of the Financing of Terrorism. Under this Act three accounts related to an entity listed on the UNSCR 1267 Sanction Committee's consolidated list, the International Sikh Youth Federation, were frozen in September 2002. While there have been some charges laid for acts in preparation of terrorism, there have been no terrorist financing charges or prosecutions under this legislation. The Security Legislation Amendment (Terrorism) Act 2002 also inserted new criminal offenses in the Criminal Code for receiving funds from, or making funds available to, a terrorist organization.

The Anti-Terrorism Act (No.2) 2005 (AT Act), which took effect on December 14, 2006, amends offenses related to the funding of a terrorist organization in the Criminal Code so that they also cover the collection of funds for or on behalf of a terrorist organization. The AT Act also inserts a new offense of financing a terrorist. The AML/CTF Act further addressed terrorist financing by placing an obligation on providers of designated remittance services to register with AUSTRAC.

Investigations of money laundering reside with the AFP and Australian Crime Commission (Australia's only national multi-jurisdictional law enforcement agency). The AFP is the primary law enforcement agency for the investigation of money-laundering and terrorist-financing offences in Australia at the Commonwealth level and has both a dedicated Financial Crimes Unit and well staffed Financial Investigative Teams (FIT) with primary responsibility for asset identification/restraint and forfeiture under the POCA 2002. The Commonwealth Director of Public Prosecutions (CDPP) prosecutes offences against Commonwealth law and to recover proceeds of Commonwealth crime. The main cases prosecuted by the CDPP involve drug importation and money laundering offences. One individual plead guilty to charges of money laundering in 2007, and legal proceedings are underway against a group of individuals arrested in late 2006 for involvement in a multi-million dollar money laundering operation.

In April 2003, the AFP established a Counter Terrorism Division to undertake intelligence-led investigations to prevent and disrupt terrorist acts. A number of Joint Counter Terrorism Teams (JCTT), including investigators and analysts with financial investigation skills and experience, are conducting investigations specifically into suspected terrorist financing in Australia. The AFP also works closely with overseas counterparts in the investigation of terrorist financing, and has worked closely with the FBI on matters relating to terrorist financing structures in South East Asia. In 2006, AFP introduced mandatory consideration of potential money laundering and crime proceeds into its case management processes, thereby ensuring that case officers explore the possibility of money laundering and crime proceeds actions in all investigations conducted by the AFP.

The GOA participates in the Strategic Alliance Group, also known as "5 Eyes". This group of five countries include representatives from the UK Serious Organized Crime Agency (SOCA), the Royal Canadian Mounted Police (RCMP), the Australian Federal Police (AFP), the New Zealand Police (NZP), the United States Immigration and Customs Enforcement (ICE), the Drug Enforcement Administration (DEA), and the Federal Bureau of Investigation (FBI), all of whom analyze various genres of criminal activity and exchange information and best practices.

Australia is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime and its protocol on migrant smuggling. In September 1999, a Mutual Legal Assistance Treaty between Australia and the United States entered into force. Australia participates actively in a range of international fora, including the FATF, the Pacific Islands Forum, and the Commonwealth Secretariat. Through its funding and hosting of the Secretariat of the Asia/Pacific Group on Money Laundering (APG), of which it serves as permanent co-chair, the GOA has elevated money laundering and terrorist financing issues to a priority concern among countries in the Asia/Pacific region. AUSTRAC is an active member of the Egmont Group of Financial Intelligence Units (FIUs). AUSTRAC has signed Exchange Instruments, mostly in the form of Memoranda of Understanding (MOUs) allowing the exchange of financial intelligence, with FinCEN and the FIUs of 48 other countries.

Following the bombings in Bali in October 2002, the Australian Government announced an AU $10 million (approximately U.S. $9 million) initiative managed by the Australian Agency for International Development (AusAID), to assist in the development of counterterrorism capabilities in Indonesia. As part of this initiative, the AFP has established a number of training centers such as the Jakarta Centre for Law Enforcement Cooperation. As part of Australia's broader regional assistance initiatives, AUSTRAC continued its South East Asia Counter Terrorism Program of providing capacity building

assistance to 10 South East Asian nations, to develop capacity in detecting and dealing with terrorist financing and money laundering. AUSTRAC is also providing further assistance in terms of IT system enhancements to the Indonesian FIU, PPATK (Indonesian Financial Transaction Reports and Analysis Center). In the Pacific region, AUSTRAC has developed and provided unique software and training for personnel to six Pacific island FIUs (Cook Islands, Solomon Islands, Samoa, Tonga, Palau and Vanuatu) to fulfill their domestic obligations and share information with foreign analogs. AUSTRAC is also undertaking IT Needs Assessments in Papua New Guinea and Nauru as part of its engagement with Pacific FIUs. AUSTRAC has worked collaboratively with the Fiji FIU to develop a larger scale information management system solution and enable the collection and analysis of financial transaction reports. The AGD received a grant of AUD7.7 million (approximately U.S. $6.9 million) over four years to establish the Anti-Money Laundering Assistance Team (AMLAT). AMLAT works cooperatively with the U.S. Department of State-funded Pacific Islands Anti-Money Laundering Program (PALP) to enhance AML/CTF regimes for Pacific island jurisdictions. The PALP, a four-year program, is managed by the Pacific Islands Forum (PIF) and employs residential mentors to develop or enhance existing AML/CTF regimes in the nonFATF member states of the PIF.

The GOA continues to pursue a comprehensive anti-money laundering/counter-terrorist financing regime that meets the objectives of the revised FATF Forty Recommendations and Nine Special Recommendations on Terrorist Financing. To enhance its AML/CTF regime, as noted in the FATF mutual evaluation, AUSTRAC has been provided with substantially increased powers to ensure compliance. There will be more on-site compliance audits and AUSTRAC can require regular compliance reports from reporting entities; can initiate monitoring orders and statutory demands for information and documents; can seek civil penalty orders, remedial directions and injunctions; and, can require a reporting entity to subject itself to an external audit of its AML/CTF program. The AML/CTF Act also provides for greater coordination amongst the regulatory agencies of its financial, securities and insurance sectors.

The GOA is continuing its exemplary leadership role in emphasizing money laundering/terrorist finance issues and trends within the Asia/Pacific region and its commitment to providing training and technical assistance to the jurisdictions in that region. Having significantly enhanced its increased focus on AML/CTF deterrence, the Government of Australia should increase its efforts to prosecute and convict money launderers.

Austria

As a major financial center, Austrian banking groups control significant shares of the banking markets in Central, Eastern and Southeastern Europe. According to Austrian National Bank statistics, Austria has one of the highest numbers of banks and bank branches per capita in the world, with about 870 banks and one bank branch for every 1,605 people. Austria is not an offshore jurisdiction. Money laundering occurs within the Austrian banking system as well as in nonbank financial institutions and businesses. The percentage of undetected organized crime may be enormous, with much of it reportedly coming from the former Soviet Union. Money laundered by organized crime groups derives primarily from serious fraud, corruption, narcotics trafficking and trafficking in persons. Criminal groups use various instruments to launder money, including informal money transfer systems, the Internet, and offshore companies.

Austria criminalized money laundering in 1993. Predicate offenses include terrorist financing and other serious crimes. Regulations are stricter for money laundering by criminal organizations and terrorist “groupings,” because in such cases the law requires no proof that the money stems directly or indirectly from prior offenses.

Amendments to the Customs Procedures Act and the Tax Crimes Act of 2004 and 2006 address the problem of cash couriers and international transportation of currency and monetary instruments from

illicit sources. Austrian customs authorities do not automatically screen all persons entering Austria for cash or monetary instruments. However, to implement the European Union (EU) regulation on controls of cash entering or leaving the EU, the Government of Austria (GOA) requires an oral or written declaration for cash amounts of 10,000 euros (approximately U.S. $13,500) or more. This declaration, which includes information on source and use, must be provided when crossing an external EU border. In December 2007 the new Schengen countries were adopted, making it possible to travel from Estonia to Portugal without border controls. Spot checks for currency at border crossings and on Austrian territory do occur. Customs officials have the authority to seize suspect cash, and will file a report with the Austrian Financial Intelligence Unit (FIU) in cases of suspected money laundering. Austria has no database for cash smuggling reports.

The Banking Act of 1994 creates customer identification, record keeping, and staff training obligations for the financial sector. Entities subject to the Banking Act include banks, leasing and exchange businesses, safe custody services, and portfolio advisers. The law requires financial institutions to identify all customers when beginning an ongoing business relationship. In addition, the Banking Act requires customer identification for all transactions of more than 15,000 euros (U.S. $20,250) for customers without a permanent business relationship with the bank. Identification procedures require that all customers appear in person and present an official photo identification card. These procedures also apply to trustees of accounts, who must disclose the identity of the account beneficiary. Procedures allow customers to carry out nonface-to-face transactions, including Internet banking, on the basis of a secure electronic signature or a copy of a picture ID and a legal business declaration submitted by registered mail.

To implement the EU's Third Money Laundering Directive (Directive 2005/60/EC), an amendment to the Banking Act has been in effect since January 1, 2008. The new regulations will tighten customer identification procedures by requiring renewed identification in case of doubt about previously obtained ID documents or data as well as requiring personal appearances of trustees. Regulations will also require institutions to determine the identity of beneficial owners and introduce risk-based customer analysis for all customers. Financial institutions must also begin to implement these requirements in their subsidiaries abroad. The 2008 Banking Act amendment also broadens the reporting requirement by replacing "well-founded suspicion" with "suspicion or probable reason to assume" that a transaction serves the purpose of money laundering or terrorist financing or that a customer has violated his duty to disclose trustee relationships.

Enhanced due diligence obligations will apply if the customer has not been physically present for identification purposes (for example, nonface-to-face transactions, Internet banking), and with regard to cross-border correspondent banking relationships. In cases where a financial institution is unable to establish customer identity or obtain other required information on the business relationship, it must decline to enter into a business relationship or process a transaction, or terminate the business relationship. The institution must also consider reporting the case to the FIU. The law also requires financial institutions to keep records on customers and account owners. The Securities Supervision Act of 1996, which covers trade of securities, shares, money market instruments, options, and other instruments listed on an Austrian stock exchange or any regulated market in the EU, refers to the Banking Act's identification regulations. The Insurance Act of 1997 includes similar regulations for insurance companies underwriting life policies. An amendment to the Insurance Act of 1997, in effect since January 1, 2008, tightened record keeping requirements for insurance companies.

The Banking Act includes a due diligence obligation, and the law holds individual bankers responsible if their institutions launder money. The Banking Act and other laws provide "safe harbor" to obligated reporting individuals, including bankers, auctioneers, real estate agents, lawyers, and notaries. The law excuses those who report from liability for damage claims resulting from delays in completing suspicious transactions. Although there is no requirement for banks to report large currency

transactions, unless they are suspicious, the FIU provides outreach and information to banks to raise awareness of large cash transactions.

On January 1, 2008, responsibility for on-site inspections of banks, exchange businesses and money transmitters moved from the Financial Market Authority (FMA) to the Austrian National Bank. These on-site inspections, including inspections at subsidiaries abroad, are all-inclusive, and will require analysis of financial flows and compliance with money laundering regulations. Money remittance businesses require a banking license from the FMA and are subject to supervision. Informal remittance systems such as hawala exist in Austria, but are subject to administrative fines for carrying out banking business without a license. On its website, the FMA has published several circular letters with details on customer identification, money laundering and terrorist financing regulations, and reporting of suspicious transactions.

The Austrian Gambling Act, the Business Code, and the Austrian laws governing lawyers, notaries, and accounting professionals introduce additional money laundering and terrorist financing regulations concerning customer identification, reporting of STRs and record keeping for dealers in high value goods, auctioneers, real estate agents, casinos, lawyers, notaries, certified public accountants, and auditors. To implement the EU's Third Money Laundering Directive, amendments to the Stock Exchange Act, the Securities Supervision Act, the Insurance Act, and Austrian laws governing lawyers and notaries are in effect since January 1, 2008. Amendments to the Gambling Act and the law governing accounting professionals are pending approval. These introduced stricter regulations regarding customer identification procedures, including requiring customer identification for all transactions of more than 15,000 euros (U.S. $20,250) for customers without a permanent business relationship. Lawyers and notaries are exempt from their reporting obligation for information obtained in course of judicial proceedings or providing legal advice to a client unless the client has sought legal advice for laundering money or financing terrorism. The Business Code amendment will require all traders, not only dealers in high-value goods, auctioneers and real estate agents, to establish the identity of customers for cash transactions of 15,000 euros (U.S. $20,250) or more.

The EU regulation on wire transfers (EC 1781/2006) entered into force on January 1, 2007, and became immediately and directly applicable in Austria. Since November 1, 2007, financial institutions require customer identification for all cash fund transfers of 1,000 euros (U.S. $1,350) or more.

Austria's financial intelligence unit (FIU) is located within the Austrian Interior Ministry's Bundeskriminalamt (Federal Criminal Intelligence Service). The FIU is the central repository of suspicious transaction reports (STRs) and has police powers. During the first ten months of 2007, the FIU received approximately 830 STRs from banks—a significant increase from the 692 suspicious transactions reported in 2006. The FIU has also responded to requests for information from Interpol, Europol, other FIUs, and other authorities. Although no information for 2007 convictions is currently available, there were three money laundering convictions in 2006.

Since 1996, legislation has provided for asset seizure and the forfeiture of illegal proceeds. The banking sector generally cooperates with law enforcement efforts to trace funds and seize illicit assets. Austria has regulations in the Code of Criminal Procedure that are similar to civil forfeiture in the U.S. In connection with money laundering, organized crime and terrorist financing, all assets are subject to seizure and forfeiture, including bank assets, other financial assets, cars, legitimate businesses, and real estate. Courts may freeze assets in the early stages of an investigation. In the first ten months of 2007, Austrian courts froze assets worth more than 100 million euros (U.S. $135 million).

The Extradition and Judicial Assistance Law provides for expedited extradition; expanded judicial assistance; acceptance of foreign investigative findings in the course of criminal investigations; and enforcement of foreign court decisions. Austria's strict bank secrecy regulations can be lifted in cases of suspected money laundering. Moreover, bank secrecy does not apply in cases in which banks and other financial institutions must report suspected money laundering.

The 2002 Criminal Code Amendment (Federal Law Gazette number I/134 of August 13, 2002) introduced the following criminal offense categories: terrorist "grouping," terrorist criminal activities, and financing of terrorism, in line with United Nations Security Council Resolution 1373. The Criminal Code defines "financing of terrorism" as a separate criminal offense category, punishable in its own right. Terrorist financing is also included in the list of criminal offenses subject to domestic jurisdiction and punishment, regardless of the laws where the act occurred. The money laundering offense is also expanded to terrorist "groupings." The Federal Economic Chamber's Banking and Insurance Department, in cooperation with all banking and insurance associations, has published an official Declaration of the Austrian Banking and Insurance Industries to Prevent Financial Transactions in Connection with Terrorism. The law also gives the judicial system the authority to identify, freeze, and seize terrorist financial assets. Asset forfeiture regulations cover funds collected or held available for terrorist financing, and permit freezing and forfeiture of all assets that are in Austria, regardless of whether the crime was committed in Austria or the whereabouts of the criminal.

The Austrian authorities distribute to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, as well as the list of Specially Designated Global Terrorists that the United States has designated pursuant to E.O. 13224, and those distributed by the EU to members. According to the Ministry of Justice and the FIU, no accounts found in Austria have shown any links to terrorist financing. The FIU immediately shares all reports on suspected terrorist financing with the Austrian Interior Ministry's Federal Agency for State Protection and Counterterrorism (BVT). Figures on suspected terrorist financing transaction reports are not available. There were no convictions for terrorist financing in 2006.

The GOA has undertaken important efforts that may help thwart the misuse of charitable or nonprofit entities as conduits for terrorist financing. The GOA has implemented the Financial Action Task Force (FATF) Special Recommendation on Terrorist Financing regarding nonprofit organizations. The Law on Associations covers charities and all other nonprofit associations in Austria. The law regulates the establishment of associations, bylaws, organization, management, association registers, appointment of auditors, and detailed accounting requirements. Since January 1, 2007, associations whose finances exceed a certain threshold are subject to special provisions. Each association must appoint two independent auditors and must inform its members about its finances and the auditor's report. Associations with a balance sheet exceeding 3 million euros (U.S. $4.05 million) or annual donations of more than 1 million euros (U.S. $1.35 million) must appoint independent auditors to review and certify the financial statements. Public collection of donations requires advance permission from the authorities. The Central Register of Associations offers basic information on all registered associations in Austria free of charge via the Internet. Stricter customer identification procedures and due diligence obligations for financial institutions will implement an additional layer to monitor charities and nonprofit organizations, particularly in cases where business relationships suggest that they could be connected to money laundering or terrorist financing.

The Law on Responsibility of Associations maintains criminal responsibility for all legal entities, general and limited commercial partnerships, registered partnerships and European Economic Interest Groupings, but not charitable or nonprofit entities. The law covers all crimes listed in the Criminal Code, including corruption, money laundering and terrorist financing.

The GOA is generally cooperative with U.S. authorities in money laundering cases. Austria has not enacted legislation that provides for sharing forfeited narcotics-related assets with other governments. However, a bilateral U.S.-Austria agreement on sharing of forfeited assets is pending parliamentary ratification. In addition to the exchange of information with home country supervisors permitted by the EU, Austria has defined this information exchange in agreements with more than a dozen other EU members including the United Kingdom, and with Croatia.

Austria is a party to the 1988 UN Drug Convention, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Austria is a member of the EU and the FATF and will undergo a FATF mutual evaluation in 2008. The FIU is a member of the Egmont Group.

The Government of Austria has implemented a viable comprehensive anti-money laundering and counter-terrorist financing regime. The GOA should ensure that it provides the FIU and law enforcement the resources that they require to effectively perform their functions. The GOA should introduce safe harbor legislation protecting FIU and other government personnel from damage claims as a result of their work. Customs authorities should continue spot-checking operations for bulk cash smuggling despite the lack of border controls with Austria's neighbors. The GOA also should consider enacting legislation that will provide for asset sharing with other governments.

Bahamas

The Commonwealth of The Bahamas is an important regional and offshore financial center. The financial services sector provides a vital economic contribution to The Bahamas, accounting for approximately 15 percent of the country's gross domestic product. The U.S. dollar circulates freely in The Bahamas, and is accepted everywhere on par with the Bahamian dollar. Money laundering in The Bahamas is primarily related to financial fraud and the proceeds of drug trafficking. Illicit proceeds from drug trafficking usually take the form of cash or are quickly converted into cash. The strengthening of anti-money laundering laws has made it increasingly difficult for most drug traffickers to deposit large sums of cash. As a result, drug traffickers store extremely large quantities of cash in security vaults at properties deemed to be safe houses. Other money laundering trends include the purchase of real estate, large vehicles and jewelry, as well as the processing of money through a complex web of legitimate businesses and international business companies.

There are presently four casinos operating in The Bahamas, with three new casinos scheduled to open within the next few years. Cruise ships that overnight in Nassau may operate casinos. Reportedly, there are over ten Internet gaming sites based in The Bahamas, although Internet gambling is illegal in The Bahamas. Under Bahamian law, Bahamian residents are prohibited from gambling. The Gaming Board of The Bahamas issues licenses and has anti-money laundering oversight for the gaming industry. Freeport is the only free trade zone in The Bahamas. There are no indications that it is used to launder money.

The financial sector of The Bahamas is comprised of onshore and offshore financial institutions, which include banks and trust companies, insurance companies, securities firms and investment funds administrators, financial and corporate service providers, cooperatives, societies, and designated nonfinancial businesses and professions (including accountants, lawyers, real estate agents, and casinos). The Bahamas has six financial sector regulators: the Central Bank of the Bahamas, which is responsible for licensing and supervision of banks and trust companies; the Securities Commission, responsible for regulating the securities and investment funds industry; the Compliance Commission, which supervises financial sector businesses that are not subject to prudential supervision such as lawyers and accountants; the Inspector of Financial and Corporate Service Providers (IFCSP), which licenses and supervises company incorporation agents and other financial service providers; the Director of Societies, which regulates credit unions and societies; and the Registrar of Insurance Companies. These six regulators comprise the Group of Financial Sector Regulators (GFSR). The GFSR meets on a monthly basis to facilitate information sharing between domestic and foreign regulators and discuss cross-cutting regulatory issues, including anti-money laundering.

The Central Bank Act 2000 (CBA) and The Banks and Trust Companies Regulatory Act 2000 (BTCRA) enhance the supervisory powers of the Central Bank to, among other things, conduct on-site and off-site inspections of banks and enhance cooperation between overseas regulatory authorities and the Central Bank. The BTCRA expands the licensing criteria for banks and trust companies, enhances the supervisory powers of the Inspector of Banks and Trust Companies, and enhances the role of the Central Bank Governor. These expanded rights include the right to deny licenses to banks or trust companies deemed unfit to transact business in The Bahamas. Draft legislation has been prepared to provide the Central Bank with the mandate to supervise nonbank money transmission businesses. Currently, these institutions are licensed and regulated by the IFCSP, and are supervised by the Compliance Commission for anti-money laundering and counter-terrorist financing purposes.

In 2001, the Central Bank enacted a physical presence requirement that means "managed banks" (those without a physical presence but which are represented by a registered agent such as a lawyer or another bank) must either establish a physical presence in The Bahamas (an office, separate communications links, and a resident director) or cease operations. The transition to full physical presence is complete. Some industry sources have suggested that this requirement has contributed to a decline in banks and trusts from 301 in 2003 to 139 as of June 30, 2007.

The International Business Companies Act 2000 and 2001 (Amendments) enacts provisions that abolish bearer shares, require international business companies (IBCs) to maintain a registered office in The Bahamas, and require the registered office to maintain a copy of the names and addresses of the directors and officers and a copy of the shareholders register. A copy of the register of directors and officers must also be filed with the Registrar General. There are approximately 115,000 registered IBCs, only 42,000 of which are active. Only banks and trust companies licensed under the BTCRA and financial and corporate service providers licensed under the Financial Corporate Service Providers Act (FCSPA) may provide registration, management, administration, registered agents, registered offices, nominee shareholders, and officers and directors for IBCs. As of year-end 2007, there were 139 banks and trust companies in the Bahamas.

The Proceeds of Crime Act 2000 criminalizes money laundering. The Financial Transaction Reporting Act 2000 (FTRA) establishes "know your customer" (KYC) requirements. By December 31, 2001, financial institutions were obliged to verify the identities of all their existing account holders and of customers without an account who conduct transactions over $10,000. All new accounts established in 2001 or later have to be in compliance with KYC rules before they are opened. As of October 2006, the Central Bank reported full compliance with KYC requirements. All nonverified accounts have been frozen.

The Bahamas Financial Intelligence Unit (FIU), established by the FIU Act 2000, operates as an independent administrative body under the Office of the Attorney General, and is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs). The FTRA requires financial and nonfinancial institutions to report suspicious transactions to the FIU when the institution suspects or has reason to believe that any transaction involves the proceeds of crime. The FIU Act 2000 protects obligated entities from criminal or civil liability for reporting transactions. Financial institutions are required by law to maintain records related to financial transactions for no less than five years. If money laundering is suspected, the FIU will disseminate STRs to the Tracing and Forfeiture/Money Laundering Investigation Section (T&F/MLIS) of the Drug Enforcement Unit (DEU) of the Royal Bahamas Police Force for investigation and prosecution in collaboration with the Office of the Attorney General. The FIU receives approximately 190 STRS annually.

The FIU has the administrative power to issue an injunction to stop anyone from completing a transaction for a period of up to three days upon receipt of an STR. In 2006, there were eight cases of asset restraints as a result of STRs. One led to the issuance of a restraint order by the Supreme Court of The Bahamas, in which approximately $2 million was restrained.

The FIU is responsible for publishing guidelines to advise entities of their reporting obligations. In March 2007, the FIU revised its guidelines to incorporate terrorist financing reporting requirements. These new guidelines give financial institutions information on requirements that must be met, how to identify suspicious transactions, and how to report these transactions to the FIU. In February 2008, the FIU plans to implement the National Strategy to Prevent Money Laundering. The Strategy arose in response to recommendations from the Financial Action Task Force (FATF) and will provide a means to ensure compliance with international anti-money laundering standards.

Between January 2000 and September 2006, 17 individuals were charged with money laundering by the T&F/MLIS, leading to seven convictions. Seven defendants await trial, while two defendants fled the jurisdiction prior to trial. There are no statistics available on prosecutions or convictions for 2007.

As a matter of law, the Government of the Commonwealth of the Bahamas (GOB) seizes assets derived from international drug trade and money laundering. The banking community has cooperated with these efforts. During 2007, nearly $8 million in cash and assets were seized or frozen. The seized items are in the custody of the GOB. Some are in the process of confiscation while some remain uncontested. Seized assets may be shared with other jurisdictions on a case-by-case basis.

In 2004, the Anti-Terrorism Act (ATA) was enacted to implement the provisions of the UN International Convention for the Suppression of the Financing of Terrorism. In addition to formally criminalizing terrorism and making it a predicate crime for money laundering, the law provides for the seizure and confiscation of terrorist assets, reporting of suspicious transactions related to terrorist financing, and strengthening of existing mechanisms for international cooperation. In 2006, the FIU received two suspicious transaction reports relating to terrorist financing from financial institutions. The reports were analyzed with one forwarded to the police for further investigation.

The Bahamas is a member of the Offshore Group of Banking Supervisors and the Caribbean Financial Action Task Force (CFATF). The Bahamas underwent a CFATF mutual evaluation in June 2006. The report, which was presented at the November 2007 CFATF plenary, will be finalized by January 2008 and published electronically via CFATF's website.

The Bahamas is a party to the UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention against Corruption. The Bahamas has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOB has neither signed nor ratified the UN Convention against Corruption. The FIU has been an active participant within the Egmont Group since becoming a member in 2001, and is currently one of the two regional representatives for the Americas. The Bahamas FIU has the ability to sign memoranda of understanding (MOU) with other counterpart FIUs to exchange information. The Bahamas has a Mutual Legal Assistance Treaty with the United States, which entered into force in 1990, and agreements with the United Kingdom and Canada. The Attorney General's Office for International Affairs manages requests for mutual legal assistance. The Bahamas has an information exchange agreement with the U.S. Securities and Exchange Commission to ensure that requests can be completed in an efficient and timely manner.

The Government of the Commonwealth of The Bahamas has enacted substantial reforms to reduce its vulnerability to money laundering and terrorist financing. The GOB should continue to enhance its anti-money laundering and counter-terrorist financing regime by implementing the National Strategy on the Prevention of Money Laundering. It should also ensure that there is a registry of the beneficial owners of all entities licensed in its offshore financial center. The Bahamas should also provide adequate resources to its law enforcement, prosecutorial and judicial entities to ensure that investigations and prosecutions are satisfactorily completed and requests for international cooperation are efficiently processed. The GOB should become a party to the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the Inter-American Convention against Terrorism.

Bahrain

Bahrain has one of the most diversified economies in the Gulf Cooperation Council (GCC). In contrast to most of its neighbors, oil accounted for only 21.3 percent of Bahrain's gross domestic product (GDP) in 2006. Bahrain has promoted itself as an international financial center in the Gulf region. It hosts a mix of: 387 diverse financial institutions, including 190 banks, of which 54 are wholesale banks (formerly referred to as off-shore banks or OBUs); 42 investment banks; and 26 commercial banks, of which 19 are foreign-owned. There are 31 representative offices of international banks. Bahrain has 34 Islamic banks and financial institutions. There are 21 moneychangers and money brokers, and several other investment institutions, including 85 insurance companies. The vast network of Bahrain's banking system, along with its geographical location in the Middle East as a transit point along the Gulf and into Southwest Asia, may attract money laundering activities. It is thought that the greatest risk of money laundering stems from questionable foreign proceeds that transit Bahrain.

In January 2001, the Government of Bahrain (GOB) enacted an anti-money laundering law that criminalizes the laundering of proceeds derived from any predicate offense. The law stipulated punishment of up to seven years in prison, and a fine of up to one million Bahraini dinars (approximately$2.66 million) for convicted launderers and those aiding or abetting them. If organized criminal affiliation, corruption, or a disguised origin of proceeds is involved, the minimum penalty is a fine of at least 100,000 dinars (approximately $266,000) and a prison term of not less than five years.

On August 12, 2006, Bahrain passed Law 54/2006, amending the anti-money laundering law. Law 54 criminalizes the undeclared transfer of money across international borders for the purpose of money laundering or in support of terrorism. Anyone convicted under the law of collecting or contributing funds, or otherwise providing financial support to a group or persons who practice terrorist acts, whether inside or outside Bahrain, will be subject to imprisonment for a minimum of ten years in prison up to a maximum of a life sentence. The law also stipulates a fine of between the equivalent of $26,700 and $1.34 million. Law 54 also codified a legal basis for a disclosure system for cash couriers, though supporting regulations must still be enacted.

A controversial feature of the new law is a revised definition of terrorism that is based on the Organization of the Islamic Conference definition. Article 2 excludes from the definition of terrorism acts of struggle against invasion or foreign aggression, colonization, or foreign supremacy in the interest of freedom and the nation's liberty.

Under the original anti-money laundering law, the Bahrain Monetary Agency (BMA), principal financial sector regulator and de-facto central bank, issued regulations requiring financial institutions to file suspicious transaction reports (STRs), to maintain records for a period of five years, and to provide ready access for law enforcement officials to account information. The BMA became the Central Bank of Bahrain (CBB) in 2006. Immunity from criminal or civil action is given to those who report suspicious transactions. Even prior to the enactment of the new anti-money laundering law, financial institutions were obligated to report suspicious transactions greater than 6,000 dinars (approximately $15,000) to the BMA/CBB. The current requirement for filing STRs stipulates no minimum thresholds and since 2005 the BMA/CBB has had a secure online website that banks and other financial institutions can use to file STRs.

In September 2006, Law 64/2006 replaced the BMA, which had acted as the de-facto central bank, with the CBB. Law 64 consolidated several laws that had previously governed the various segments of the financial services industry. Under the law, the CBB enjoys reinforced operational independence and enhanced enforcement powers. Part 9 of the law, for example, outlines investigational and administrative proceedings at the CBB's disposal to ensure licensee compliance with rules and regulations. The CBB's compliance arm was upgraded from a unit to a directorate.

The original law also provided for the formation of an interagency committee to oversee Bahrain's anti-money laundering regime. Accordingly, in June 2001, the Policy Committee for the Prohibition and Combating of Money Laundering and Terrorist Financing was established and assigned the responsibility for developing anti-money laundering policies and guidelines. In early 2006, the chairmanship of the Policy Committee was transferred from the Ministry of Finance to the CBB. The committee's membership was also expanded, to comprise representatives from the Ministries of Finance, Industry and Commerce, Interior, and Social Development; the Directorates of Customs and Legal Affairs; the Office of Public Prosecution; the National Security Agency; the Bahrain Stock Exchange; and the Central Bank of Bahrain.

In addition, the original law provided for the creation of the Anti-Money Laundering Unit (AMLU) as Bahrain's financial intelligence unit (FIU). The AMLU, which is housed in the Ministry of Interior, is empowered to receive reports of money laundering offenses; conduct investigations; implement procedures relating to international cooperation under the provisions of the law; and execute decisions, orders, and decrees issued by the competent courts in offenses related to money laundering. The AMLU became a member of the Egmont Group of FIUs in July 2003.

The AMLU receives STRs from banks and other financial institutions, investment houses, broker/dealers, moneychangers, insurance firms, real estate agents, gold dealers, financial intermediaries, and attorneys. Financial institutions must also file STRs with the Central Bank, which supervises these institutions. Nonfinancial institutions are required under a Ministry of Industry and Commerce (MOIC) directive to also file STRs with that ministry. The Central Bank analyzes the STRs, of which it receives copies, as part of its scrutiny of compliance by financial institutions with anti-money laundering and counter terrorist financing (AML/CTF) regulations, but it does not independently investigate the STRs (responsibility for investigation rests with the AMLU). The Central Bank may assist the AMLU with its investigations where special banking expertise is required.

The Central Bank of Bahrain is the regulator for other nonbanking financial institutions including insurance companies, exchange houses, and capital markets. The Central Bank inspected seven insurance companies in 2006 and had conducted eight more inspections by September 2007. Additional insurance industry inspections are scheduled for 2008. Anti-money laundering regulations for investment firms and securities brokers were revised in April 2006.

In November 2007, the MOIC published new anti-money laundering guidelines, which govern designated nonfinancial businesses and professions (DNFBPs). The MOIC has also announced an increased focus on enforcement, noting some 300 visits to DNFBPs in 2005, including car dealers, jewelers, and real estate agencies. By November 2006, the MOIC had conducted an additional 274 enforcement follow-up visits. A total of 140 of these have been assigned an MOIC compliance officer as a result. The MOIC has also increased its inspection team staff from four to seven.

The MOIC system of requiring dual STR reporting to both it and the AMLU mirrors the Central Bank's system. Good cooperation exists between MOIC, Central Bank, and AMLU, with all three agencies describing the double filing of STRs as a backup system. The AMLU and Central Bank's compliance staff analyze the STRs and work together on identifying weaknesses or criminal activity, but it is the AMLU that must conduct the actual investigation and forward cases of money laundering and terrorist financing to the Office of the Public Prosecutor.

From January through December 2007, the AMLU has received and investigated 183 STRs, 39 of which have been forwarded to the courts for prosecution. The GOB completed its first successful money laundering prosecution in May 2006. The prosecutions resulted in the convictions of two ex-patriot felons with sentences of one and three years and fines of $380 and $1900 respectively.

In August of 2006, Bahrain passed its first law specifically criminalizing terrorism and establishing harsh penalties for terrorist crimes including financing and money laundering in support of terrorism.

The government used this law to bring charges against five suspects in October 2007. The five face a range of charges, including the financing of terrorism. As of January 2008, trial proceedings remained ongoing.

Bahrain is moving ahead with plans to establish a special court to try financial crimes, and judges are undergoing special training to handle such crimes. Six Bahraini judges will join a group of twelve Jordanian judges on loan to the Ministry of Justice to serve on the court, which is expected to begin hearing cases in March 2008.

There are 54 Central Bank-licensed wholesale banks (formerly referred to as offshore banking units OBUs) that are branches of international commercial banks. The license that changed OBUs to wholesale banks allows wholesale banks to accept deposits from citizens and residents of Bahrain, and undertake transactions in Bahraini dinars (with certain exemptions, such as dealings with other banks and government agencies). In all other respects, wholesale banks are regulated and supervised in the same way as the domestic banking sector. They are subject to the same regulations, on-site examination procedures, and external audit and regulatory reporting obligations.

However, Bahrain's Commercial Companies Law (Legislative Decree 21 of 2001) does not permit the registration of offshore companies or international business companies (IBCs). All companies must be resident and maintain their headquarters and operations in Bahrain. Capital requirements vary, depending on the legal form of company, but in all cases the amount of capital required must be sufficient for the nature of the activity to be undertaken. In the case of financial services companies licensed by the Central Bank, various minimum and risk-based capital requirements are also applied in line with international standards of Basel Committee's "Core Principles for Effective Banking Supervision."

BMA Circular BC/1/2002 states that money changers may not transfer funds for customers in another country by any means other than Bahrain's banking system. In addition, all Central Bank licensees are required to include details of the originator's information with all outbound transfers. With respect to incoming transfers, licensees are required to maintain records of all originator information and to carefully scrutinize inward transfers that do not contain the originator's information, as they are presumed to be suspicious transactions. Licensees that suspect, or have reasonable grounds to suspect, that funds are linked or related to suspicious activities-including terrorist financing-are required to file STRs. Licensees must maintain records of the identity of their customers in accordance with the Central Bank's anti-money laundering regulations, as well as the exact amount of transfers. During 2004, the BMA consulted with the industry on changes to its existing AML/CTF regulations, to reflect revisions by the FATF to its Forty plus Nine Recommendations. Revised and updated BMA regulations were issued in mid-2005.

Legislative Decree No. 21 of 1989 governs the licensing of nonprofit organizations. The Ministry of Social Development (MSD) is responsible for licensing and supervising charitable organizations in Bahrain. In February 2004, as part of its efforts to strengthen the regulatory environment and fight potential terrorist financing, MSD issued a Ministerial Order regulating the collection of donated funds through charities and their eventual distribution, to help confirm the charities' humanitarian objectives. The regulations are aimed at tracking money that is entering and leaving the country. These regulations require organizations to keep records of sources and uses of financial resources, organizational structure, and membership. Charitable societies are also required to deposit their funds with banks located in Bahrain and may have only one account in one bank. Banks must report to the Central Bank any transaction by a charitable institution that exceeds 3,000 Bahraini dinars (approximately $8,000). MSD has the right to inspect records of the societies to insure their compliance with the law. The Directorate of Development and Local Societies (DDLS) has a very small staff to undertake the necessary reviews of the financial information submitted by societies or to undertake inspections of these organizations

Bahrain is a leading Islamic finance center in the region. The sector has grown considerably since the licensing of the first Islamic bank in 1979. Bahrain has 34 Islamic banks and financial institutions. Given the large share of such institutions in Bahrain's banking community, the Central Bank has developed an appropriate framework for regulating and supervising the Islamic banking sector, applying regulations and supervision as it does with respect to conventional banks. In March 2002, the Central Bank introduced a comprehensive set of regulations for Islamic banks called the Prudential Information and Regulatory Framework for Islamic Banks (PIRI). The framework was designed to monitor certain banking aspects, such as capital requirements, governance, control systems, and regulatory reporting.

Bahrain is a party to the 1988 UN Drug Convention. Bahrain has signed but not yet ratified the UN Convention against Corruption. In March 2004, Bahrain issued a Legislative Decree ratifying the UN Convention against Transnational Organized Crime. In June 2004, Bahrain published two Legislative Decrees ratifying the UN International Convention for the Suppression of the Financing of Terrorism, and the UN International Convention for the Suppression of Terrorist Bombings. In January 2002, the BMA issued a circular implementing the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing as part of the Central Bank's AML regulations, and subsequently froze two accounts designated by the UNSCR 1267 Sanctions Committee and one account listed under U.S. Executive Order 13224.

In November 2004, Bahrain hosted the inaugural meeting of the Middle East and North Africa Financial Action Task Force (MENAFATF), which decided to place its Secretariat in Bahrain's capital city of Manama. An initial planning meeting was held in Manama in January 2004, and the FATF unanimously endorsed the MENAFATF proposal in July 2004. As a FATF-style regional body, it promotes best practices on AML/CTF issues, conducts mutual evaluations of its members against the FATF standards, and works with its members to comply with international standards and measures. In November 2006, MENAFATF approved a mutual evaluation report on Bahrain. The creation of the MENAFATF is critical to encourage jurisdictions in the region to improve the transparency and regulatory frameworks of their financial sectors.

The Government of Bahrain has demonstrated a commitment to establish a strong anti-money laundering and terrorist financing system and appears determined to engage its large financial sector in this effort. MENAFATF commended Bahrain for its achievements in the area of AML/CTF and praised the government for its commitment to implement the FATF recommendations. However, work remains to be done. Bahrain should continue to develop a disclosure or declaration system for the country's borders that fulfills FATF's Special Recommendation Nine covering bulk cash smuggling. The Anti-Money Laundering Unit should maintain its efforts to obtain and solidify the necessary expertise in tracking suspicious transactions. Nevertheless, there should not be an over-reliance on suspicious transaction reporting to initiate money laundering investigations. Authorities should continue to raise awareness within the capital markets and designated nonfinancial businesses and professions regarding STR reporting obligations and consider applying sanctions for willful noncompliance. Adequate resources should be devoted to the Ministry of Social Development to increase its oversight of NGOs and charities.

Bangladesh

Bangladesh is not a regional or offshore financial center. Under the new caretaker government that declared a state of emergency when it came to power on January 11, 2007, evidence of funds laundered through the official banking system escalated. The new government instituted a stringent anticorruption campaign that netted more than $30 million in proceeds—a fraction of the estimated total amount of corrupt funds located both domestically and abroad. Money transfers outside the formal banking and foreign exchange licensing system are illegal and therefore not regulated. The

principal money laundering vulnerability remains the widespread use of the underground hawala or "hundi" system to transfer money and value outside the formal banking network. The vast majority of hundi transactions in Bangladesh are used to repatriate wages from expatriate Bangladeshi workers.

The Central Bank (CB) reports a considerable increase in remittances since 2002 through official channels. The figure more than doubled from $2 billion to $4.3 billion in fiscal year 2006 (July 1-June 30) and then rose again to $5.9 billion in fiscal year 2007. The increase is due to competition from commercial banks through improved delivery time, guarantees, and value-added services such as group life insurance. However, hundi remains entrenched because it is used to avoid taxes, customs duties, and currency controls. The nonconvertibility of the local currency (the taka) coupled with intense scrutiny on foreign currency transactions in formal financial institutions also contribute to the popularity of both hundi and black market money exchanges.

In Bangladesh, hundi primarily uses trade goods to provide counter valuation or a method of balancing the books in transactions. It is part of trade-based money laundering and a compensation mechanism for the significant amount of goods smuggled into Bangladesh. An estimated $1 billion dollars worth of dutiable goods are smuggled every year from India into Bangladesh. A comparatively small amount of goods are smuggled out of the country into India. Hard currency and other assets flow out of Bangladesh to support the smuggling networks.

Fighting corruption is a keystone of the caretaker government under the state of emergency. For the past twenty years, corrupt practices became so common that between 2001 and 2005, Bangladesh was ranked by Transparency International's Corruption Perception Index as the country with the highest level of perceived corruption in the world. In 2007, Bangladesh was ranked 162 out of 179 countries surveyed. The sweep of corrupt officials and businessmen resulted in over 200 arrests including the two former prime ministers.

Bangladeshis are not allowed to carry cash outside of the country in excess of the equivalent of $3,000 to South Asian Association for Regional Cooperation (SAARC) countries and the equivalent of $5,000 to other countries. Proper documents are required by authorized foreign exchange banks and dealers. There is no limit on how much currency can be brought into the country, but amounts over $5,000 must be declared within 30 days. Customs is primarily a revenue collection agency, accounting for 40-50 percent of Bangladesh's annual government income.

The CB conducts training for commercial banks' headquarters around the country in "know your customer" procedures. Additional training is conducted in identifying suspicious transactions and reporting them to the Central Bank, where the country's financial intelligence unit is located. Since Bangladesh only began in mid-2007 to develop a national identity card (in the form of a voter registration card) and because the vast majority of Bangladeshis do not have a passport, there are difficulties in enforcing customer identification requirements. In most cases, banking records are maintained manually. Some accounting procedures used by the Central Bank do not always achieve international standards. In 2004, the Central Bank issued "Guidance Notes on Prevention of Money Laundering" and designated anti-money laundering compliance programs as a "core risk" subject to the annual bank supervision process of the CB. Banks are required to have an anti-money laundering compliance unit in their head office and a designated anti-money laundering compliance officer in each bank branch. The CB conducts regular training programs for compliance officers based on the Guidance Notes and routinely works with the banks and, if need be, investigates compliance with regulations to curb financial irregularities. Instructors from the CB also conduct regional workshops.

In May 2007 the Central Bank's Anti-Money Laundering Unit (AMLU) was named Bangladesh's Financial Intelligence Unit (FIU). The FIU along with the National Board of Revenue (NBR), the country's tax authority, are the only entities authorized to collect bank statements. While the NBR can freeze an account without a court order, the FIU cannot. Both institutions require a court order to seize

and/or forfeit the accounts. The CB has link analysis capability for investigating suspicious transactions.

Since the Money Laundering Prevention Act (MLPA) was enacted in 2002, the Central Bank has received approximately 470 suspicious transaction reports. To date, there have been no successful prosecutions. In part, this is due to procedural problems in adjusting to inter-agency cooperation. A major setback occurred in December 2005 when the newly created Anti-Corruption Commission (ACC) advised the bank that it would not investigate the cases and returned them. As a result, the Criminal Investigation Division of the national police force agreed to take the cases. During 2006, the bank and police hammered out a procedure to pursue investigations initiated through suspicious transactions reports. With the State of Emergency, a differently configured law enforcement regime headed by military officers began. The results have yielded solid evidence of money laundering. They are not prosecuting these cases as money laundering but as tax evasion or unexplained wealth.

The caretaker Government has pledged to pass amendments to strengthen the current MLPA. The legislation is in the final stages of review. Reportedly, the draft anti-money laundering provisions meet most of the international recommendations set forth by the Egmont Group, including sharing appropriate information with domestic and international law enforcement. The draft legislation addresses asset forfeiture. It does not criminalize terrorist financing. In 2006, the government announced that it wanted a separate Anti-Terrorism law that would criminalize terrorist financing, stipulating that the Anti-Terrorism Act (ATA) would have to be passed before the anti-money laundering legislation. As of late 2007 the anti-terrorism law is still pending with the Law Advisor (de facto Law Minister) repeatedly saying that Bangladesh does not need an anti-terrorism law.

Since 2003, Bangladesh has frozen nominal sums in accounts of three designated entities on the UNSCR 1267 Sanctions Committee's consolidated list. In 2004, following investigation of the accounts of an entity listed on the UNSCR 1267 consolidated list, the Central Bank fined two local banks for failure to comply with CB regulatory directives. In 2005, the Government of Bangladesh (GOB) became a party to the UN International Convention for the Suppression of the Financing of Terrorism and is now a party to twelve UN Conventions and protocols on Terrorism. The GOB is a party to the 1988 UN Drug Convention and the UN Convention against Corruption. The GOB is not a party to the Convention against Transnational Organized Crime. Bangladesh is a member of the Asia-Pacific Group, a Financial Action Task Force (FATF)-style regional body.

Although progress has been made, the Government of Bangladesh should continue to strengthen its anti-money laundering/terrorist finance regime so that it adheres to world standards. Bangladesh should criminalize terrorist finance. There should be technology enhancements to reporting channels from outlying districts to the Central Bank. Bangladesh law enforcement and customs should examine forms of trade-based money laundering. A crackdown on pervasive customs fraud would add new revenue streams for the GOB. Continued efforts should be made to fight corruption, which is intertwined with money laundering, smuggling, customs fraud, and tax evasion. The GOB should ratify the UN Convention against Transnational Organized Crime.

Barbados

A transit country for illicit narcotics, Barbados remains vulnerable to money laundering, which primarily occurs in the formal banking system. Domestically, money laundering is largely drug-related and is appears to be derived from the trafficking of cocaine and marijuana. There is also evidence of Barbados being exploited in the layering stage of money laundering with funds originating abroad. The major source of these funds appears to be connected to fraud.

As of December 2007, there are six commercial banks in Barbados. The offshore sector includes 4,635 international business companies (IBCs), 164 exempt insurance companies and 55 qualified exempt

insurance companies, seven mutual funds companies and one exempt mutual fund company, seven trust companies, seven finance companies, and 55 offshore banks. There are no free trade zones and no offshore casinos.

The International Business Companies Act (1992) provides for the general administration of IBCs. The Ministry of Industry and International Business vets and grants licenses to IBCs after applicants register with the Registrar of Corporate Affairs. The International Business (Miscellaneous Provisions) Act 2001 enhanced due diligence requirements for IBC license applications and renewals. Bearer shares are not permitted, and financial statements of IBCs are audited if total assets exceed $500,000.

The Central Bank regulates and supervises domestic and offshore banks, trust companies, and finance companies. The Ministry of Finance issues banking licenses after the Central Bank receives and reviews applications, and recommends applicants for licensing. The International Financial Services Act (IFSA) requires offshore applicants to disclose directors and shareholders names and addresses. Offshore banks must submit quarterly statements of assets and liabilities and annual balance sheets to the Central Bank. The Central Bank has the mandate to conduct on-site examinations of offshore banks. This allows the Central Bank to augment its off-site surveillance system of reviewing anti-money laundering policy documents and analyzing prudential returns. Additionally, permission must be obtained from the Central Bank to move currency abroad.

In 2007, the Central Bank revised the anti-money laundering guidelines for licensed financial institutions to reflect changes in international standards, and to include guidance on how licensees can fulfill their obligations in relation to combating the financing of terrorism. The guideline applies to all entities that are incorporated in Barbados and are licensed under the Financial Institutions Act (FIA) 1996 and the IFSA. The Central Bank conducts off-site surveillance and undertakes regular on-site examinations of licensees to assess compliance with anti-money laundering legislation and regulations. Licenses can be revoked by the Minister of Finance for noncompliance.

The Government of Barbados (GOB) criminalized drug money laundering through the Proceeds of Crime Act and the Drug Abuse (Prevention and Control) Act, 1990-14. The Money Laundering (Prevention and Control) Act 1998 (MLPCA) and subsequent amendments extends the offense of money laundering beyond drug-related crimes by criminalizing the laundering of proceeds from unlawful activities. Under the MLPCA, money laundering is punishable by a maximum of 25 years in prison and a maximum fine of $1 million. The MLPCA applies to a wide range of financial institutions, including domestic and offshore banks, IBCs, insurance companies, money remitters, investment services, and any other services of a financial nature. These institutions are required to identify their customers, cooperate with domestic law enforcement investigations, report and maintain records of all transactions exceeding $5,000 for a period of five years, and establish internal audit and compliance procedures. Financial institutions must also report suspicious transactions to the Anti-Money Laundering Authority (AMLA).

Established by the MLPCA, the AMLA supervises financial institutions' compliance with the MLPCA, and issues training requirements and regulations for financial institutions. The AMLA is comprised of nine members including a chairperson, selected from the private sector; a deputy chairperson, from the University of the West Indies; the Solicitor General; the Commissioner of Police; the Commissioner of Inland Revenue; Comptroller of Customs; the Supervisor of Insurance; the Registrar of Corporate Affairs; and a representative of the Central Bank. The Barbados Financial Intelligence Unit (FIU) is the operational arm of the AMLA and carries out the AMLA's supervisory function over financial institutions.

Established in 2000, the FIU is an independent agency housed in the office of the Attorney General. The FIU is responsible for receiving and analyzing suspicious transactions reports from financial institutions; instructing financial institutions to take steps that would facilitate an investigation; and conduct awareness training in regards to record and reporting obligations. There are no laws that

prevent disclosure of information to relevant authorities and persons who report to the FIU are protected under the law.

Financial institutions are required to report transactions when the entity has reasonable grounds to suspect the transaction involves the proceeds of crime; involves the financing of terrorism; or is suspicious in nature. In cases where the FIU suspects a transaction involves the proceeds of crime, the FIU will forward the report for further investigation to the Commissioner of Police. As of June 30, 2007, the FIU had received 56 SARs; none were referred to the Commissioner of Police. Government entities and financial institutions are required to provide the FIU with information requested by the Director of FIU. The Royal Barbados Police force pursues all potential prosecutions.

The MLPCA provides only for criminal asset seizure and forfeiture. In 2001, the GOB amended legislation to shift the burden of proof to the accused to demonstrate that property in his or her possession or control is derived from a legitimate source. Absent such proof, the presumption is that such property was derived from the proceeds of crime. The law also enhances the GOB's ability to freeze bank accounts and to prohibit transactions from suspect accounts. Legitimate businesses and other financial institutions are subject to criminal sanction, which can result in the termination of operating licenses. Tracing, seizing and freezing assets may be done by the FIU and the police. Freezing orders are usually granted for six months at a time after which they need to be reviewed. Frozen assets may be confiscated on application by the Director of Public Prosecutions and are paid into the National Consolidated Fund. No asset sharing law has been enacted, but bilateral treaties as well as the Mutual Assistance in Criminal Matters Act have provisions for asset tracing, freezing and seizure between countries.

The Anti-Terrorism Act of 2002 as well as provisions of the Money Laundering Financing of Terrorism (Prevention and Control) Act (MLFTA) criminalizes the financing of terrorism. The MLFTA is also designed to control bulk cash smuggling and the use of cash couriers. The GOB circulates the names of suspected terrorists and terrorist organizations listed on the United Nations 1267 Sanctions Committee's Consolidated List and the list of Specially Designated Global Terrorists designated by the United States. In 2007, the GOB found no evidence of terrorist financing. The GOB has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and nonprofit entities.

Barbados has bilateral tax treaties that eliminate or reduce double taxation with the United Kingdom, Canada, Finland, Norway, Sweden, Switzerland, and the United States. The United States and the GOB ratified amendments to its bilateral tax treaty in 2004. The treaty with Canada currently allows IBCs and offshore banking profits to be repatriated to Canada tax-free after paying a much lower tax in Barbados. A Mutual Legal Assistance Treaty (MLAT) and an extradition treaty between the United States and the GOB each entered into force in 2000.

Barbados is a member of the Caribbean Financial Action Task Force (CFATF) and underwent a mutual evaluation in December 2006. The report is anticipated to be finalized in the summer of 2008 and published electronically via CFATF's website. Barbados is a member of the Offshore Group of Banking Supervisors, the Caribbean Regional Compliance Association, and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The FIU is a member of the Egmont Group. Barbados is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GOB has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the Inter-American Convention against Terrorism.

The Government of Barbados has taken a number of steps in recent years to strengthen its anti-money laundering and counter-terrorist financing legislation, and should continue to implement these reforms. The GOB should be more aggressive in conducting examinations of the financial sector and

maintaining strict control over vetting and licensing of offshore entities. The GOB should consider adopting civil forfeiture and asset sharing legislation. The GOB should ensure adequate supervision of nonprofit organizations and charities. It should also work to improve information sharing between regulatory and enforcement agencies. Additionally, Barbados should continue to provide adequate resources to its law enforcement and prosecutorial personnel, to ensure mutual legal assistance treaty requests are efficiently processed. The GOB should also ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Belarus

Belarus is not a regional financial center. A general lack of transparency throughout the financial sector means that assessing the level of or potential for money laundering and other financial crimes is difficult. Due to excessively high taxes, underground markets, and the dollarization of the economy, a significant volume of foreign-currency cash transactions eludes the banking system. Shadow incomes from offshore companies, filtered through small local businesses, constitute a significant portion of foreign investment. Smuggling is prevalent. Corruption is a severe problem in Belarus, which hinders law enforcement and impedes much-needed reforms. Economic decision-making in Belarus is highly concentrated within the top levels of government. Recent decrees have further concentrated economic power into the hands of the president, granting the Presidential Administration the power to manage, dispose of, and privatize all state-owned property and to confiscate at will any plot of land for agricultural, environmental, recreational, historical, or cultural uses.

Belarus is not considered an offshore financial center, and offshore banks, shell companies, and trusts are not permitted. As of early September 2007, the Belarusian banking sector totaled 27 banks and 383 subsidiaries. Twenty-three banks involved foreign capital, with seven being foreign-owned. In Belarus, there are currently eight offices of foreign banks, including those based in Germany, Latvia, Lithuania, Russia and Ukraine, and a representative office of the CIS Interstate Bank. The state-owned Belarus Bank is the largest and most influential bank in Belarus. In February 2006, the government abolished the 1997 identification requirements for all foreign currency exchange transactions at banks.

Belarus has established six free economic zones (FEZs) based on a 1996 Presidential Decree, one in each of the regions of Belarus. The president creates FEZs upon the recommendation of the Council of Ministers and can dissolve or extend the existence of a FEZ at will. The Presidential Administration, the State Control Committee (SCC), and regional authorities supervise the activities of companies in the FEZs. According to the SCC, applying organizations are fully vetted before they are allowed to operate in an FEZ in an effort to prevent money laundering and terrorism finance. Presidential Decree 66 has tightened FEZ regulations on transaction reporting and security, including mandatory installation of video surveillance systems. A 2005 National Bank resolution changed the status of banks in the zones by removing special provisions. Banks in the zones are currently subject to all regulations that apply to banks outside the zones.

Belarus uses customs declaration forms at points of entry and exit to fulfill cross-border currency reporting requirements for both inbound and outbound currency. Upon entry into or departure from the country, travelers must declare in writing any sum over $3,000. Travelers crossing the Belarus border with sums exceeding $10,000 require permission from the National Bank to carry that amount of currency. Officials have reported several cases of attempts to smuggle undeclared cash across borders.

Belarus' "Law on Measures to Prevent the Laundering of Illegally Acquired Proceeds" (AML Law), amended in 2005, establishes the legal and organizational framework to prevent money laundering and terrorist financing. Measures in the law apply to all entities that conduct financial transactions in Belarus, including credit and financial institutions; stock and currency exchanges; investment funds and dealers in securities; insurance institutions; dealers' and brokers' offices; notary offices; gaming establishments; pawn shops; leasing and estate agents; post offices; dealers in precious stones and

metals; attorneys conducting financial transactions on behalf of clients; and other organizations conducting financial transactions.

The AML Law makes individuals, businesses, government entities, and entities without legal status criminally liable for money laundering, although the punishments for laundering or financing terrorism are not explicitly codified. However, Article 235 of the Belarusian criminal code ("legalization of illegally acquired proceeds") stipulates penalties of fines or prison terms of up to ten years for money laundering. The law defines "illegally acquired proceeds" as currency, securities or other assets, including real and intellectual property rights, obtained in violation of the law. The National Bank of the Republic of Belarus (National Bank or NBRB) has suggested anti-money laundering and counter-terrorist financing (AML/CTF) regulations, including know your customer (KYC) and due diligence requirements. Although not legally binding, they are treated as mandatory by the institutions that the National Bank supervises. A 2005 International Monetary Fund (IMF) Financial System Stability Assessment pointed out that these regulations needed to be significantly upgraded to meet Financial Action Task Force (FATF) standards.

The AML Law authorizes the following government bodies to monitor financial transactions for the purpose of preventing money laundering: the State Control Committee (Department of Financial Monitoring, or DFM); the Securities Committee; the Ministry of Finance; the Ministry of Justice; the Ministry of Communications and Information; the Ministry of Sports and Tourism; the Committee on Land Resources; the Ministry on Taxes and Duties (MTD); and other state bodies. The MTD also provides oversight and has released binding regulations on its subject institutions.

There is a threshold reporting requirement. Individual and corporate financial transactions exceeding approximately $27,000 and $270,000, respectively, are subject to special inspection. Banks that violate the law face fines of up to one percent of their registered capital and suspension of their licenses for up to one year. However, the AML Law exempts most government transactions and those sanctioned by the President from extraordinary inspection. The government has used the AML Law as a pretext for preventing several pro-democracy NGOs from receiving foreign assistance.

In January 2005, the President signed a decree on the regulation of the gaming sector, imposing stricter tax regulations on owners of gaming businesses. In addition, a provision intended to combat money laundering requires those participating in gaming activities to produce identification to receive winnings.

The National Bank is the monitoring agency for the majority of transactions conducted by financial institutions. Information regarding suspicious transactions is reported to the Bank's Department of Bank Monitoring. Failure to report and transmit required information on financial transactions may subject financial institutions to criminal liability. Although the banking code stipulates that the National Bank has primary regulatory authority over the banking sector, in practice, the Presidential Administration exerts significant influence over it. Any member of the Board of the National Bank may be removed from office by the president with a simple notification to the National Assembly.

Financial institutions conducting transfers subject to special monitoring are required to disclose to the Department of Financial Monitoring (DFM) within one business day the identity of the individuals and businesses ordering the transaction or the person on whose behalf the transaction is being placed, information about the beneficiary of a transaction, and account information and document details used in the transaction. Article 121 of the Banking Code provides a "safe harbor" for banks and other financial institutions that provide otherwise confidential transaction data to investigating authorities, provided the information is given in accordance with the procedures established by law, and reporting individuals are protected by law when notifying authorities of suspicious transactions. Under the State Control Committee (SCC), the Department of Financial Investigations, in conjunction with the Prosecutor General's Office, has the legal authority to investigate suspicious financial transactions and

examine the internal rules and enforcement mechanisms of any financial institution. The DFM also has the authority to initiate its own investigations.

In 2003, Belarus established the Department of Financial Monitoring (DFM) as its financial intelligence unit (FIU). As the primary government agency responsible for gathering, monitoring and disseminating financial intelligence, the DFM analyzes financial information for evidence of money laundering and forwards it to law enforcement officials for prosecution. The DFM also has the power to penalize those who violate money laundering laws and suspend the financial operations of any company suspected of money laundering or financing terrorism. The DFM cooperates with counterparts in foreign states and with international organizations to combat money laundering and is a member of the Egmont Group. Since its accession to the Egmont Group, the DFM's workload has increased, which the DFM attributes not only to its Egmont membership, but also to increased interest by law enforcement in the FIU's work.

Financial institutions are obligated to report to the DFM transactions subject to special monitoring, including: transactions whose suspected purpose is money laundering or terrorist financing; cases where the person performing the transaction is a known terrorist or controlled by a known terrorist; cases in which the person performing the transaction is from a state that does not cooperate internationally to prevent money laundering and terrorist financing; and finally, transactions exceeding the currency reporting threshold that involve cash, property, securities, loans or remittances. If the total value of transactions conducted in one month exceeds set thresholds and there is reasonable evidence to suggest that the transactions are related, then all the transaction activity must be reported.

All remittances by law must be conducted through licensed banks. The government does not acknowledge alternative remittance systems. Currency exchange is allowed only through licensed currency exchange kiosks. All charities are registered with the Department of Humanitarian Assistance in the Presidential Administration. Charity assistance provided by foreign states, international organizations and individuals are regulated by Presidential Decree 24 passed in 2003 which requires all organizations and individuals receiving charity assistance to open charity accounts in a local bank.

Terrorism is a crime in Belarus and the AML Law establishes measures to prevent terrorism finance. Belarus' law on counterterrorism also states that knowingly financing or otherwise assisting a terrorist group constitutes terrorist activity. Under the Belarusian Criminal Code, the willful provision or collection of funds in support of terrorism by nationals of Belarus or persons in its territory constitutes participation in terrorism by aiding and abetting. In December 2005, the Belarusian Parliament amended the Criminal Code to stiffen the penalty for the financing of terrorism and thus bring Belarusian regulations into compliance with the International Convention for the Suppression of the Financing of Terrorism. The amendments explicitly define terrorist activities and terrorism finance and carry an eight to twelve year prison sentence for those found guilty of sponsoring terrorism. In February 2006, the Interior Ministry announced the establishment of a new counterterrorism department within its Main Office against Organized Crime and Corruption.

Belarusian legislation provides for broad seizure powers for law enforcement to identify and trace assets. Forfeiture is permitted in the Criminal Code for all serious offenses, including money laundering. Seizure of assets from third parties appears possible but is not specifically codified. The seizure of funds or assets held in a bank requires a court decision, a decree issued by a body of inquiry or pre-trial investigation, or a decision by the tax authorities.

A 2002 directive issued by the Board of Governors of the National Bank prohibits all transactions with accounts belonging to terrorists, terrorist organizations and associated persons. This directive also outlines a process for circulating to banks the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list. The National Bank is required to disseminate to banks the updates to the consolidated list and other information related to terrorist finance as it is received from the Ministry of Foreign Affairs. The directive gives banks the authority

to freeze transactions in the accounts of terrorists, terrorist organizations and associated persons. In accordance with a resolution passed in March 2006, the Belarusian KGB compiled a list of 221 individuals suspected of participation in terrorism which the National Bank distributed to all domestic banks. Through 2007, Belarus has not identified any assets as belonging to individuals or entities included on the UNSCR 1267 Sanctions Committee's consolidated list.

Domestically, Belarus has made an effort to ensure cooperation and coordination between state bodies through the Interdepartmental Working Group established specifically to address these AML/CTF issues. This Working Group includes representatives of the Prosecutor's office, the National Bank, MTD, State Security Committee, Department of Financial Investigation, and the DFM. The Director of the DFM serves as the head of this Group.

Belarus has signed bilateral treaties on law enforcement cooperation with Afghanistan, Bulgaria, India, Latvia, Lithuania, the People's Republic of China, Poland, Romania, Syria, Turkey, the United Kingdom, and Vietnam. In September 2006, Belarus signed an AML agreement with the People's Bank of China. Belarus is also a party to five agreements on law enforcement cooperation and information sharing among CIS member states, including the Agreement on Cooperation among CIS Member States in the Fight against Crime and the Agreement on Cooperation among Ministries of Internal Affairs in the Fight against Terrorism. In 2004, Belarus joined the Eurasian Regional Group Against Money Laundering and the Financing of Terrorism (EAG), which is a FATF-style regional body (FSRB) with observer status in FATF. The DFM is a member of the Egmont Group, attaining membership in that body in May 2007. Belarus has also assumed international commitments to combat terrorism as a member of the Collective Security Treaty Organization (CSTO), which includes Armenia, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan. In April 2007 the National Banks of Belarus and Kyrgyzstan signed an agreement on financial information exchange and training for fighting money laundering and terrorist financing.

Belarus is a party to the UN Convention against Corruption. In July 2006 President Lukashenko signed an anticorruption law to comply with the Council of Europe's 1999 Criminal Law Convention on Corruption, which Belarus ratified in 2004. In June 2007 Parliament passed Criminal Code amendments to toughen penalties for various offences by officials, including larceny through abuse of office, embezzlement, and legalization of assets illegally obtained. In July 2007 President Lukashenko issued an edict mandating the formation of specialized departments within prosecutors' offices, police stations and the KGB to fight against corruption and organized crime. Despite recent legislation, corruption remains a serious obstacle to enforcing laws dealing with financial crimes. Belarus ranked number 150 out of 180 territories listed in Transparency International's 2007 International Corruption Perception Index.

Belarus is a party to the 1988 UN Drug Convention, to the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism, though it has been actively expanding ties with Iran and Syria, both state sponsors of terrorism.

The Government of Belarus (GOB) has taken steps to construct a legal and regulatory framework to fight money laundering and terrorist financing. It should also focus on the implementation of the law by law enforcement, increasing the investigation and prosecution of money laundering and terrorist financing offenses. This could be accomplished through training and outreach by the FIU and other regulators. Belarus should increase the transparency of its business, finance, and banking sectors. Belarus' AML legislation should be amended to comport with international standards and to provide for more transparency and accountability. The GOB can accomplish this by extending the application of its current AML legislation to cover the governmental transactions that are currently exempted under the law, and ensure that the regulations and guidance provided by the National Bank and other regulators are legally binding. Similarly, the National Bank should be given the authority to carry out

its responsibilities, and not be subject to influence by the Presidential Administration. The GOB should implement strict regulation on its industries operating abroad and on those operating within the FEZ areas. The GOB needs to reinstate the identification requirement for foreign currency exchange transactions, and reconsider the relationships it wishes to foster with state sponsors of terrorism. Belarus should continue to hone its guidance and enforcement of suspicious transaction reporting and provide adequate staff, tools, training and financial resources to its FIU so that it can operate effectively, especially with the increased attention and reporting that the DFM has generated of late. The GOB must work to further improve the coordination between agencies responsible for enforcing AML measures. The GOB also needs to take steps to ensure that the AML framework operates more objectively and less as a political tool. The GOB should take serious steps to combat corruption in commerce and government.

Belgium

With assets of over $2.5 trillion dollars in 2006, Belgium has a formidable banking industry. Strong legislative and oversight provisions are in place in the formal financial sector to combat money laundering and terrorist financing. However, the informal financial sector is particularly vulnerable to money laundering especially through the use of alternative remittance and underground banking. The diamond industry has also long been a sector of vulnerability. Belgian officials have also noted that criminals are increasing their use of the nonfinancial professions to facilitate access to the official financial sector.

Belgium criminalized money laundering through the Law of 11 January 1993, On Preventing Use of the Financial System for Purposes of Money Laundering. This law outlines customer due diligence and reporting requirements, which are also applicable to designated nonfinancial business and professions (DNFBPs). Obligated entities include estate agents, private security firms, funds transporters, diamond merchants, notaries, bailiffs, auditors, chartered accountants, tax advisors, certified accountants, surveyors, and casinos. Additional laws make the requirements applicable to other sectors including credit institutions, investment firms, intermediaries, investment advisors and attorneys. The Belgian Banking and Finance Commission (CBFA) supervises financial institutions, including exchange houses, stock brokerages, and insurance companies. The Belgian Gaming Commission oversees casinos.

Belgian law mandates reporting of suspicious transactions by a wide variety of financial institutions and nonfinancial entities, including notaries, accountants, bailiffs, real estate agents, casinos, cash transporters, external tax consultants, certified accountant-tax experts, and lawyers. Lawyers in particular do not consistently comply with reporting requirements. Belgian lawyers, for example, reported three suspicious transactions to the financial intelligence unit (FIU) in 2006. An association of Belgian lawyers has appealed the law to Belgium's court of arbitration on the grounds that it violates basic principles of the independence of the lawyer and of professional secrecy. Belgium is still awaiting a decision from the court of arbitration on this matter.

Article 505 of the Penal Code sets penalties of up to five years' imprisonment for money laundering convictions. Any unlawful activity may serve as the predicate offense. Legislation implementing the Second European Union (EU) Directive on Money Laundering, or Council Directive 2001/97/EC On Prevention of the Use of the Financial System for Money Laundering, has broadened the scope of money laundering predicate offenses beyond drug trafficking to include the financing of terrorist acts or organizations.

The most recent mutual evaluation of Belgium was conducted by the Financial Action Task Force (FATF) in June 2005. Of the 49 recommendations, one of which was not applicable, Belgium received 41 ratings of "compliant" or "largely compliant." Although the report concluded that Belgium's anti-money laundering and counter-terrorist financing (AML/CTF) regime is effective, the assessment

team found partial or noncompliance in some areas. These areas include: due diligence and regulation requirements for DNFBPs, licensing or registration of businesses providing money or value transfer services, allocation of adequate resources to the authorities charged with combating financial crimes, elimination of bearer bonds, development of an independent authority to freeze assets, and implementation of a system to monitor cross-border currency movements. Belgium is currently working to address these deficiencies.

Royal Decree of 5 October 2006, On Measures to Control Cross-border Transportation of Cash came into force on June 15, 2007. This decree implements regulation 1889/2005 of the EU Council on controls of cash entering or leaving the EU: travelers must declare transportation of currency into or out of the EU worth 10,000 euros (U.S. $14,600) or more. In case of nondeclaration, or if there is a suspicion that the funds being declared originates from illegal activities or is intended to finance such activities, the Belgian Customs and Excise administration will confiscate the cash for a maximum period of 14 days and file a report. The Belgian FIU examines all the declarations and Customs reports that are filed. Since June 2007, Belgian Customs has received information on approximately 4.5 million euros (U.S. $6.6 million) in cash being transported through Zaventem International Airport. To date, Belgian Customs has confiscated 670,000 euros (U.S. $978,200) and filed eight reports with the FIU.

Belgian financial institutions must comply with "know your customer" principles, regardless of the transaction amount. Institutions must maintain records on the identities of clients engaged in transactions that are considered suspicious or that involve an amount equal to or greater than 10,000 euros (approximately U.S. $14,650). Institutions must retain records of suspicious transactions reported to the FIU for at least five years. Financial institutions must train their personnel in the detection and handling of suspicious transactions that could be linked to money laundering. Financial institutions or other entities with reporting requirements are also liable for illegal activities occurring under their control. Penalties for failure to comply with the AML legislation, including failure to report, include a fine of up to $1.72 million.

Money laundering legislation imposes prohibitions on cash payments for real estate, except for an amount not exceeding 10 percent of the purchase price or 15,000 euros (U.S. $21,900), whichever is lower. Cash payments over 15,000 euros (U.S. $21,900) for goods are illegal.

Belgium has long permitted the issuance of bearer bonds ("titres au porteur"), widely used to transfer wealth between generations and to avoid taxes, for individuals as well as for institutions. In late 2005 the Belgian federal parliament adopted a law to cease the issuance of bearer bonds beginning on January 1, 2008. Bearer bonds issued before that date will still be valid, however, as well as nonBelgian bearer bonds.

Belgium needed to implement the Third EU Money Laundering Directive by December 15, 2007. The European Commission adopted recommendations for EU member states and a framework for a code of conduct for the nonprofit/charitable sector. Belgian officials are working to increase transparency in this sector through better enforcement of registration and reporting procedures. Requirements for nonprofit organizations include registering, furnishing copies of their statues and lists of members, providing minutes from council meetings, and filing budget reports.

A growing problem, according to government officials, is the proliferation of illegal underground banking activities. Beginning in 2004, Belgian police made a series of raids on "phone shops"—small businesses where customers can make inexpensive phone calls and access the Internet. In some "phone shops," authorities uncovered money laundering operations and hawala-type banking activities. In 2006, further raids uncovered numerous counterfeit phone cards and illegal or undocumented workers in addition to evidence of money laundering activities in some locations. Since 2004, the Belgian authorities have closed more than 150 "phone shops" and have estimated that the Belgian state may have been deprived of up to $256 million in lost tax revenue each year through tax evasion by these

businesses. Authorities report that "phone shops" often declare bankruptcy and later reopen under new management, making it difficult for officials to trace ownership and collect tax revenues. Authorities believe that 3,500 "phone shops" may be operating in Belgium. Only an estimated one-quarter of these shops have licenses to operate, and Belgian authorities are considering enforcing a stricter licensing regime. Some Brussels communes have also proposed heavy taxes on these types of shops in an effort to dissuade illegitimate commerce.

Belgium's robust diamond industry presents special challenges for law enforcement. Despite some diffusion in recent years, Belgium continues to be the world's diamond-trading center. Fully 90 percent of the world's crude diamonds and 50 percent of cut diamonds pass through Belgium. Most of the "blood" or "conflict diamonds" from long-running African civil wars were processed in Antwerp. Authorities have transmitted a number of cases relating to diamonds to the public prosecutor, and that office is examining the sector closely in cooperation with local police and diamond industry officials. Additionally, the Kimberley certification process (a joint government, international diamond industry, and civil society initiative designed to stem the flow of illicit diamonds) has introduced much-needed transparency into the global diamond trade. However, diamonds of questionable origin continue to appear on the Belgian market. The Government of Belgium (GOB) recognizes the particular importance of the diamond industry, as well as the potential vulnerabilities it presents to the financial sector. The GOB has distributed typologies outlining its experiences in pursuing money laundering cases involving the diamond trade, especially those involving the trafficking of African conflict diamonds. A regulation approved by a Royal Decree dated October 22, 2006 contains a detailed description of the required obligations for diamond dealers. This regulation primarily deals with the different aspects of client identification, including the identification of "nonface to face" operations and of the beneficial owner, customer due diligence, and obligations regarding the internal organization.

The Belgian financial intelligence unit (FIU), known in French as Cellule de Traitement des Informations Financières and in Flemish as Cel voor Financiële Informatieverwerking (CTIF-CFI), was created in June 1993. The FIU is an autonomous and independent public administrative authority, supervised by the Ministries of Justice and Finance. Institutions and persons subject to the reporting obligations fund the FIU. Although these contributions are compulsory, the contributing entities do not exercise any formal control over the FIU. CTIF-CFI's primary mission is to receive, analyze, and disseminate all suspicious transaction reports submitted by regulated entities. Operating as a filter between obligated entities and judicial authorities, CTIF-CFI reports possible money laundering or terrorist financing transactions to the public prosecutor. The financial sector cooperates actively with CTIF-CFI to guard against illegal activity. Institutions, their employees, and representatives are protected from civil, penal, or disciplinary actions when reporting transactions in good faith to CTIF-CFI. Legislation also exists to protect witnesses, including bank employees, who report suspicions of money laundering, or who come forward with information about money laundering crimes. Belgian officials have imposed sanctions on institutions or individuals that knowingly permitted illegal activities to occur. CTIF-CFI also acts as the supervisory body for professions not supervised by CBFA or other authorities. CTIF-CFI has analyzed the diamond industry and is working to eliminate its potential for money laundering and terrorist financing. It has initiated several meetings with the Belgian Ministry of Economic Affairs and the High Council for Diamonds to clarify the obligations of diamond traders with respect to AML/CTF laws, and how diamond traders apply this legislation.

Financial experts, including three magistrates (public prosecutors) appointed by the King to a six-year renewable term of service, comprise the leadership of CTIF-CFI. A magistrate presides over the body. In addition to administrative and legal support, the investigative department consists of inspectors, analysts, three liaison police officers, one customs officer, and one officer of the Belgian intelligence service charged with maintaining contact with the various law enforcement agencies in Belgium.

In the first half of 2007, CTIF-CFI received 5,995 STRs and opened 2,301 case files, of which 551 were transmitted to the public prosecutor. By comparison, in 2006, the FIU received 9,938 disclosures, opened 3,367 new cases, and transmitted 912 cases to the public prosecutor. A breakdown of the 2007 figures was not available; but, in 2006, nearly 80 percent of disclosures on files transmitted to the federal prosecutor were made by credit institutions. Foreign exchange offices and foreign counterpart units accounted for an additional 15 percent of the files transmitted with notaries, casinos, and other entities also reporting. The files concerning narcotics trafficking represented 15 percent of the total number of cases in 2006, while cases regarding terrorism and terrorist finance represented about four percent of the total number. The FIU reported 36 cases regarding terrorism or terrorist financing to the judicial authorities.

To date, Belgian courts have convicted 1,880 individuals for money laundering on the basis of cases forwarded by the FIU. These convictions have yielded combined total sentences of 2,819 years. Although five years is the maximum sentence for money laundering, the length of the sentence may increase if the financial crime is compounded by another type of crime such as drug trafficking. Belgian authorities have confiscated more than approximately $788 million connected with money laundering crimes. The majority of convictions in relation to money laundering are based upon disclosures made by the financial institutions and others to CTIF-CFI.

The federal police must also transmit suspected money laundering cases to the public prosecutor. In 2006 the federal police referred a total of 2,241 individuals to the public prosecutor for various crimes. More than 20 percent of these (450 individual cases) involved money laundering, fraud, and corruption. According to the FATF MER, the criminal prosecution authorities have the necessary power to carry out their functions; however, in some places or at some times, the prosecutors and police seem to lack resources to properly perform their AML/CTF duties.

The federal police enjoy good cooperation with their counterparts in neighboring countries. Belgium does not require an international treaty as a prerequisite to lending mutual assistance in criminal cases. The federal police and the specialized services of the Central Office for the Fight against Organized Economic and Financial Crimes utilize a number of tactics to uncover money laundering operations, including investigating significant capital injections into businesses, examining suspicious real estate transactions, and conducting random searches at all international airports. In 2005, Project Cash Watch, carried out under the auspices of the federal police in Belgium's international airports and other transit venues, netted seizures of more $2.45 million.

According to the FATF MER, Belgium has created a sophisticated and comprehensive confiscation and seizure regime, which includes the Central Office for Seizures and Confiscation (COSC). COSC operates under the auspices of the Ministry of Justice. Belgian law allows for criminal forfeiture of assets. A July 2006 law allows for the possibility, on a reciprocal basis, of the sharing of seized assets from serious crimes, including those related to narcotics, with affected countries. Since a judicial order is necessary before carrying out confiscations and seizures, COSC ensures that confiscations and seizures are executed smoothly and efficiently in accordance with Belgian law.

Belgian authorities attempt to sell confiscated items such as cars, computers, and cell phones soon after confiscation to minimize the loss of the market value of the goods over time. If a suspect is later found innocent, he/she receives the cash equivalent of the item(s) sold, plus accrued interest. COSC has a commercial account for the deposit of confiscated funds. As of October 2007, the fund held more than $165 million. COSC also maintains safe deposit boxes for the storage of high value items, such as jewelry. Seizures in Belgium can be direct or indirect. Direct seizures involve the seizure of items linked directly to a crime. Noncash items are held in the clerks' offices in one of Belgium's 27 judicial districts. Indirect seizures are "seizures by equivalence," usually homes, cars, jewels, and other items of value not directly linked to the crime in question. Money from seizures and from the sale of seized goods is deposited into the Belgian Treasury.

Belgian legislation implementing the EU Council's Framework Decision on Combating Terrorism criminalizes terrorist acts and the provision of material and financial support for terrorist acts. It also allows judicial freezes on terrorist assets. The law followed the Second European Money Laundering Directive and also implemented eight of FATF's Special Recommendations. Article 140 of the Penal Code criminalizes participation in the activity of a terrorist group, and Article 141 specifically penalizes the provision of material resources, including financial assistance, to terrorist groups; the penalty is five to ten years' imprisonment.

Under Belgium's AML/CTF law, bank accounts can be frozen on a case-by-case basis if there is sufficient evidence that a money laundering crime has been committed. The FIU has the legal authority to suspend a transaction for a period of up to two working days to complete its analysis. If criminal evidence exists, the FIU forwards the case to the public prosecutor.

The Ministry of Justice can freeze assets related to terrorist crimes. However, the burden of proof in such cases is relatively high. In order for an act to constitute a criminal offense, authorities must demonstrate that the target gave support knowing that it would contribute to the commission of a crime by the terrorist group. Because the law does not establish a national capacity for designating foreign terrorist organizations, Belgian authorities must demonstrate in each case that the group that received the support actually constitutes a terrorist group.

In Belgium, the Ministry of Finance can administratively freeze assets of individuals and entities associated with Al-Qaida, the Taliban and Usama Bin Laden on the United Nations (UN) 1267 Sanctions Committee's consolidated list. It can also do so if the individual or entity is covered by an EU asset freeze regulation. Frozen assets are transferred to the Ministry of Finance. If an entity appears on the UN 1267 Sanctions Committee's consolidated list, but not on the EU list, the GOB passes a ministerial decree to freeze assets to comply with the UN requirement. Assets of entities appearing on the EU list are automatically subject to a freeze without additional legislative or executive procedures. Belgium is working on legislation to permit the administrative freeze of terrorist assets in the absence of a judicial order or UN or EU designation.

Belgium's FIU is active with its colleagues in sharing information. CTIF-CFI has signed a memorandum of understanding with its United States counterpart that governs their collaborative work. CTIF-CFI was a founding member of the Egmont Group and headed the secretariat from 2005 to 2006. Belgium is a cooperative and reliable partner in law enforcement efforts as well.

Belgium is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Belgium has signed, but not yet ratified, the UN Convention against Corruption. A mutual legal assistance treaty (MLAT) between Belgium and the United States has been in force since January 2000, and an extradition treaty between the two countries has been operative since September 1997. Bilateral instruments amending and supplementing these treaties, in implementation of the U.S.-EU Extradition and Mutual Assistance Agreements, were signed with Belgium in December 2004, and await ratification, including by the U.S. side.

Belgium's continuing work on implementing the FATF recommendations complements an already solid AML regime and a clear official commitment to fighting against financial crimes, including the financing of terrorism. However, the Government of Belgium should continue to work through proposed legislation that pursues tougher and faster independent asset-freezing capability, as well as the optimal disposition of seized assets. The Government of Belgium should continue its efforts to uncover, investigate, and prosecute illegal banking operations, as well as increase attention to and dedicate more resources toward tracking the informal financial sector and nonbank financial institutions. This is especially applicable to the identification, regulation and enforcement of hawala enterprises that the GOB has already articulated as a concern. The GOB should strengthen adherence to reporting requirements by some nonfinancial entities in Belgium, such as lawyers and notaries, and

enhance the regulations and reporting obligations for the nonprofit and charitable sector. To be even more effective in its efforts, Belgium may need to devote more resources, including investigative personnel, to police, prosecutors, and key Belgian agencies that work on money laundering, terrorist financing, and other financial crimes.

Belize

Belize is not a major regional financial center. In an attempt to diversify Belize's economic activities, authorities have encouraged the growth of offshore financial activities and have pegged the Belizean dollar to the U.S. dollar. Belize continues to offer financial and corporate services to nonresidents. Belizean officials suspect that money laundering occurs primarily within the country's offshore financial sector. Money laundering, primarily related to narcotics trafficking and contraband smuggling, is suspected to occur through banks operating in Belize. Criminal proceeds laundered in Belize are derived primarily from foreign criminal activities. There is no evidence to indicate that money laundering proceeds are primarily controlled by local drug-trafficking organizations, organized criminals or terrorist groups.

Offshore banks, international business companies, and trusts are authorized to operate from within Belize, although shell banks are prohibited within the jurisdiction. The Offshore Banking Act, 1996 governs activities of Belize's offshore banks. By law, offshore banks cannot serve customers who are citizens or legal residents of Belize. To legally operate from within Belize, all offshore banks must be licensed by the Central Bank and be registered with international business companies (IBCs). Before the Central Bank issues the license, the Central Bank must verify shareholders' and directors' backgrounds, ensure the adequacy of capital, and review the bank's business plan. The legislation governing the licensing of offshore banks does not permit directors to act in a nominee (anonymous) capacity.

Presently, there are eight licensed offshore banks, approximately 32,800 active registered IBCs, one licensed offshore insurance company, one mutual fund company, and 30 trust companies and agents operating in Belize. Only nonresident entities have access to offshore banks, and banks are not permitted to issue bearer shares. Local money exchange houses, which were suspected of money laundering, were closed effective July 2005. There is also an undisclosed number of Internet gaming sites operating from within the country. These gaming sites are unregulated at this time. Currently there are no offshore casinos operating from within Belize.

The International Business Companies Act of 1990 and its 1995 and 1999 amendments govern the operation of IBCs. The 1999 amendment to the Act allows IBCs to operate as banks and insurance companies. The International Financial Services Commission regulates the rest of the offshore sector. All IBCs must be registered. Although nonbank IBCs are allowed to issue bearer shares, the registered agents of such companies must know the identity of the beneficial owners of the bearer shares. Belize's legislation allows for the appointment of nominee directors of nonbank IBCs. The legislation for trust companies, the Belize Trust Act, 1992, is not as stringent as the legislation for other offshore financial services and does not preclude the appointment of nominee trustees.

There is one free trade zone presently operating in Belize, at the border with Southern Mexico. There are also designated free trade zones in Punta Gorda, Belize City, and Benque Viejo, but they are not operational. Data Pro Ltd. is designated as an Export Processing Zone (EPZ) and is regulated in accordance with the EPZ Act. Commercial free zone (CFZ) businesses are allowed to conduct business within the confines of the CFZ, provided they have been approved by the Commercial Free Zone Management Agency (CFZMA) to engage in business activities. All merchandise, articles, or other goods entering the CFZ for commercial purposes are exempted from the national customs regime. However, any trade with the national customs territory of Belize is subject to the national Customs and Excise law. The CFZMA, in collaboration with the Customs Department and the Central

Bank of Belize, monitors the operations of CFZ business activities. There is no indication the CFZ is presently being used in trade-based money laundering schemes or by financiers of terrorism.

Alternative remittance systems are illegal in Belize. However, Belizean authorities acknowledge the existence and use of indigenous alternative remittance systems that bypass, in whole or part, financial institutions. Therefore, Belizean authorities monitor such activities at the borders with Mexico and Guatemala.

Allegedly, there is a significant black market for smuggled goods in Belize. However, there is no evidence to indicate that the smuggled goods are significantly funded by narcotics proceeds, or evidence to indicate significant narcotic-related money laundering. The funds generated from contraband are undetermined.

The Money Laundering (Prevention) Act (MLPA), in force since 1996 and amended in 2002, criminalizes money laundering related to many serious crimes, including drug trafficking, forgery, terrorism, blackmail, arms trafficking, kidnapping, fraud, illegal deposit taking, false accounting, counterfeiting, extortion, robbery, and theft. The minimum penalty for a money laundering offense as defined by the MLPA is three years imprisonment. Other legislation to combat money laundering includes the Money Laundering Prevention Guidance Notes; the Financial Intelligence Unit Act, 2002; the Misuse of Drugs Act; The International Financial Services Practitioners Regulations (Code of Conduct), 2001 (IFSPR); Money Laundering Prevention Regulations 1998 (MLPR); and the Offshore Banking Act, 2000, renamed the International Banking Act, 2002 (IBA).

The Central Bank of Belize supervises and examines financial institutions for compliance with anti-money laundering and counter-terrorist financing laws and regulations. The banking regulations governing offshore banks are different from the domestic banking regulations in terms of capital and operational requirements. Nevertheless, all licensed financial institutions in Belize (onshore and offshore) are governed by the same legislation and must adhere to the same anti-money laundering and counter-terrorist financing requirements. Government of Belize (GOB) officials have reported an increase in financial crimes, such as bank fraud, cashing of forged checks, and counterfeit Belizean and United States currency. The Central Bank of Belize has engaged in public awareness activities and training sessions to regulate counterfeit currency.

The Central Bank issued Supporting Regulations and Guidance Notes in 1998. Licensed banks and financial institutions are required to establish due diligence ("know-your-customer") provisions, monitor their customers' activities and report any suspicious transaction to the financial intelligence unit (FIU) of Belize. Belize law obligates banks and other financial institutions to maintain business transactions records for at least five years when the transactions are complex, unusual or large. Money laundering controls are also applicable to nonbank financial institutions, such as exchange houses, insurance companies, lawyers, accountants and the securities sector, which are regulated by the International Financial Services Commission. Financial institution employees are exempt from civil, criminal or administrative liability for cooperating with regulators and law enforcement authorities in investigating money laundering or other financial crimes. Belize does not have any bank secrecy legislation that prevents disclosure of client and ownership information.

The reporting of all cross-border currency movement is mandatory. All individuals entering or departing Belize with more than $10,000 in cash or negotiable instruments are required to file a declaration with the authorities at Customs, the Central Bank and the FIU.

The FIU of Belize, established in 2002, is an independent agency presently housed at the Central Bank. Current laws do not provide for the funding of the FIU, and the FIU has to apply to the Ministry of Finance for funds. Due to financial constraints, the FIU is not adequately staffed and existing personnel lack sufficient training and experience. In November 2005, the director of the FIU resigned, leaving the FIU with only four employees; the new FIU director did not begin until July 2006. In

December 2007, both the financial examiner and the office attendant resigned from their posts. According to the FIU's office manager, however, replacements for both employees have already been identified.

The Director of the Public Prosecutions Office and the Belizean Police Department are responsible for investigating all crimes. However, the FIU also has administrative, prosecutorial and investigative responsibilities for financial crimes, such as money laundering and terrorist financing. The FIU received 38 suspicious transaction reports (STRs) from obligated entities in 2007, nine of which became the subject of investigations. In 2007, there were press reports indicating a possible money laundering scheme by a former public official, but no subsequent investigation was conducted. Overall there were no major money laundering cases to report in 2007, and the anti-money laundering regime in Belize remains relatively ineffective.

Although the FIU has access to records and databanks of other GOB entities and financial institutions, there are no formal mechanisms for the sharing of information with domestic regulatory and law enforcement agencies. However, the FIU is empowered to share information with FIUs in other countries. On several occasions, the FIU has cooperated with the United States.

Belizean law makes no distinctions between civil and criminal forfeitures. All forfeitures resulting from money laundering or terrorist financing are treated as criminal forfeitures. The banking community cooperates fully with enforcement efforts to trace funds and seize assets. The FIU and the Belize Police Department are the entities responsible for tracing, seizing and freezing assets, and the Ministry of Finance can also confiscate frozen assets. With prior court approval, Belizean authorities have the power to identify, freeze, and seize assets related to money laundering or terrorist financing. Currently, the GOB's legislation does not specify the length of time assets can be frozen. There are no limitations to the kinds of property that may be seized, and any property—tangible or intangible—that may be related to a crime or is shown to constitute the proceeds of a crime, including legitimate businesses, may be seized. However, Belizean law enforcement lacks the resources necessary to effectively trace and seize assets.

GOB authorities are considering the enactment of a Proceeds of Crime law, which will address the seizure or forfeiture of assets of narcotics traffickers, financiers of terrorism, or organized crime. Currently, the GOB is not engaged in any bilateral or multilateral negotiations with other governments to enhance asset tracing and seizure. However, the GOB cooperates with the efforts of foreign governments to trace or seize assets related to financial crimes.

Belize criminalized terrorist financing via amendments to its anti-money laundering legislation, The Money Laundering (Prevention) (Amendment) Act, 2002. GOB authorities have circulated the names of suspected terrorists and terrorist organizations listed on the United Nations (UN) 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to all financial institutions in Belize. There are no indications that charitable or nonprofit entities in Belize have acted as conduits for the financing of terrorist activities. Consequently, the country has not taken any measures to prevent the misuse of charitable and nonprofit entities from aiding in the financing of terrorist activities.

Belize has signed and ratified a Mutual Legal Assistance Treaty with the United States, which provides for mutual legal assistance in criminal matters and entered into force in 2003. Amendments to the MLPA preclude the necessity of a Mutual Legal Assistance Treaty for exchanging information or providing judicial and legal assistance to authorities of other jurisdictions in matters pertaining to money laundering and other financial crimes. Belize is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention. The GOB has signed, but not yet ratified, the Inter-American Convention against Terrorism, and has neither signed nor ratified the UN Convention against Corruption. Belize is a member of the Organization of American States Inter-American Drug

Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). The FIU became a member of the Egmont Group of financial intelligence units in 2004.

The Government of Belize should ensure effective implementation of its anti-money laundering and counter-terrorist financing regime. The GOB should increase resources to provide adequate staffing levels and training to those entities responsible for enforcing Belize's anti-money laundering and counter-terrorist financing laws, including the financial intelligence unit and the asset forfeiture regime. Belize should take steps to address the vulnerabilities in its supervision of its offshore sector, particularly the lack of supervision of the gaming sector, including Internet gaming facilities. Belize should immobilize bearer shares and ensure that the offshore sector complies with anti-money laundering and counter-terrorist financing reporting requirements. The GOB should also become a party to the UN Convention against Corruption.

Bolivia

Although Bolivia is not a regional financial center, money laundering activities related to public corruption, contraband smuggling, trafficking in persons, and narcotics trafficking continue to be vulnerabilities. Bolivia's long tradition of bank secrecy and the lack of effective government oversight of nonbank financial activities facilitate the laundering of the profits of organized crime and narcotics trafficking, evasion of taxes, and the laundering of other illegally obtained earnings.

Bolivia's financial sector consists of approximately 13 commercial banks, six private financial funds, nine mutual funds, 23 savings and credit cooperatives, 14 insurance companies and one stock exchange, all of which are subject to the same anti-money laundering controls. The Bolivian financial system is highly dollarized, with approximately 69 percent of deposits and 81 percent of loans distributed in U.S. dollars rather than bolivianos, the local currency. Free trade zones exist in the cities of El Alto, Cochabamba, Santa Cruz, Oruro, Puerto Aguirre, and Desaguadero.

Many entities that move money in Bolivia remain unregulated. Hotels, currency exchange houses, illicit casinos, cash transporters, and wire transfer businesses are known to transfer money freely into and out of Bolivia but are not subject to anti-money laundering controls. Informal exchange businesses, particularly in the department of Santa Cruz, also transmit money to avoid law enforcement scrutiny.

Law 1768 of 1997 criminalizes money laundering in Bolivia. Law 1768 modifies the penal code; criminalizes money laundering related only to narcotics trafficking, organized criminal activities and public corruption; provides for a penalty of one to six years for money laundering; and defines the use of asset seizure beyond drug related offenses. However, the law cannot be applied unless the prosecution demonstrates in court that the accused participated in and was convicted of the predicate offense. Law 1768 also created Bolivia's financial intelligence unit (FIU), the Unidad de Investigaciones Financieras (UIF), within the Office of the Superintendence of Banks and Financial Institutions. Supreme Decree 24771 of 1997 defines the attributes and functions of the UIF.

As Bolivia's FIU, the UIF is responsible for collecting and analyzing data on suspected money laundering and other financial crimes, and sharing this information with the Bolivian National Police and the Public Ministry (Attorney General's Office) as appropriate. Decree 24771 requires banks, insurance companies, and securities brokers to identify their customers, retain records of every transaction for a minimum of ten years, and report to the UIF all transactions that are considered unusual (without apparent economic justification or licit purpose) or suspicious (customer refuses to provide information or the explanation and/or documents presented are clearly inconsistent or incorrect). There is no requirement for obligated entities to report cash transactions above a designated threshold under the current law, and no requirement exists stating that persons entering or leaving the

country declare the transportation of currency over a designated threshold. However, the UIF may request additional information from obligated financial institutions to assist prosecutors with their investigations.

The UIF is responsible for implementing anti-money laundering controls, and may request that the Superintendent of Banks sanction obligated institutions for noncompliance with reporting requirements. The UIF also conducts on-site inspections of obligated entities to review their compliance with the reporting of suspicious transactions. Given the size of Bolivia's financial sector, compliance with reporting requirements is extremely low, with the UIF receiving an average of 50 suspicious transaction reports (STRs) per year. According to the UIF, banks in Bolivia were reporting more frequently in 2007: in the first six months of 2007, the UIF received 60 STRs. The UIF is currently reviewing a total of 110 reports.

The Special Group for Investigation of Economic Financial Affairs (GIAEF) was created in 2002 within Bolivia's Special Counter-Narcotics Force (FELCN) and is responsible for investigating narcotics-related money laundering cases. Currently, there are three GIAEF units in Bolivia with a total of 27 personnel. The GIAEF reported 26 money-laundering investigations and over $9 million in assets seized over the last 12 months. The GIAEF, UIF, Public Ministry, National Police, and FELCN have established mechanisms for the exchange and coordination of information, including formal exchange of bank secrecy information.

Corruption remains a serious issue in Bolivia. According to 2006 estimates by the U.S. Agency for International Development (USAID), corruption costs Bolivians approximately $115 million per year. Traditionally, allegations against high-ranking law enforcement officials were routinely dismissed or forgotten. However, recent anti-corruption laws increased the effectiveness of investigations and the number of cases related to corruption is growing. The Office of Professional Responsibility (OPR) of the National Police has investigated a total of 1,779 cases involving allegations of misconduct and/or impropriety alleged against police officers. Of these, 205 cases were investigated involving police officers assigned to FELCN. Of these 205 cases involving FELCN officers, however, none resulted in findings of corruption.

To further combat corruption, the Government of Bolivia (GOB) promulgated Supreme Decree 28695, the Organizational Structure for the Fight against Corruption and Illicit Enrichment, in April 2006. Among a number of other provisions, the decree provides for the creation of a "Financial and Property Intelligence Unit," which would replace the UIF. Decree 28695 originally repealed Decree 24771, which gave the UIF its authority. However, because the repeal of Decree 24771 would eliminate the UIF before its replacement was operational, the GOB passed Decree 28956 in November 2006, eliminating the portion of Decree 28695 that had repealed Decree 24771 and allowing the UIF to continue to operate until the Financial and Property Intelligence Unit becomes a functioning entity.

As a result of the new decree and the plans to establish the Financial and Property Intelligence Unit, the UIF has lost a number of staff, bringing the number of personnel down to only five. Limitations in its reach, a lack of resources, and weaknesses in its basic legal and regulatory framework have hampered the UIF's effectiveness as a financial intelligence unit. There is no indication that the establishment of the Financial and Property Intelligence Unit will resolve these problems and allow for a more effective UIF.

In addition to Decrees 28695 and 28956, the Constitutional Commission of the Bolivian Chamber of Deputies is considering two competing anti-money laundering bills. Although the draft law provides a mission for the Financial and Property Intelligence Unit, there are concerns regarding the functions and authorities of the new entity, as its primary function would be to investigate cases of corruption rather than money laundering. The law also does not criminalize "self-laundering," meaning that a person could only be convicted of money laundering if he/she launders the funds generated by a crime committed by a third party. In general, the law does not include provisions to bring Bolivia's anti-

money laundering regime into greater compliance with international standards, in spite of suggestions and input from the Financial Action Task Force for South America (GAFISUD), the International Monetary Fund (IMF), the UIF, and the Government of the United States. The draft was presented to Chamber of Deputies in early December 2006, but the Chamber has not acted on it.

The second draft anti-money laundering law addresses more of the deficiencies in Bolivia's current level of compliance with the international standards for combating money laundering. This draft criminalizes self-laundering, permits special investigative techniques, and prohibits bank secrecy. This draft expands predicate offenses for money laundering beyond the three current offenses, but they are still limited to a list of specific offenses, rather than all serious crimes. Although the bill establishes terrorist financing as a predicate offense for money laundering, terrorist financing is not a crime in Bolivia. The draft law expands the number of obligated entities (to include exchange houses and money remitters); but other entities that are required to be regulated under the Financial Action Task Force (FATF) standards, such as dealers in precious metals and jewels, are not included. The draft law also does not provide legal protection for obligated entities when filing STRs or responding to requests for information from the UIF.

There are also concerns that the new legislation will not improve the GOB's overall anti-money laundering regime, which is undermined by the lack of a legal and bureaucratic framework for money laundering investigations. To prosecute a money laundering case, Bolivian law requires that the crime of money laundering be charged alongside an underlying predicate offense. Although the Public Prosecutors are responsible for prosecuting money laundering offenses, they do not have a specialized dedicated unit. Judges trying these cases are challenged to understand their complexities. To date, there has been only one conviction involving money laundering.

There are also serious deficiencies in Bolivia's legal framework with regard to civil responsibility. Under Bolivian law, there is no protection for judges, prosecutors or police investigators who make good-faith errors while carrying out their duties. If a case is lost initially or on appeal, or if a judge rules that the charges against the accused are unfounded, the accused can request compensation for damages, and the judges, prosecutors, or investigators can be subject to criminal charges for misinterpreting the law. This is particularly problematic for money laundering investigations, as the law is full of inconsistencies and contradictions, and is open to wide interpretation. For these reasons, prosecutors are often reluctant to pursue these types of investigations.

While traditional asset seizure continues to be employed by counternarcotics authorities, until recently the ultimate forfeiture of assets was problematic. Prior to 1996, Bolivian law permitted the sale of property seized in drug arrests only after the Supreme Court confirmed the conviction of a defendant. A 1995 decree permitted the sale of seized property with the consent of the accused and in certain other limited circumstances. The Directorate General for Seized Assets (DIRCABI) is responsible for confiscating, maintaining, and disposing of the property of persons either accused or convicted of violating Bolivia's narcotics laws. DIRCABI, however, has been poorly managed for years, and has only auctioned confiscated goods sporadically. In 2007, DIRCABI submitted a draft decree proposing changes in the existing law and procedures relating to asset seizure, forfeiture, and sharing. The President signed Decree 29305 on October 10, 2007. However, the decree does not correct problems related to the sharing of forfeited assets among law enforcement entities. DIRCABI initiated 485 cases in the first six months of 2007, with 16 bank accounts containing over $4 million subject to seizure or forfeiture.

The UIF, with judicial authorization, may also freeze accounts for up to 48 hours in suspected money laundering cases. To date, this law has only been applied on one occasion.

Although terrorist acts are criminalized under the Bolivian Penal Code, the GOB currently lacks legislation that criminalizes the financing of terrorism or grants the GOB the authority to identify, seize, or freeze terrorist assets. Nevertheless, the UIF distributes the terrorist lists of the United

Nations and the United States, receives and maintains information on terrorist groups, and can freeze suspicious assets under its own authority for up to 48 hours, as it has done in counternarcotics cases. The UIF created a draft terrorist financing law in 2006 and presented it to the Superintendence of Banks. However, the bill has not yet been presented to Congress.

The GOB's lack of terrorist financing legislation resulted in Bolivia's suspension from the Egmont Group of financial intelligence units on July 31, 2007. The Egmont Group amended its membership requirements in June 2004, requiring all member states to criminalize the financing of terrorism and their FIUs to receive STRs related to terrorist financing. Existing members, which included Bolivia, were given until June 2007 to draft terrorist financing legislation. Bolivia was the only Egmont member that had not drafted legislation by the deadline and as a result, the UIF was suspended from the Egmont Group. The suspension bars the UIF from participating in Egmont meetings or using the Egmont Secure Web (the primary means of information exchange among Egmont members) to share information with other FIUs. If the GOB does not take significant steps towards the criminalization of terrorist financing by June 2008, the UIF will be expelled from the Egmont Group.

The GOB is a member of GAFISUD, and its most recent mutual evaluation was conducted in April 2006. As a result of the GOB's failure to pay its membership dues for the past three years, GAFISUD placed sanctions on Bolivia in July and suspended its membership on December 1, 2007. The GOB made a partial payment of its arrears immediately following its December 1 suspension. At its December plenary meeting, GAFISUD agreed to reinstate Bolivia's membership, on the condition that the remainders of its debts are paid by July 2008. As a result of GAFISUD members' concerns regarding the GOB's failure to meet the FATF standards on combating money laundering and terrorist financing, the GAFISUD Secretariat sent a high level delegation to meet with senior GOB officials in November 2007.

Bolivia is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and GAFISUD. Bolivia is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption and the UN Convention against Transnational Organized Crime. The GOB has signed, but not ratified, the Inter-American Convention against Terrorism. The GOB and the United States signed an extradition treaty in June 1995, which entered into force in November 1996.

While the Government of Bolivia is taking some necessary steps to combat corruption, the GOB should ensure that any changes in its anti-corruption legislation strengthen its anti-money laundering regime. The GOB should also improve its current money laundering legislation so that it conforms to the standards of the FATF and GAFISUD. Money laundering should be an autonomous offense without requiring prosecution for the underlying predicate offense, and currently unregulated sectors should be subject to anti-money laundering and counter-terrorist financing controls. The GOB should criminalize terrorist financing in a timely manner and allow for the blocking of terrorist assets, to fulfill its international obligations. Doing so will also ensure that the UIF is not expelled from the Egmont Group. In addition to the need to make significant changes to the current laws, Bolivia should also ensure that the UIF and its potential replacement have sufficient staff and resources. The UIF should also have the authority to receive suspicious transaction reports on activities indicative of terrorist financing and reports from nonbank financial institutions. The GOB should also pay its GAFISUD dues to avoid being suspended from GAFISUD again. Finally, Bolivia needs to strengthen the relationships and cooperation between all government entities involved in the fight against money laundering and other financial crimes.

Bosnia and Herzegovina

Bosnia and Herzegovina (BiH) has a cash-based economy and is not an international, regional, or offshore financial center. The laundering of illicit proceeds derives from criminal activity including the proceeds from smuggling, corruption, and widespread tax evasion. Due to its porous borders and weak enforcement capabilities, BiH is a significant market and transit point for illegal commodities including cigarettes, narcotics, firearms, counterfeit goods, lumber, and fuel oils. BiH authorities have had some success over the past few years in clamping down on money laundering through the formal banking system. There are four active Free Trade Zones in BiH, with production based mainly on automobiles and textiles.

There are multiple jurisdictional levels in Bosnia and Herzegovina, including the State, the two entities (the Federation of Bosnia and Herzegovina and the Republika Srpska), and Brcko District. The Federation is further divided into ten cantons. Criminal and criminal procedure codes from the State, the two entities, and Brcko District were enacted and harmonized in 2003, although jurisdictions maintain their own enforcement bodies. Although state-level institutions are becoming more firmly grounded and are gaining increased authority, there remains a fair amount of confusion regarding jurisdictional matters between the entities and state-level institutions. Unless otherwise specified, relevant laws and institutions are at the state level.

Money laundering is a criminal offense in all state and entity criminal and criminal procedure codes. At the state level, the Law on the Prevention of Money Laundering determines the measures and responsibilities for detecting, preventing, and investigating money laundering and terrorist financing. The law also prescribes measures and responsibilities for international cooperation and establishes a financial intelligence unit (FIU) within the State Investigative and Protection Agency (SIPA). The law requires banks to submit suspicious financial transactions to the state-level FIU. Those convicted of money laundering exceeding the equivalent of $30,000 receive prison terms between one and ten years. For lesser amounts, the penalty is imprisonment between six months and five years.

The Law on the Prevention of Money Laundering requires twenty-six types of entities to report to the FIU all transactions of U.S. $18,000 or more as well as all transactions (regardless of amount) suspected of connections to money laundering or terrorist financing. The money laundering law applies to all banks, individuals and several nonbank financial institutions including post offices, investment and mutual pension companies, stock exchanges and stock exchange agencies, insurance companies, casinos, currency exchange offices and intermediaries such as lawyers and accountants. In addition to cash and suspicious transaction reporting requirements, the law requires that customs officials from the Indirect Tax Authority (ITA) forward to the FIU all reports of cross-border transportation of cash and securities in excess of $6,000. All banks have the ability to send electronic cash transaction reports (CTRs) and suspicious transactions reports (STRs) to the FIU, which then stores them in a central database. Although the law places reporting obligations on twenty-six types of entities, the banking sector and the ITA file the majority of reports, leaving a majority of the nonbank sector even more vulnerable to money laundering.

BiH has not enacted bank secrecy laws that prevent the disclosure of client and ownership information to bank supervisors and law enforcement authorities. The law requires banks and other financial institutions to know, record, and report the identity of customers engaging in significant transactions, including currency transactions above the equivalent of $18,000. Financial institutions must maintain records for twelve years to respond to law enforcement requests. Bosnian law protects reporting individuals with respect to law enforcement cooperation. Although there is no state-level banking supervision agency, entity level banking supervision agencies oversee and examine financial institutions for compliance with anti-money laundering and counter-terrorist financing laws and regulations. There is, however, no formal supervision mechanism in place for nonbank financial institutions and intermediaries. Nonbank financial transfers are reportedly very difficult for law

enforcement and customs officials to investigate. This is due not only to a lack of reporting, but also to a lack of understanding of indigenous methodologies, many of which are found in the underground economy and are enabled by smuggling and the misuse of trade .

Police at both the state and entity levels investigate financial crimes. At the state level, SIPA and the FIU are responsible for investigating financial crimes. In addition, the Federation Police has an Economic Crime Unit which focuses on public corruption, economic crimes, money laundering, and cyber crime. Although Republika Srpska (RS) police also investigate financial crimes, they do not have a specialized unit to handle such crimes. Both the Federation Police and the RS police lack adequate resources and training. In addition, both agencies acknowledge that the level of cooperation and information exchange with SIPA is poor and needs improvement.

The ITA suffers from a lack of resources and sufficiently trained personnel. BiH is largely a cash economy, and it is typical to carry large amounts of cash, even across borders. Bosnia and Herzegovina also receives significant remittances from emigrants. Official remittances constitute over 20 percent of GDP. While some of this will come into the country through bank transfers, others will also cross the border via courier.

The Financial Intelligence Department (FID), Bosnia-Herzegovina's FIU, is a hybrid body, performing analytical duties while maintaining limited criminal investigative responsibilities. The FID receives, collects, records, analyzes, and forwards information related to money laundering and terrorist financing to the State Prosecutor. It also provides expert support to the Prosecutor regarding financial activities and handles international cooperation on money laundering issues. Officially, the FID has access to the records of other government entities and formal mechanisms for inter-agency information sharing are in place. In practice, however cooperation between the FID and other government agencies is weak, with little information shared among agencies. This applies particularly to information sharing between the FID and the different police forces, as the banking agencies do share information with the FID. When suspicion of illicit activity exists, the FID has the power to freeze accounts for five days. During this time, if the FID is able to collect sufficient evidence of possible criminal activity, it may forward the case to the Prosecutor. At that point, the freeze on the accounts may be extended. The FID reports that it froze KM 752,439 (approximately U.S. $537,456) in six different cases during the first nine months of 2007.

The September 2006, International Monetary Fund's Financial System Stability Assessment report praised Bosnia Herzegovina for the progress made since MONEYVAL's 2005 mutual evaluation report. It cited in particular "the development of an effective state-level FIU." This has been augmented by the FID's hiring and training of several new analysts in late 2006. The report also cited the problems with information-sharing, coordination, and communication, as well as jurisdictional issues between the Financial Police and other State agencies.

In the first nine months of 2007, FID received 195,170 currency reports from banks and other financial institutions. Of these, the FID identified 57 cases as suspicious and investigated them. The FID submitted 12 reports to the BIH Prosecutor—eight related to money laundering and four related to other crimes such as abuse of position and tax evasion. Since BiH established its AML regime, there have been 28 confirmed convictions for money laundering. The FID is not the only active agency in the regime: the RS entity police agency and the Federation Financial Police, among others, all reported cases. In the first nine months of 2007, Bosnia-Herzegovina had seven convictions for money laundering.

BiH has no specific asset forfeiture law as regards money laundering, with the exception of the Persons Indicted for War Crimes (PIFWC) support laws which allow for the seizure of PIFWC assets or assets of those providing material support to them. Articles 110 and 111 of the BiH Criminal Code (along with similar laws in the harmonized entity and Brcko Criminal Codes) are the only legal provisions that authorize asset forfeiture. These provisions authorize the "confiscation of material

gain" (or a sum of money equivalent to the material gain if confiscation is not feasible) from illegal activity. The law does not provide for the seizure and forfeiture of assets that may have been used or facilitated the commission of the illegal activity. The courts administer confiscation, which can only take place as part of a verdict in a criminal case. The courts decide whether the articles will be "sold under the provisions applicable to judicial enforcement procedure, turned over to the criminology museum or some other institution, or destroyed. The proceeds obtained from sale of such articles shall be credited to the budget of Bosnia and Herzegovina." Prosecutors and courts do not have the administrative mechanisms in place to seize assets, maintain them in storage, dispose of them, or route the proceeds to the appropriate authorities. The government may seize property as punishment for criminal offenses for which a term of imprisonment of five years or more is prescribed. In such cases, asset seizure is possible without proving a specific relationship between the assets and the crime. There is no mechanism for civil forfeiture. There are no laws for sharing seized assets with other governments. BiH authorities have the authority to identify, freeze, seize, and forfeit terrorist-finance-related and other assets. The banking agencies (Federation and RS Banking Agencies) in particular have the capability to freeze assets without undue delay. The banking community cooperates with law enforcement efforts to trace funds and freeze accounts.

Article 202 of the criminal procedure code criminalizes terrorist financing. BiH is a party to the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Entity banking agencies are cognizant of the requirements to sanction individuals and entities listed by the UNSCR 1267 Sanctions Committee's consolidated list, but the state authorities do not regularly circulate this list to entity authorities. The U.S. Embassy, however, provides updates to appropriate entity authorities

In 2006, after a cooperative investigation between BiH and law enforcement authorities in several European Union countries, authorities initiated a prosecution at the Court of Bosnia and Herzegovina against five people suspected of terrorist crimes. Four of the defendants were found guilty in January 2007, and this verdict was affirmed by a three-judge appellate panel of the BiH State Court in June, making the verdict final and binding. In 2004, the government disrupted the operations of Al Furqan (aka Sirat, Istikamet), Al Haramain & Al Masjed Al Aqsa Charity Foundation, and Taibah International, organizations listed by the UNSCR 1267 Committee as having direct links with al-Qaida. Authorities continue to investigate other organizations and individuals for links to terrorist financing.

Bosnia and Herzegovina has no Mutual Legal Assistance Treaty with the U.S. BiH succeeded to the extradition treaty concluded between the Kingdom of Serbia and the United States in 1902; while this treaty covers some financial crimes, it does not address contemporary forms of money laundering. There is no formal bilateral agreement between the United States and BiH regarding the exchange of records in connection with narcotics investigations and proceedings. Authorities have made good faith efforts to exchange information informally with officials from the United States. BiH is a party to the 1988 UN Drug Convention (by way of succession from the former Yugoslavia), the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the UN International Convention for the Suppression of the Financing of Terrorism. Unfortunately, on many occasions, BiH has not passed implementing legislation for the international conventions to which it is a signatory.

The Government of Bosnia and Herzegovina (GOBH) should continue to strengthen institutions with responsibilities for money laundering prevention, particularly those at the state level. Due to a lack of resources and bureaucratic politics, SIPA and the FID, like many state institutions, remain under funded and under-resourced. The GOBH should make efforts to increase funding for its AML/CTF programs and enhance cooperation between concerned departments and agencies. Although prosecutors, financial investigators, and tax administrators have received training on tax evasion, money laundering and other financial crimes, the GOBH should provide training to ensure that they

understand diverse methodologies and aggressively pursue investigations. BiH authorities should undertake efforts to understand the illicit markets and their role in trade-based money laundering and alternative remittance systems. The banking agencies in BiH need to increase awareness by improving outreach programs with respect to compliance with AML/CTF regulations. Major vulnerabilities that they should address include the identification of shell companies and beneficial owners as well as the monitoring of NGO's. In addition, GOBH should implement a formal supervisory mechanism for nonbank financial institutions and intermediaries. The adoption of such a mechanism would help increase reporting in the nonbank sector, thereby reducing the vulnerability to money laundering that currently exists in that sector. BiH law enforcement and customs authorities should take additional steps to control the integrity of the border and limit smuggling. BiH should study the formation of centralized regulatory and law enforcement authorities and take specific steps to combat corruption at all levels of commerce and government. BiH should also adopt a comprehensive asset forfeiture law which provides a formal mechanism for the administration of seized assets, and should consider establishing a civil forfeiture regime. The government should enact implementing legislation for the international conventions to which it is a signatory

Brazil

Brazil is the world's fifth largest country in both size and population, and its economy is the tenth largest in the world. Due to its size and significant economy, Brazil is considered a regional financial center, although it is not an offshore financial center. Brazil is also a major drug-transit country. Brazil maintains adequate banking regulations, retains some controls on capital flows, and requires disclosure of the ownership of corporations. Brazilian authorities report that money laundering in Brazil is primarily related to domestic crime, especially drug trafficking, corruption, organized crime, and trade in contraband, all of which generate funds that may be laundered through the banking system, real estate investment, financial asset markets, luxury goods or informal financial networks. However, use of the Brazilian financial system to launder the proceeds of foreign criminal activity also persists. For example, Colombian narcotics trafficker Juan Carlos Ramirez Abadia, who is currently pending extradition to the United States, laundered millions in Norte Valle drug cartel proceeds through Brazil.

A primary source of criminal activity and contraband is the Tri-Border Area (TBA) shared by Argentina, Brazil, and Paraguay. Brazilian authorities have expressed particular concern over the trafficking in arms and drugs in the TBA. Brazilian authorities note that the proceeds of domestic drug trafficking and organized crime feed a regional arms trade, operating in the TBA. In addition, a wide variety of counterfeit goods, including cigarettes, compact discs (CDs), digital versatile discs (DVDs), and computer software, are smuggled across the border from Paraguay into Brazil; a significant portion of these counterfeit goods originate in Asia. The U.S. Government believes the TBA to be a source of terrorist financing, although the Government of Brazil (GOB) maintains that it has not seen any evidence of such. In recent years, the GOB has enhanced its border controls in the TBA, particularly at the Foz do Iguacu border crossing, in an attempt to combat the significant inflow of contraband goods and subsequent tax revenue loss.

The GOB has a comprehensive anti-money laundering regulatory regime in place. Law 9.613 of 1998 criminalizes money laundering related to drug trafficking, terrorism, arms trafficking, extortion by kidnapping, crimes against the public administration or the national financial system, and organized crime, and penalizes offenders with a maximum of 10 years in prison. The law expands the GOB's asset seizure and forfeiture provisions, and exempts "good faith" compliance from criminal or civil prosecution. Regulations issued in 1998 require that individuals transporting more than 10,000 reais (then approximately U.S. $10,000, now approximately U.S. $5,500) in cash, checks, or traveler's checks across the Brazilian border must fill out a customs declaration that is sent to the Central Bank.

Law 10.467 of 2002, which modifies Law 9.613, put into effect Decree 3.678 of 2000, thereby penalizing active corruption in international commercial transactions by foreign public officials. Law 10.467 also adds penalties for this offense under Chapter II of Law 9.613. Law 10.701 of 2003, which also modifies Law 9.613, establishes terrorist financing as a predicate offense for money laundering. The law also establishes crimes in foreign jurisdictions as predicate offenses, requires the Central Bank to create and maintain a registry of information on all bank account holders, and enables the Brazilian financial intelligence unit (FIU) to request from all government entities financial information on any subject suspected of involvement in criminal activity.

Law 9.613 establishes Brazil's FIU, the Conselho de Controle de Atividades Financeiras (COAF), which is housed within the Ministry of Finance. The COAF includes representatives from regulatory and law enforcement agencies, including the Central Bank and Federal Police. The COAF regulates those financial sectors not already under the jurisdiction of another supervising entity. Currently, the COAF has a staff of 42, comprised of 20 analysts, two international organizations specialists, a counterterrorism specialist, two lawyers, and support staff.

Since 1999, the COAF has issued a series of regulations that require customer identification, record keeping, and reporting of suspicious transactions to the COAF by obligated entities. Entities that fall under the regulation of the Central Bank, the Securities Commission (CVM), the Private Insurance Superintendence (SUSEP), and the Office of Supplemental Pension Plans (PC) file suspicious activity reports (SARs) with their respective regulator, either in electronic or paper format. The regulatory body then electronically submits the SARs to COAF. Entities that do not fall under the regulations of the above-mentioned bodies, such as real estate brokers, money remittance businesses, factoring companies, gaming and lotteries, dealers in jewelry and precious metals, bingo, credit card companies, commodities trading, and dealers in art and antiques, are regulated by the COAF and send SARs directly to COAF, either via the Internet or using paper forms.

In addition to filing SARs, banks are also required to report cash transactions exceeding 100,000 reais (approximately $55,000) to the Central Bank. The lottery sector must notify COAF of the names and data of any winners of three or more prizes equal to or higher than 10,000 reais within a 12-month period. COAF Resolution 14 of 2006 further extended these anti-money laundering requirements to the real estate sector. The insurance regulator, SUSEP, clarified its reporting requirements for insurance companies and brokers in Circular 327 of May 2006, which requires these entities to have an anti-money laundering program and report large insurance policy purchases, settlements or otherwise suspicious transactions to both SUSEP and COAF. In addition, on January 8, 2008, the Securities Commission (CVM) extended anti-money laundering requirements to additional entities, including luxury goods dealers and persons or companies that conduct business activities involving a large volume of cash.

Since 2006, the COAF, Central Bank, SUSEP, and the Pension Funds Secretariat have issued resolutions and circulars mandating the reporting of suspected terrorist financing activity, and the reporting of suspicious or large cash transactions by politically exposed persons (PEPs). The Central Bank issued Circular 3339 in December 2006, defining procedures for monitoring the financial accounts of PEPs. SUSEP Circular 21 of December 2006 addresses reporting procedures for transactions and possible transactions linked to terrorism and terrorist financing. SUSEP Circular 341, issued April 30, 2007, amends Circular 327 of May 2006, and includes procedures to be observed regarding PEPs. On March 28, 2007, COAF issued Resolutions 15 and 16, which respectively expand reporting requirements regarding suspected terrorist financing and transactions by PEPs. The Pension Funds Secretariat published new rules on PEPs on December 11, 2007, through Circular Letter SPC 18/2007.

The COAF has direct access to the Central Bank database, so that it has immediate access to the SARs and cash transaction reports (CTRs) filed with the Central Bank. The COAF also has access to a wide

variety of government databases. The COAF may request additional information directly from the entities it supervises and the supervisory bodies of other obligated entities. Complete bank transaction information may be provided to government authorities, including the COAF, without a court order. Domestic authorities that register with the COAF may directly access the COAF databases via a password-protected system. In 2007, the COAF received 50,320 CTRs and 18,960 SARs per month. In 2007, the COAF sent 1,555 reports to law enforcement authorities for further investigation, and responded to 1,047 requests for information received from law enforcement and prosecutorial authorities in the last year.

The Central Bank has established the Departamento de Combate a Ilícitos Cambiais e Financeiros (Department to Combat Exchange and Financial Crimes, or DECIC) to implement anti-money laundering policy, examine entities under the supervision of the Central Bank to ensure compliance with suspicious transaction reporting, and forward information on the suspect and the nature of the transaction to the COAF. In 2005, the DECIC brought on-line a national computerized registry of all current accounts (e.g., checking accounts) in the country. The COAF also has access to this database. Banks must report identifying data on both parties for all foreign exchange transactions and money remittances, regardless of the amount of the transaction.

The GOB has institutionalized its national strategy for combating money laundering, holding its fifth annual high-level planning and evaluation session in November 2007. At these sessions, the GOB defines annual goals within the scope of its overall strategy that aims to advance six strategic goals: improve coordination of disparate federal and state level anti-money laundering efforts, utilize computerized databases and public registries to facilitate the fight against money laundering, evaluate and improve existing mechanisms to combat money laundering, increase international cooperation to fight money laundering and recover assets, promote an anti-money laundering culture, and prevent money laundering before it occurs. The national anti-money laundering strategy has put in place more regular coordination and clarified the division of labor among various federal agencies involved in combating money laundering. In 2006, following a number of high-level corruption cases, the national strategy was expanded to include anti-corruption initiatives as well.

In 2003, the GOB created specialized money laundering courts. Fifteen of these courts have been established in 14 states, including two in Sao Paulo, with each court headed by a judge who receives specialized training in national money laundering legislation. A 2006 national anti-money laundering strategy goal aimed to build on the success of the specialized courts by creating complementary specialized federal police financial crimes units in the same jurisdictions. During November 2007, two judges, a prosecutor and investigator visited the United States as part of an International Visitor Leadership Program to gain information on the U.S. regime for combating money laundering.

Brazil has a limited ability to employ advanced law enforcement techniques such as undercover operations, controlled delivery, and the use of electronic evidence and task force investigations that are critical to the successful investigation of complex crimes, such as money laundering. Generally, such techniques can be used only for information purposes, and are not admissible in court. In 2007, the Ministry of Justice, working through its National Program of Citizens' Public Security (PRONASCI), entered into agreements to establish money laundering forensic laboratories in the Federal District and the states of Rio de Janeiro and Sao Paulo as part of an overall plan to establish ten such facilities in states throughout the country by the end of 2008.

GOB reports appeared to indicate a reversal in 2007 of the upward trend, begun in 2003, of annual growth in the number of money laundering investigations, trials, and convictions. However, the Ministry of Justice indicated that it changed its methodology in 2007 for calculating these statistics to more accurately reflect the number of investigations, trials, and convictions. The Ministry of Justice is currently working to convert data from previous years to correspond to this new methodology, which

it expects will lower results from past years. In 2007, there were 590 investigations, 37 trials, and 190 convictions.

Brazil has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets. The COAF and the Ministry of Justice manage these systems jointly. Police authorities and the customs and revenue services are responsible for tracing and seizing assets, and have adequate police powers and resources to perform such activities. A GOB computerized registry of all seized assets to improve tracking and disbursal is currently being tested and is now in the pilot phase. The judicial system has the authority to forfeit seized assets, and Brazilian law permits the sharing of forfeited assets with other countries.

A COAF-supported amendment, PLS 209, to Law 9.613 was introduced to the legislature in 2003. The bill has passed in the Chamber of Deputies, and is currently in the Senate for consideration. COAF expects the amendment to pass in 2008. If passed, PLS 209 would expand the definition of money laundering to encompass additional predicate offenses, such as tax evasion and trafficking in persons. It would also expand the scope of Law 9.613 to cover games of chance, slot machines and the clandestine art trade; tighten bank secrecy rules; and enhance cooperation between the public prosecutor's office and the COAF. A Senate-proposed amendment to PLS 209 would include penalties for those who finance or collect funds for the purpose of causing crimes that result in widespread panic or constrain the state. The Senate amendments would also require the financial sector to adopt stricter anti-money laundering controls, require attorneys and accountants to report suspicious transactions, and increase the maximum penalty for involvement in money laundering activities from ten to 18 years imprisonment.

Although terrorist financing is considered to be a predicate offense for money laundering under Law 10.701 of 2003, terrorist financing is not an autonomous crime. There have been no money laundering prosecutions to date in which terrorist financing was a predicate offense, and so it remains to be seen if the financing of terrorism could be contested as an enforceable predicate offense due to the lack of legislation specifically criminalizing it. If the Senate-proposed amendment to PLS 209 is adopted, its passage should bring the GOB into greater compliance with the anti-money laundering and counter-terrorist financing standards of the Financial Action Task Force (FATF) and the Egmont Group of financial intelligence units.

The GOB has generally responded to U.S. efforts to identify and block terrorist-related funds. Since September 11, 2001, the COAF has run inquiries on hundreds of individuals and entities, and has searched its financial records for entities and individuals on the UNSCR Sanctions Committee's consolidated list. None of the individuals and entities on the consolidated list has been found to be operating or executing financial transactions in Brazil, and the GOB insists there is no evidence of terrorist financing in Brazil.

On December 6, 2006, the U.S. Department of Treasury placed nine individuals and two entities in the Tri-Border Area that have provided financial or logistical support to Hezbollah on its list of Specially Designated Nationals. The nine individuals operate in the Tri-Border Area and all have provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was previously designated by the U.S. Treasury in June 2004 for his support to Hezbollah leadership. The two entities, Galeria Page and Casa Hamze, are located in Ciudad del Este, Paraguay, and have been used to generate or move terrorist funds. The GOB has publicly disagreed with the designations, stating that the United States has not provided any new information that would prove terrorist financing activity is occurring in the Tri-Border Area.

In 2001, the Mutual Legal Assistance Treaty between Brazil and the Government of the United States (USG) entered into force, and a bilateral Customs Mutual Assistance Agreement, which was signed in 2002, entered into force in 2005. Using the Customs Agreement framework, the GOB's tax and customs authority (Receita Federal) and U.S. Immigration and Customs Enforcement (ICE)

established a trade transparency unit (TTU) in 2006 to detect trade-based money laundering. In 2007, Receita conducted five investigations with other law enforcement agencies, resulting in 108 arrests and 5 convictions. ICE and the Brazilian Federal Police currently have two major on-going investigations into trade-based money laundering activities. Future plans include an upgrade of USG and GOB program-related computer systems and USG-sponsored training for Receita officials.

Brazil is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention against Terrorism. Brazil is a member of the FATF and the Financial Action Task Force for South America (GAFISUD). The GOB will hold the presidency of the Financial Action Task Force (FATF) in 2008, and the COAF's director will assume the role of FATF president. Brazil is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The COAF has been a member of the Egmont Group since 1999. The GOB also participates in the "3 Plus 1" Security Group between the United States and the Tri-Border Area countries.

The Government of Brazil should criminalize terrorist financing as an autonomous offense. To continue to successfully combat money laundering and other financial crimes, Brazil should also ensure the passage of legislation to regulate the sectors in which money laundering is an emerging issue. Brazil should enact and implement legislation to provide for the effective use of advanced law enforcement techniques, to provide its investigators and prosecutors with more advanced tools to tackle sophisticated organizations that engage in money laundering, financial crimes, and terrorist financing. Brazil should also enforce currency controls and cross-border reporting requirements, particularly in the Tri-Border region. Additionally, the GOB and the COAF should continue to fight against corruption and ensure the enforcement of existing anti-money laundering laws.

British Virgin Islands

The British Virgin Islands (BVI) is a Caribbean overseas territory of the United Kingdom (UK). The BVI remains vulnerable to money laundering, primarily due to drug trafficking and its significant offshore financial services industry. As of June 2007, the BVI has approximately nine banks, 2,550 active mutual funds, 19 local insurance companies, 402 captive insurance companies, 208 trust licenses, seven authorized custodians, 18 company management companies, 100 registered agents, 430 limited partnerships, 10,666 local companies, and 802,850 BVI business companies or international business companies (IBCs).

The BVI International Finance Centre (BVI IFC) was created in 2002 under the Ministry of Finance and Economic Development to promote and market the BVI as an offshore financial center. The BVI IFC recently announced a new outreach program that includes "ambassadors" from the public and private sectors. The "ambassadors" include senior executives and officials from the private sector and the government, including regulators. These individuals will promote the BVI's offshore regime at select trade shows, international conferences, media interviews, and networking events.

The International Business Companies Act (IBCA) of 1984 was created to facilitate companies wishing to conduct international transactions from a tax exempt environment. According to the IBCA, IBCs registered in the BVI cannot engage in business with BVI residents, provide registered offices or agent facilities for BVI-incorporated companies, or own an interest in real property located in the BVI (except for office leases). All IBCs must be registered in the BVI by a registered agent; and the IBC or the registered agent must maintain an office in the BVI. The process for registering banks, trust companies, and insurers is governed by legislation that requires detailed documentation, such as a business plan and vetting by the appropriate supervisor within the Financial Services Commission (FSC). Registered agents must verify the identities of their clients.

As a UK overseas territory, the Government of the British Virgin Islands (GOBVI) has to comply with the European Union Code of Conduct on Business Taxation. The code, among other things, requires that local and offshore companies be treated equally for tax purposes. To address this, and to update the BVI companies' legislation, the BVI Business Companies Act (BCA) 2004 came into force in 2005. The BCA superseded the IBCA act in January 2007, and now exclusively regulates all companies incorporated in the BVI. The BCA retains many of the same requirements of the IBCA including exemption from BVI taxes, privacy of directors and share registries, no director member residency requirements, and no requirement to file accounts or retain visible and tangible evidence of incorporation. The BCA places all companies, offshore and onshore, within a zero tax regime. Companies registered under the IBCA were provided a two-year transition period. During this period, IBCs had the option of re-registering as business companies under the BCA. Any IBC that did not re-register was automatically re-registered as a business company on January 1, 2007.

While the IBCA only permitted the incorporation of companies limited by shares, the BCA offers seven different types of companies: companies limited by shares, which is the most widely used vehicle; companies limited by guarantee authorized to issue shares, which are typically used for structuring transactions by combining equity and guarantee membership; companies limited by guarantee not authorized to issue shares; unlimited companies that are authorized to issue shares; unlimited companies that are not authorized to issue shares; restricted purposes companies, which are used primarily in structured finance and securitization transactions; and segregated portfolio companies, which are presently limited to insurance companies and mutual funds. The BCA permits the use of numbered names for businesses, i.e. BVI Company # (followed by a number). If a company chooses this format, it will also be permitted to have a foreign character name; an English translation of the name is not required. The BVI reports that Asian countries continue to be a high user of BVI companies, and predicts that the use of BVI companies by Asian countries will increase in the future.

The Financial Services Commission (FSC) is the independent regulatory authority responsible for the licensing and supervision of regulated entities, which include banking and fiduciary businesses, investment businesses, insolvency services, accountants, insurance companies, and company management and registration businesses. Money remitters, however, are not subject to licensing or supervision. The FSC is also responsible for on-site inspections of these entities. The FSC instituted a new penalty regime in 2007. The Financial Services (Administrative Penalties) Regulations went into effect in January 2007, and are intended to deter and penalize regulated entities that are found to be noncompliant with BVI regulatory laws. The lowest penalty that may be imposed is $100 and the highest is $20,000.

The FSC cooperates with its foreign counterparts and law enforcement agencies. In 2000, the Information Assistance (Financial Services) Act (IAFSA) was enacted to increase the scope of cooperation between the BVI's regulators and regulators from other countries. In 2007, the FSC published the Handbook on International Cooperation and Information Exchange. The Handbook is publicly available via the FSC's website and explains the statutory mandates and regulations established in the BVI to facilitate and improve international cooperation.

The Proceeds of Criminal Conduct Act 1997 (POCCA) criminalizes money laundering in the BVI. The POCCA establishes all indictable offences except drug trafficking as predicates for money laundering; drug trafficking predicated money laundering is established under similar provisions in the Drug Trafficking Offences Act 1992. The Proceeds of Criminal Conduct (Amendment) Act, 2006 mandates financial institutions and other providers of financial services to report suspected money laundering transactions. The POCCA allows the BVI Court to grant confiscation orders against those convicted of an offense or who have benefited from criminal conduct. Although procedures exist for the freezing and confiscation of assets linked to criminal activity, including money laundering and terrorist financing, the procedures for the forfeiture of assets that are not directly linked to narcotics-related crimes are unclear.

The POCCA mandates the creation of a financial intelligence unit (FIU), the Reporting Authority. The Financial Investigation Agency Act 2003 reorganizes and renames the FIU. The Financial Investigation Agency (FIA) is responsible for the collection, analysis, investigation, and dissemination of financial information. The FIA receives approximately 200 suspicious transaction reports (STRs) annually. The FIA's staff is comprised of a director, two senior police officers, one senior customs officer, a chief operating officer, and an administrative assistant. A Board is responsible for setting the policy framework under which the FIA operates. The Board members include the Deputy Governor as chairperson, the Attorney General, the Financial Secretary, Managing Director/CEO of the Financial Services Commission, Commissioner of Police, and Comptroller of Customs. The FIA has a memorandum of understanding (MOU) with the FSC to facilitate information exchange between the two agencies. The FIA exchanges information with foreign counterpart FIUs, and does not require an MOU.

In 2007, the FIA Act was amended to redefine the FIA's responsibilities to include investigation and analysis of any offense in relation to money laundering and terrorist financing, although the financing of terrorism is not an offense in the BVI. The amendment gave the FIA authority to receive disclosures of suspected terrorist financing. It also empowered the FIA to investigate matters relating to the breach of any domestic or international sanction prescribed by or under any enactment.

The Joint Anti-Money Laundering Coordinating Committee (JAMLCC) coordinates all anti-money laundering initiatives in BVI. The JAMLCC is a broad-based, multi-disciplinary body comprised of private and public sector representatives. In December 2000, the Anti-Money Laundering Code of Practice of 1999 (AMLCP) entered into force. The AMLCP establishes procedures to identify suspicious transactions and report them to the FIA. Obligated entities are protected from liability for reporting suspicious transactions. The AMLCP also requires covered entities to create a clearly defined reporting chain for employees to follow when reporting suspicious transactions, and to appoint a reporting officer to receive these reports. The reporting officer must conduct an initial inquiry into the suspicious transaction and report it to the authorities, if sufficient suspicion remains. Failure to report could result in criminal liability. The JAMLCC, in conjunction with the FIA, are currently revising anti-money laundering and counter-terrorist financing guidelines.

The United Kingdom's Terrorism (United Nations Measures) (Overseas Territories) Order 2001 and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002 extend to the BVI. The Afghanistan (United Nations Sanctions) (Overseas Territories) Order 2001 and the Al-Qaida and Taliban (United Nations Measures) (Overseas Territories) Order 2002 also apply to the BVI. However, the BVI has not specifically criminalized the financing of terrorism.

The BVI is a member of the Caribbean Financial Action Task Force (CFATF) and will undergo a mutual evaluation in 2008. The BVI is an Observer to the Offshore Group of Supervisors. The FIA is a member of the Egmont Group, and participates in the Egmont Training Working Group. The BVI is subject to the 1988 UN Drug Convention and, as a British Overseas Territory, has implemented measures in accordance with this convention and the UN Convention against Transnational Organized Crime. The UK extended the application of the UN Convention against Corruption to the BVI in October 2006. Application of the U.S.-UK Mutual Legal Assistance Treaty (MLAT) concerning the Cayman Islands was extended to the BVI in 1990. If an MLAT request's subject matter falls within the FIA's purview, it is forwarded to the FIA for further investigation after it is received and reviewed by the Office of the Attorney General.

The Government of the British Virgin Islands should criminalize the financing of terrorism. The GOBVI should continue to strengthen its anti-money laundering regime by fully implementing its programs and legislation. The BVI should also extend the provisions of its anti-money laundering and counter-terrorist financing regulations to a wider range of entities, including money remitters. The GOBVI should ensure that there are a sufficient number of regulators and examiners to exercise

effective due diligence and regulation of its more than 800,000 offshore entities in a manner compliant with international standards.

Bulgaria

Bulgaria is not considered an important regional financial center or an offshore financial center. Its significance in terms of money laundering stems from its geographical position, its well-developed financial sector relative to other Balkan countries, and its relatively lax regulatory control. Although Bulgaria is a major transit point for drugs into Western Europe, it is unknown whether drug trafficking constitutes the primary generator of criminal proceeds and subsequent money laundering in Bulgaria. Financial crimes, including fraud schemes of all types, smuggling of persons and commodities, and other organized crime offenses also generate significant proceeds susceptible to money laundering. Although Bulgaria is primarily a cash economy, ATM and credit card fraud remain serious problems. Tax fraud is prevalent. The sources for money laundered in Bulgaria likely derive from both domestic and international criminal activity. In some cases, organized crime groups, which in the past have operated openly in Bulgaria, are moving into legitimate business operations or even slowly legitimizing themselves, making it difficult to trace the origins of their wealth. Public officials, watchdog institutions, and journalists who challenge organized crime operations often feel intimidated. Smuggling remains a problem in Bulgaria, sustained by ties with shady financiers and corrupt businessmen. While counterfeiting of currency, negotiable instruments, and identity documents has historically been a serious problem in Bulgaria, joint activities by the Government of Bulgaria (GOB) and the U.S. Secret Service have contributed to a decline in counterfeiting in recent years. There has been no indication that Bulgarian financial institutions engage in narcotics-related currency transactions involving significant amounts of U.S. currency or otherwise affecting the United States.

With support and pressure from the United States, the European Union (EU), and nongovernmental organizations (NGOs), the government has continued efforts to address the operation of duty free shops and petrol stations as a funding source for the gray economy and as a conduit for the smuggling of excise goods. Duty free shops play a major role in cigarette smuggling in Bulgaria, as well as smuggling of alcohol, and to a lesser extent perfume and other luxury goods. Attempts by the Ministry of Finance (MOF) to close down all duty free shops and petrol stations operating in Bulgaria have been unsuccessful, in large part due to political opposition within the ruling coalition. Bulgaria's January 2007 accession to the EU mandated the country close nine duty free shops and six petrol stations operating at Bulgaria's borders with neighboring EU countries. However, in December 2006, the Bulgarian Parliament granted permanent licenses for duty free trade to all existing operators and allowed them to relocate businesses to Bulgaria's external nonEU borders. A substantial portion of excise goods sold at duty-free shops and stations stay within the country avoiding taxation. Analysts describe this scheme as protected smuggling, which results in significant losses for the state budget.

While duty free shops and petrol stations are largely perceived as tools to violate customs and tax regimes, duty free shops may be used to facilitate other crimes, including financial crimes. Credible allegations have linked duty free trade in Bulgaria to organized crime interests involved in fuel smuggling, forced prostitution, the illicit drug trade, and human trafficking. There is no indication, of links between duty free shops or free trade areas and terrorist financing. The MOF's Customs Agency and General Tax Directorate have supervisory authority over the duty free shops. According to some NGOs, reported revenues and expenses by the shops have clearly included unlawful activities, in addition to duty free trade. Good procedures for identifying unlawful activity are lacking. MOF inspections have revealed that it is practically impossible to monitor whether customers at the numerous duty free shops have actually crossed an international border.

Article 253 of the Bulgarian Penal Code criminalizes money laundering. Amendments made to the Penal Code in 2006 increase penalties (including in cases of conspiracy and abuse of office), clarify that predicate crimes committed outside Bulgaria can support a money laundering charge brought in Bulgaria, and allow prosecution on money laundering charges without first obtaining a conviction for the predicate crime. Article 253 criminalizes money laundering related to all crimes. As such, drug trafficking is but one of many recognized predicate offenses.

The Law on Measures against Money Laundering (LMML) is the legislative backbone of Bulgaria's anti-money laundering regime. The LMML was adopted in 1998 and has since been amended several times, most recently in 2007. Bulgaria has strict and wide-ranging banking, tax, and commercial secrecy laws that limit the dissemination of financial information absent the issuance of a court order. Bulgaria's financial intelligence unit (FIU), the Financial Intelligence Agency (FIA), is the main administrative unit for collecting and analyzing information on suspected money laundering transactions. Unlike all other government institutions, the FIU is not bound by the typical secrecy provisions that are often cited as an impediment to law enforcement functions. In an effort to lessen the impact of secrecy laws on law enforcement functions, in 2006, the GOB issued amendments to both the LMML and the Law on Credit Institutions. The amendments to the Law on Credit Institutions facilitate the investigation and prosecution of financial crimes by giving the Prosecutor General the right to request financial information from banks without a court order in cases involving money laundering and organized crime. The FIA does not participate in criminal investigations.

Prior to December 2007, the FIA was a fully independent agency operating under the MOF, with the independence of the FIA director being guaranteed by the LMML. It had the authority to perform onsite compliance inspections, obtain information without a court order, share all information with law enforcement, and receive reports of suspected terrorist financing. However, on December 11, 2007, the Parliament passed legislation, which came into force on January 1, 2008. This law, the Act on the State Agency for National Security, established a new national intelligence agency, the State Agency for National Security (SANS). The law also restructures the FIA by changing its status from an independent agency within the MOF to a directorate within the SANS. The legislation lacks clarity regarding the new FIU's autonomy, operational status, and ability to exchange information consistent with international standards. The FIU's ability to conduct on-site inspections as well as its free access all government databases has been removed. In addition, the analytical capacity of FIA is not precisely defined: the SANS law permits the FIU to acquire and handle national security-related information, but financial crimes information is not necessarily of national security importance. The FIA is no longer an individual legal entity with its own budget. The status of the joint instructions signed between FIA and other government organizations such as the Ministry of Interior and the Prosecution Service is now unclear. The FIA's authority to exchange information with international partners, which was explicitly provided for in the LMML, has been removed. Exchange of classified information with other Bulgarian agencies is not clearly defined.

Although the oversight and other authorities of the new FIU are set to be addressed in supplemental legislation or implementing regulations that are to be drafted by March 2008, each of the legal gaps listed above potentially undermines the financial intelligence unit's ability to execute its mission and uphold its international commitments. As such, in January 2008, the Egmont Group temporarily suspended Bulgaria's access to their secure information exchange system, pending further clarification of the FIU's proposed structure and operational capacities.

Banks and the 29 other reporting entities under the LMML are required to apply "know your customer" (KYC) standards. Since 2003, all reporting entities are required to ask for the source of funds in any transaction greater than 30,000 BGN (approximately $22,500) or foreign exchange transactions greater than 10,000 BGN (approximately $7,500). Reporting entities are also required to notify the FIA of any cash payment greater than 30,000 BGN ($22,500). Current reporting requirements do not mandate that banks and other reporting entities report the actual amounts involved

in a currency transaction greater than 30,000 BGN ($22,500); they are only required to report the fact that such a transaction occurred. Concerted action by NGOs and others is underway to convince the MOF and the Bulgarian National Bank (BNB) to change the law so as to require reporting of the actual amount of the transaction.

The LMML obligates financial institutions to a five-year record keeping requirement and provides a "safe harbor" to reporting entities. Penal Code Article 253B was enacted in 2004 to establish criminal liability for noncompliance with LMML requirements. Although case law remains weak, Bulgaria's anti-money laundering legislation was determined to be in full compliance with all EU standards when it was assessed in September 2003 for purposes of EU accession.

In 2006, the Ministry of the Interior (MOI), the Prosecutor's Office, and the FIA signed a joint instruction establishing new procedures for closer cooperation when following leads contained in a suspicious transaction report (STR). A 2007 supplement to the instruction institutes a political-level contact group comprised of high-level representatives of the three institutions to improve cooperation. As of October 2007, the group had held two meetings to discuss cooperation mechanisms and improved protection of the reporting entities' employees. Reports prepared by FIA were forwarded to the Prosecutor General with a copy for the MOI, which subsequently produced a report on the enforcement potential of the case within 30 days of receipt.

From January 2007 through October 2007, the FIA received 293 STRs on money laundering, totaling 219,291,944 BGN (approximately $161,244,000). The FIA also received one STR on suspected terrorist financing activity. During the same period, the FIA received 158,000 currency transaction reports (CTRs). On the basis of the forwarded reports, 249 cases valued at 219,191,944 BGN (approximately $161,170,000) were opened, 15 cases valued at 35,309,072,BGN (approximately $26,000 000) were referred to the Supreme Prosecutor's Office of Cassation, and 203 cases valued at 151,337,126 BGN (approximately $111,278,000) were referred to the Ministry of Interior and copied to the Supreme Cassation Prosecution.

In response to pressure from the EU, in 2006, Bulgaria's Parliament tightened the LMML with further amendments. These amendments expanded the definition of money laundering and the list of reporting entities; outlawed anonymous bank accounts; expanded the definition of "currency"; and required the disclosure of source for currency exported from the country Under the LMML, 30 categories of entities, including lawyers, real estate agents, auctioneers, tax consultants, and security exchange operators, are required to file suspicious transactions reports. The banking sector has substantially complied with the law's filing requirement. Reporting by other sectors, however, has been much lower. Historic lower rates of reporting compliance by exchange bureaus, casinos, and other nonbank financial institutions can be attributed to numerous factors, including a lack of understanding of or respect for legal requirements, lack of inspection resources, and the general absence of effective regulatory control over the nonbank financial sector.

Following the 2006 amendments to the LMML, which instituted compliance checks for the nonbanking sector, the FIA noted a slight improvement in reporting. As of October 2007, the FIA inspected four banks, 19 exchange offices, 14 financial houses, three insurance companies, eight investment intermediaries, four casinos, 10 public notaries, four leasing undertakings, six car dealers, five sports organizations, one wholesale dealer, and eight real estate agents in 2007, imposing fines in 42 cases. Most of the violations disclosed were for failure to declare the origin of funds, perform identification procedures for clients, or report transactions over 30,000 BGN (approximately $22,500). The National Revenue Agency also conducted 509 on-site inspections of exchange offices.

In October 2006, the courts rendered the country's first two convictions for money laundering In 2007, money laundering convictions increased, reaching 11 by October. A total of 25 people were indicted on money laundering charges. Only four of the initiated cases ended in acquittal and nine were awaiting a court's decision.

Although there are few indications of terrorist financing directly connected with Bulgaria, the possibility remains that terrorism-related funds can transit across Bulgarian borders through cash couriers and other informal mechanisms. Article 108a of the Penal Code criminalizes terrorism and terrorist financing. Article 253 of the Criminal Code qualifies terrorist acts and terrorist financing as predicate crimes under the "all crimes" approach to money laundering. In February 2003, the GOB enacted the Law on Measures Against Terrorist Financing (LMATF), which links counterterrorism measures with financial intelligence, and compels all covered entities to report any suspicion of terrorist financing or pay a penalty of up to 50,000 BGN (approximately $37,500). The law is consistent with Financial Action Task Force (FATF) Nine Special Recommendations on Terrorist Financing, and authorizes the FIA to use its resources and financial intelligence to combat terrorist financing along with money laundering.

Under the LMATF, the GOB may freeze the assets of a suspected terrorist for 45 days. Key players in the process of asset freezing and seizing, as prescribed in existing law, include the MOI, MOF (including the FIA), Council of Ministers, Supreme Administrative Court, Sofia City Court, and the Prosecutor General. The FIA and the Bulgarian National Bank circulate the names of suspected terrorists and terrorist organizations, as found on the UNSCR 1267 Sanctions Committee's Consolidated List, as well as the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224, and those designated by the relevant EU authorities. To date, no suspected terrorist assets have been identified, frozen, or seized by Bulgarian authorities.

Although alternative remittance systems may operate in Bulgaria, their scope is unknown and there are no reported initiatives underway to address them. In general, regulatory controls over nonbank financial institutions are weak, with some of those institutions engaging in banking activities absent any regulatory oversight. Some anecdotal evidence suggests that charitable and nonprofit legal status is occasionally used to conceal money laundering.

The Bulgarian Penal Code provides legal mechanisms for forfeiting assets (including substitute assets in money laundering cases) and instrumentalities. Both the money laundering and the terrorist financing laws include provisions for identifying, tracing, and freezing assets related to money laundering or the financing of terrorism. A new criminal asset forfeiture law, targeted at confiscation of illegally acquired property, came into effect in March 2005. The law permits forfeiture proceedings to be initiated against property valued in excess of 60,000 BGN (approximately $45,100) if the owner of the property is the subject of criminal prosecution for enumerated crimes (terrorism, drug trafficking, human trafficking, money laundering, bribery, major tax fraud, and organizing, leading, or participating in a criminal group) and a reasonable assumption can be made that the property was acquired through criminal activity. As required by the law, an Assets Identification Commission was established and became operational in 2006. The Commission has the authority to institute criminal asset identification procedures, as well as request from the court both preliminary injunctions and ultimately the forfeiture of assets. As of March 2007, the Commission has filed with the court 38 injunction requests for property valued at 19,037,365 BGN (approximately $14.2 million) and 10 forfeiture requests for property valued at 3,453,783 BGN (approximately $2.5 million)

In September 2007, the United States and Bulgaria signed a mutual legal assistance treaty (MLAT), implementing the U.S.-EU Mutual Legal Assistance Agreement, which has yet to come into force. The 2005 ratification of the UN Convention against Transnational Organized Crime by the U.S. established an MLAT-type relationship between the two countries (Bulgaria having ratified the Convention in 2001). As of October 2007, the FIA had bilateral memoranda of understanding (MOU) regarding information exchange relating to money laundering with 28 countries. The FIA is authorized by law to exchange financial intelligence on the basis of reciprocity without the need of an MOU. As of October 2007, the FIA sent 261 requests for information to foreign FIUs and received 54 requests for assistance from foreign FIUs.

Bulgaria participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The most recent mutual evaluation of Bulgaria was conducted by MONEVAL in 2007. The mutual evaluation report (MER) is still in draft format.

The FIA is a member of the Egmont Group and also participates in information sharing with foreign counterparts. As of January 1, 2008, some of the FIA's rights within the Egmont Group were temporarily suspended pending a review of its authorities under the new legislation for the State Agency for National Security. Bulgaria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. The GOB is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

In 2005, the Bulgarian Parliament passed amendments to the 1969 law on Administrative Violations and Penalties, which establishes the liability of legal persons (companies) for crimes committed by their employees. This measure is in accordance with international standards and allows the government to implement its obligations under international agreements, including: the OECD Anti-Bribery Convention, the Civil Law Convention on Corruption, the Criminal Law Convention on Corruption, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Under the amendments, Bulgaria also aligns itself with the provisions of the EU Convention on the Protection of the Financial Interests of the European Communities and its Protocols.

Until December 2007 Bulgaria's legislative framework was largely viewed as consistent with international anti-money laundering standards. The new legislation on the State Agency for National Security brings uncertainty as to the authority of the financial intelligence unit, potentially jeopardizing its independence and investigatory mandate. It also raises questions about the FIA's ability to cooperate on equal basis with its international partners. The Government of Bulgaria should address these issues. The GOB should also take steps to improve and tighten its regulatory and reporting regime, particularly with regard to nonbank sectors and cash payments. The GOB should improve the consistency of its customs reporting enforcement and should also establish procedures to identify the origin of funds used to acquire banks and businesses during privatization. Inter-agency cooperation should be streamlined to ensure effective implementation of Bulgaria's anti-money laundering and counter-terrorist financing regime, and to improve prosecutorial effectiveness in money laundering and terrorist financing cases. The GOB should close duty free shops, or establish procedures for identifying unlawful activities associated with duty free shops, thereby tackling organized crime involved in smuggling and other financial crimes. The GOB should also disseminate the UNSCR 1267 Sanctions Committee's Consolidated List of designated terrorist entities to all financial institutions.

Burma

Burma, a major drug-producing country, has taken steps to strengthen its anti-money laundering regulatory regime in 2007. The country's economy remains dominated by state-owned entities, including the military. Agriculture and extractive industries, including natural gas, mining, logging and fishing provide the major portion of national income, with heavy industry and manufacturing playing minor roles. The steps Burma has taken over the past several years have reduced vulnerability to drug money laundering in the banking sector. However, with an underdeveloped financial sector and large volume of informal trade, Burma remains a country where there is significant risk of drug money being funneled into commercial enterprises and infrastructure investment. Traffic in narcotics, people, wildlife, gems, timber, and other contraband flow through Burma. Regionally, value transfer via trade is of concern and hawala/hundi networks frequently use trade goods to provide counter-

valuation. Burma's border regions are difficult to control and poorly patrolled. In some remote regions active in smuggling, there are continuing ethnic tensions with armed rebel groups that hamper government control. Collusion between traffickers and Burma's ruling military junta, the State Peace and Development Council (SPDC), allows organized crime groups to function with virtual impunity. Although progress was made in 2007, the criminal underground faces little risk of enforcement and prosecution. Corruption in business and government is a major problem. Burma is ranked 179 out of 179 countries in Transparency International's 2007 Corruption Perception Index.

The Government of Burma (GOB) has addressed some key areas of concern identified by the international community by implementing some anti-money laundering measures. In October 2006, the Financial Action Task Force (FATF) removed Burma from the FATF list of Non-Cooperative Countries and Territories (NCCT). To ensure continued effective implementation of reforms in Burma, the FATF, in consultation with the relevant FATF-style regional body (FSRB), will continue to monitor developments there for a period of time after de-listing. Burma is scheduled to undergo a mutual evaluation by the FSRB Asia-Pacific Group on Money Laundering in January 2008.

The United States maintains other sanctions on trade, investment and financial transactions with Burma under Executive Order 13047 (May 1997), Executive Order 13310 (July 2003), the Narcotics Control Trade Act, the Foreign Assistance Act, the International Financial Institutions Act, the Export-Import Bank Act, the Export Administration Act, the Customs and Trade Act, the Tariff Act (19 USC 1307), and the 2003 Burmese Freedom and Democracy Act (P.L. 108-61). In September and October 2007, under Executive Order 13310, the United States imposed additional sanctions on leaders of the Burmese regime, as well as key businessmen. In October 2007, Executive Order 13448 was issued. It expands the Treasury Department's existing authority to designate individuals for sanctions to include individuals responsible for human rights abuses and public corruption and individuals and entities who provide material or financial support to designated individuals or to the Government of Burma.

Burma enacted a "Control of Money Laundering Law" in 2002. It also established the Central Control Board of Money Laundering in 2002 and a financial intelligence unit (FIU) in 2003. The law created reporting requirements to detect suspicious transactions. It set a threshold amount for reporting cash transactions by banks and real estate firms, albeit at a high level of 100 million kyat (approximately U.S. $75,000). As of May 2007, over 40,000 cash transaction reports were filed. The GOB's 2004 anti-money laundering measures amended regulations instituted in 2002-2003 that set out 11 predicate offenses, including narcotics activities, human trafficking, arms trafficking, cyber-crime, and "offenses committed by acts of terrorism," among others. In 2004 the GOB added fraud to the list of predicate offenses, established legal penalties for leaking information about suspicious transaction reports, and adopted a "Mutual Assistance in Criminal Matters Law." The 2003 regulations, further expanded in 2006, require banks, customs officials and the legal and real estate sectors to file suspicious transaction reports (STRs) and impose severe penalties for noncompliance.

The GOB established a Department against Transnational Crime in 2004. Its mandate includes anti-money laundering activities. It is staffed by police officers and support personnel from banks, customs, budget, and other relevant government departments. In response to a February 2005 FATF request, the GOB submitted an anti-money laundering implementation plan and produced regular progress reports in 2006 and 2007. In 2005, the government also increased the size of the FIU to 11 permanent members, plus 20 support staff. In August 2005, the Central Bank of Myanmar issued guidelines for on-site bank inspections and required reports that review banks' compliance with AML legislation. Since then, the Central Bank has sent teams to instruct bank staff on the new guidelines and to inspect banking operations for compliance.

In 2007, the Burmese Government amended its "Control of Money Laundering Law" to expand the list of predicate offences to all serious crimes to comport with FATF's recommendations. In July 2007, the Central Control Board issued five directives to bring more nonbank financial institutions,

including dealers in precious metals and stones, under the AML/CTF compliance regime. As of August 2007, 823 STRs had been received. One case related to trafficking in persons was filed for prosecution, resulting in the convictions of one individual under the "Control of Money Laundering Law" and the Trafficking in Persons Law. In the first eight months of 2007, seven cases have been identified as potential money laundering investigations.

The United States maintains the separate countermeasures it adopted against Burma in 2004, and identified the jurisdiction of Burma and two private Burmese banks, Myanmar Mayflower Bank and Asia Wealth Bank, to be "of primary money laundering concern" pursuant to Section 311 of the 2001 USA PATRIOT Act. These countermeasures prohibited U.S. banks from establishing or maintaining correspondent or payable-through accounts in the United States for or on behalf of Myanmar Mayflower and Asia Wealth Bank and, with narrow exceptions, for all other Burmese banks. Myanmar Mayflower and Asia Wealth Bank had been linked directly to narcotics trafficking organizations in Southeast Asia. In March 2005, following GOB investigations, the Central Bank of Myanmar revoked the operating licenses of Myanmar Mayflower Bank and Asia Wealth Bank, citing infractions of the Financial Institutions of Myanmar Law. The two banks no longer exist. In August 2005, the Government of Burma also revoked the license of Myanmar Universal Bank (MUB), and convicted the bank's chairman under both the Narcotics and Psychotropic Substances Law, and the Control of Money Laundering Law. Under the money laundering charge, the court sentenced him to one 10-year and one unlimited term in prison and seized his and his bank's assets.

Burma also remains under a separate 2002 U.S. Treasury Department advisory stating that U.S. financial institutions should give enhanced scrutiny to all financial transactions related to Burma. The Section 311 rules complement the 2003 Burmese Freedom and Democracy Act (renewed in July 2006) and Executive Order 13310 (July 2003), which impose additional economic sanctions on Burma following the regime's May 2003 attack on a peaceful convoy of the country's pro-democracy opposition led by Nobel laureate Aung San Suu Kyi. The sanctions prohibit the import of most Burmese-produced goods into the United States, ban the provision of financial services to Burma by any U.S. persons, freeze assets of the ruling junta and other Burmese institutions, and expand U.S. visa restrictions to include managers of state-owned enterprises as well as senior government officials and family members associated with the regime. In September 2007, the U.S. Treasury amended and reissued the Burmese Sanctions Regulations in their entirety to implement the 2003 Executive Order that placed these sanctions on Burma.

Burma became a member of the Asia/Pacific Group on Money Laundering in March 2006. The GOB is a party to the 1988 UN Drug Convention. Over the past several years, Burma has expanded its counter narcotics cooperation with other states. The GOB has bilateral drug control agreements with India, Bangladesh, Vietnam, Russia, Laos, the Philippines, China, and Thailand. These agreements include cooperation on drug-related money laundering issues. In July 2005, the Myanmar Central Control Board signed an MOU with Thailand's Anti-Money Laundering Office governing the exchange of information and financial intelligence. The government signed a cooperative MOU with Indonesia's FIU in November 2006.

Burma is a party to the UN Convention against Transnational Organized Crime and ratified the UN International Convention for the Suppression of the Financing of Terrorism in August 2006. Burma signed the UN Convention on Corruption in December 2005, but has yet to deposit an instrument of ratification with the UN Secretary General. Likewise, Burma signed the Treaty on Mutual Legal Assistance in Criminal Matters among Like-Minded ASEAN Member Countries in January 2006, but has yet to deposit its instrument of ratification with the Attorney General of Malaysia.

The Government of Burma has in place a framework to allow mutual legal assistance and cooperation with overseas jurisdictions in the investigation and prosecution of serious crimes. To fully implement a strong anti-money laundering/counter-terrorist financing regime, Burma must provide the necessary

resources to administrative and judicial authorities who supervise the financial sector so they can apply and enforce the government's regulations to fight money laundering successfully. Burma must also continue to improve its enforcement of the new regulations and oversight of its banking system, and end all government policies that facilitate the investment of drug money and proceeds from other crimes into the legitimate economy. The reporting threshold for cash transactions should be lowered to a realistic threshold that fits the Burmese context. Customs should be strengthened and authorities should monitor more carefully the misuse of trade and its role in informal remittance or hawala/hundi networks. The GOB should ratify the UN Convention against Corruption, as well as the Treaty On Mutual Legal Assistance In Criminal Matters Among Like-Minded ASEAN Member Countries. The GOB should take serious steps to combat smuggling of contraband and its link to the pervasive corruption that permeates all levels of business and government. The GOB should criminalize the financing of terrorism.

Cambodia

Cambodia is neither an important regional financial center nor an offshore financial center. While there are only four reported money laundering cases in Cambodia, it serves as a transit route for heroin from Burma and Laos to international drug markets such as Vietnam, mainland China, Taiwan, and Australia. The major crimes reported by the Cambodian authorities are human trafficking and exploitation (which is widespread), drug trafficking, kidnapping for ransom and corruption. Its weak but improving anti-money laundering regime, a cash-based economy with an active informal banking system, porous borders with attendant smuggling and widespread corruption of officials also contributes to the significant money laundering risk in Cambodia. The vulnerability of Cambodia's financial sector is further exacerbated because of the intersection of the casino and banking interests with four companies having whole or partial shares in both banks and casinos. In addition, terrorist financing is a significant risk in Cambodia as highlighted by two recent cases involving Jemaah Islamiyah (JI) and the Cambodian Freedom Fighters (CFF).

In June 2007, The Royal Government of Cambodia promulgated a new "Law on Anti-Money Laundering and Combating the Financing of Terrorism" (AML). This law creates the framework for a National Bank of Cambodia financial investigations unit (FIU) to have far-reaching regulation over all banks and a long list of nonbank financial institutions such as casinos and realtors and can include entities to be designated by the FIU. In July 2007, a new Counterterrorism Law criminalized the financing and provision of material support to terrorism.

The National Bank of Cambodia (NBC) is making strides to regulate large or suspicious financial transactions, but is still in the process of working with relevant ministries to draft a prakas (decree) and related sub-decrees to fully implement the new anti-money laundering law. The prakas is expected to be issued in the first half of 2008. The Ministry of Interior has legal responsibility for oversight of the casinos and providing security; however, it exerts little supervision.

Cambodia's banking sector is small but expanding, with fifteen commercial banks, five specialized banks, and numerous microfinance institutions. Bank operations are primarily undertaken in U.S. dollars and on a cash basis. However, overall lending and banking activity remains limited as most Cambodians keep their assets outside the banking system. Economists note that while a typical country would have a bank deposit to GDP ratio of roughly 60 percent, Cambodia's ratio is only 29.2 percent (September 2007), low even by developing economy standards. Cambodia's banking system is highly consolidated, with two banks—Canadia Bank and ANZ Royal—accounting for more than 30 percent of all bank deposits. Besides banks, individual and legal persons can undertake foreign exchange provided they register with the NBC. There were 647 registered money changers in December 2006—53 in Phnom Penh and 594 in provinces.

The NBC has regulatory responsibility for the banking sector. The NBC regularly audits individual banks to ensure compliance with laws and regulations. The new AML law requires that banks and other financial institutions declare transactions over 40,000,000 riel (approximately U.S. $10,000). The NBC reports that its audits reveal that this requirement is generally followed. While there are no reports to indicate that banking institutions themselves are knowingly engaged in money laundering, until the FIU is fully established, government audits would likely not be a sufficient deterrent to money laundering through most Cambodian banks. With increased political stability and the gradual return of normalcy in Cambodia after decades of war and instability, bank deposits have risen by about 15 percent per year since 2000 and the financial sector shows some signs of deepening as domestic business activity continues to increase in the handful of urban areas. Foreign direct investment, while limited, is increasing after several years of contraction.

Cambodia lacks meaningful statistics on the extent of financial crime which exists and only a few crime statistics and open source information is available to evaluate the major sources of illicit funds in Cambodia. As the FIU is still being established, some larger scale money laundering in Cambodia may also flow through informal banking activities or business activities. The Cambodian authorities consider that there are informal money or value transfer operations carried out by money changers, or individuals within Cambodia or cross border. There is a significant black market in Cambodia for smuggled goods, including drugs, including the importing and local production of the methamphetamine ATS. Most of the smuggling that takes place is intended to circumvent official duties and taxes and involves items such as fuel, alcohol and cigarettes. Some government officials and their private sector associates have a significant amount of control over the smuggling trade and its proceeds. Cambodia has a cash-based and dollar-based economy, and the smuggling trade is usually conducted in dollars. Such proceeds are rarely transferred through the banking system or other financial institutions. Instead, they are readily converted into land, housing, luxury goods or other forms of property. It is also relatively easy to hand-carry cash into and out of Cambodia.

The NBC's Financial Investigations Unit (FIU) has the authority to apply anti-money laundering controls to nonbank financial institutions such as casinos and other intermediaries, such as lawyers or accountants. The FIU is under the control of the NBC with a permanent secretariat working under the authority of a board composed of one senior representative each from the Council of Ministers and the Ministries of Economy and Finance, Justice, and Interior.

The major nonbank financial institutions in Cambodia are the casinos, which the authorities have noted are particularly vulnerable to money laundering. Foreigners are allowed to gamble but Cambodians nationals are prohibited from entering casinos. The regulation of casinos falls under the jurisdiction of the Ministry of Interior, although the Ministry of Economy and Finance issues casino licenses and the NBC Financial Investigations Unit will have the newly legislated power to receive reports on financial transactions at casinos and cooperate with casino regulators on AML, including suspicious transactions. There are currently more than 20 licensed casinos in Cambodia, with a few more either under construction or applying for a license. Most are located along Cambodia's borders with Thailand or Vietnam. There is one large casino in Phnom Penh that has avoided the regulation that all casinos be at least 200 kilometers from the capital city. Casino patrons placing small bets simply hand-carry their money across borders, while others use either bank transfers or junket operators. Cambodian casinos have accounts with major Thai or Vietnamese banks and patrons can wire large amounts of money to one of these foreign accounts. After a quick phone call to verify the transfer, the Cambodian casino issues the appropriate amount in chips. Casinos also work with junket operators who, despite their name, only facilitate money transfers and do not serve as travel or tour operators. Players deposit money with a junket operator in Vietnam or Thailand, the casino verifies the deposit and issues chips to the player-typically up to double the amount of the deposit. After the gambling session ends, the junket operator then has 15 days to pay the casino for any losses. Because

the junket operator is responsible for collecting from the patrons, casinos see little need to investigate the patron's ability to cover his/her potential debt or the source of his/her wealth.

Although there is a legal requirement to declare to Cambodian Customs the entry of more than U.S. $10,000 into the country, in practice there is no effective oversight of cash movement into or out of Cambodia. Article 13(1) of the Law of Foreign Exchange requires the import of export of any means of payment equal to or exceeding U.S. $10,000 or equivalent to be reported to the Customs authorities at the border crossing point and Customs should transmit this information on a monthly basis to the National Bank of Cambodia. Outbound travelers are in practice not required to fill in a declaration form concerning the amount of currency or negotiable instruments they are carrying. There is no explicit power to stop or restrain transported funds and negotiable instruments to ascertain whether evidence of money laundering or terrorist financing exists. No specific provisions exist to sanction persons involved in cross border cash smuggling for money laundering or terrorist financing purposes or seize the cash or instruments involved.

In 1996, Cambodia criminalized money laundering related to narcotics trafficking through the Law on Drug Control. In 1999, the government also passed the Law on Banking and Financial Institutions. Together with the recently passed AML law, these two laws provide an additional legal basis for the NBC to regulate the financial sector. The NBC also uses the authority of these laws to issue and enforce new regulations. The NBC expects to issue a prakas (decree) on the AML in the first half of 2008. One current regulation, dated October 21, 2002, is specifically aimed at money laundering. The decree established standardized procedures for the identification of money laundering at banking and financial institutions. In October 2003, the NBC issued a circular to assist banks in identifying suspicious transactions and in fulfilling "Know Your Customer" best practices, though no suspicious transactions have yet been reported to the NBC. In addition to the NBC, the Ministries of Economy and Finance, Interior, Foreign Affairs, and Justice also are involved in anti-money laundering matters.

In 2005, Cambodia became a party to the 1988 UN Drug Convention, the UN Convention Against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. The new Counterterrorism Law criminalizes terrorist financing; and regulation of transactions suspected of financing terrorism are covered by the new AML. Under the new counter terrorism law the Minister of Justice may order the prosecutor to freeze property of a person if he is listed on the list of persons and entities belonging or associated with the Taliban and Al Qaida issued by the UNSCR 1267 committee or if he is a person who has committed a offence as defined in the law or a corresponding offence under the law of another state. The NBC circulates to financial institutions the list of individuals and entities included on the UNSCR 1267 Sanction Committee's consolidated list, and reviews the banks for compliance in maintaining this list and reporting any related activity. To date, there has not been an opportunity to monitor compliance of these new provisions. However, there have been no reports of designated terrorist financiers using the Cambodian banking sector. Should sanctioned individuals or entities be discovered using a financial institution in Cambodia, the NBC has the legal authority to freeze the assets until prosecution commences and a competent court has adjudicated the case. Penal sanctions for convictions of money laundering or financing terrorism include seizure of the assets to become state property.

In June 2004, Cambodia joined the Asia/Pacific Group on Money Laundering (APG), a Financial Action Task Force (FATF) style regional body. In May 2007, Cambodia underwent a comprehensive AML/CTF assessment that was conducted by the World Bank and APG. This assessment report was adopted by the APG in July 2007 and noted the progress, and remaining deficiencies the GOC's AML/CTF regime. This report marks the first time there has been detailed external scrutiny of AML/CTF in Cambodia and publication of the findings. However, questions regarding the government's ability to implement and enforce the new measures on money laundering remain, and approval of an implementing decree and related sub-decrees are important next steps. The GOC should also take the necessary steps to enhance its nascent FIU and should gain control over its porous

borders as well as increasing the capability of its law enforcement and judicial sectors to investigate, prosecute and adjudicate financial crimes. To achieve these ends, the GOC should continue its engagement with the Asia/Pacific Group on projects supported by the United States, Australia, the World Bank and the UN Office on Drugs and Crime (UNODC) to develop a comprehensive viable anti-money laundering/counter-terrorist financing regime that comports with international standards.

Canada

Money laundering in Canada is primarily associated with drug trafficking and financial crimes, particularly those related to fraud. The International Monetary Fund indicates that approximately U.S. $22-50 billion is laundered annually in Canada. Organized criminal groups involved in drug trafficking remain a concern of the Government of Canada (GOC). According to the Criminal Intelligence Service Canada's 2007 Annual Report on Organized Crime, there are approximately 950 organized crime groups operating in Canada, with approximately 80 percent of all crime groups in Canada involved in the illicit drug trade. With U.S. $1.5 billion in trade crossing the border each day, both the United States and Canadian governments are concerned about the criminal cross-border movements of currency, particularly the illicit proceeds of drug trafficking.

The GOC enacted the Proceeds of Crime (Money Laundering) Act in 2000 to assist in the detection and deterrence of money laundering, facilitate the investigation and prosecution of money laundering, and create the financial intelligence unit (FIU), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). The Proceeds of Crime (Money Laundering) Act was amended in December 2001 to become the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The list of predicate money laundering offenses was expanded to cover all indictable offenses, including terrorism and the trafficking of persons. In addition to amending the PCMLTFA, the 2001 reforms made it a crime under the Canadian Criminal Code to knowingly collect or give funds to carry out terrorism; denied or removed charitable status from those supporting terrorism; and facilitated freezing and seizing their assets.

The PCMLTFA created a mandatory reporting system for suspected terrorist property, suspicious financial transactions, large cash transactions, large international electronic funds transfers, and cross-border movements of currency and monetary instruments totaling $10,000 or more. Failure to report cross-border movements of currency and monetary instruments could result in seizure of funds or penalties ranging from approximately U.S. $250 to $5,000. Failure to file a suspicious transaction report (STR) could result in up to five years' imprisonment, a fine of approximately U.S. $2 million, or both. The law protects those filing suspicious transaction reports from civil and criminal prosecution. There has been no apparent decline in deposits made with Canadian financial institutions as a result of Canada's revised laws and regulations.

In December 2006, Parliament passed Bill C-25 to amend the PCMLTFA. The new legislation expands the coverage of Canada's anti-money laundering and counter-terrorist financing regime by bringing additional business sectors, including lawyers and dealers in precious metals and stones, under the authority of the PCMLTFA and related regulations. Bill C-25 also enhances client identification and record-keeping requirements. In addition, Bill C-25 mandates that FINTRAC create a national registry for money service businesses, and establish a system of administrative monetary penalties for noncompliance. The proposed measures will improve compliance with the reporting, record keeping, and client identification provisions of the PCMLTFA. The Bill permits FINTRAC to include additional information in the intelligence product that FINTRAC can disclose to law enforcement and national security agencies, as recommended in a 2004 Canadian Auditor General's Report.

FINTRAC, established in 2006, is an independent agency with regulatory and FIU functions. The majority of FINTRAC's 300-member staff works as analysts, compliance officers, and information

technology specialists. FINTRAC is the sole authority with the mandate to ensure compliance with the PCMLTFA and associated regulations. Guidelines explaining the PCMLTFA and its requirements were published by FINTRAC in 2002; further additions were made in 2003 and in July 2007. The guidelines provide an overview of FINTRAC's mandate and responsibilities, and include background information about money laundering and terrorist financing, including their international scope and nature. The guidelines also provide an outline of the Canadian legislative requirements for a compliance regime, record-keeping, client identification, and reporting transactions. FINTRAC also works closely with Canada's Office of the Superintendent of Financial Institutions (OSFI) concerning the policies and procedures that reporting entities have in place for complying with the PCMLFTA.

FINTRAC's compliance program is risk-based and emphasizes awareness training, compliance examinations, disclosures to law enforcement of reporting entities' noncompliance, and minimizing the regulatory burden for obligated entities. During 2006 and 2007, over 14,000 individuals representing all reporting sectors participated in a variety of FINTRAC's awareness initiatives. FINTRAC has Memoranda of Understanding (MOUs) with Canadian national regulators, including OSFI and the Investment Dealers Association of Canada (IDA), as well as provincial regulators. These MOUs permit FINTRAC and the regulators to exchange compliance information. FINTRAC, together with national and provincial regulators, conducted a record number of compliance examinations across all reporting sectors in 2006 and 2007.

As Canada's FIU, FINTRAC receives and analyzes reports from financial institutions and other financial intermediaries (such as money service businesses, casinos, accountants, and real estate agents) as mandated by the PCMLTFA, and makes disclosures to law enforcement and intelligence agencies. FINTRAC may only disclose information related to money laundering or terrorist financing offences. FINTRAC has access to other law enforcement and national security agencies databases through an MOU and, on a case-by-case basis, with other relevant agencies. FINTRAC received approximately 15 million reports from reporting entities in 2006 and 2007, which includes approximately 29,000 suspicious transaction reports (STRs), 6 million cash transaction reports, 50,000 cross-border reports, and 9 million electronic funds transfer reports (which includes funds that enter and exit the country). FINTRAC produced a total of 193 case disclosures in 2006 and 2007, totaling approximately $10 billion. Of the 193 case disclosures, 152 were suspected money laundering, 33 were suspected terrorist activity, and 8 involved suspected money laundering, terrorist financing, and/or threats to the security of Canada. FINTRAC has the ability to exchange information with foreign FIUs through an MOU, and has signed over 45 MOUs with its counterparts. In 2006 and 2007, FINTRAC made 35 disclosures to 14 counterpart FIUs.

In a 2004 report to Parliament, Canada's Auditor General stated that "privacy concerns restrict FINTRAC's ability to disclose intelligence to the Police, and as a result, law enforcement and security agencies usually find that the information they receive is too limited to justify launching investigations." United States law enforcement officials have echoed concerns that Canadian privacy laws and the high standard of proof required by Canadian courts inhibit the full sharing of timely and meaningful intelligence on suspicious financial transactions. Such intelligence may be critical to investigating and prosecuting international terrorist financing or major money laundering investigations. Recently, concern has focused on the inability of United States and Canadian law enforcement officers to exchange information promptly concerning suspicious sums of money found in the possession of individuals attempting to cross the United States-Canadian border. A 2005 MOU on exchange of cross-border currency declarations expanded the extremely narrow disclosure policy. However, the scope of the exchange remains restrictive.

The PCMLTFA enables Canadian authorities to identify, deter, disable, prosecute, convict, and punish terrorist groups. The PCMLTFA expands FINTRAC's mandate to include counter-terrorist financing and allow disclosure to the Canadian Security Intelligence Service of information related to financial transactions relevant to threats to the security of Canada. The GOC has also listed and searched

financial records for suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list. There are currently more than 500 individuals and entities associated with terrorist activities designated by the GOC. This designation effectively freezes their assets and prohibits fund-raising on their behalf in Canada.

In addition to new legislation, the GOC is undertaking other initiatives to bolster its ability to combat money laundering and terrorist financing. Canada's Department of Finance has created a public/private sector advisory committee to discus matters of mutual interest in the ongoing fight against money laundering and counter-terrorist financing. In May 2006, the GOC announced that it had added in the 2006 budget approximately U.S. $58 million over the next two years for FINTRAC, the Royal Canadian Mounted Police (RCMP), and the Department of Justice. The new funding will increase the number of RCMP officers working in the counter-terrorist financing and anti-money laundering units; increase the capabilities of the Canada Border Services Agency (CBSA) to detect unreported currency at airports and border crossings; enable Canada's Department of Justice to handle the expanding litigation workload that will result from increasing the enforcement resources of other GOC agencies; and ensure that FINTRAC can better analyze transactions reports and monitor compliance of unregulated financial sectors, such as money remitters.

Canada has longstanding agreements with the United States on law enforcement cooperation, including treaties on extradition and mutual legal assistance, as well as an asset sharing agreement. Canada has provisions for sharing seized assets, and exercises them regularly. The CBSA and the United States Department of Homeland Security Immigration and Customs Enforcement (ICE) are in the process of negotiating an MOU to share information on currency seizures.

Canada is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. The GOC has also ratified the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, the Inter-American Convention against Terrorism, and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. On October 2, 2007, the GOC ratified the UN Convention against Corruption.

Canada is a member of the Financial Action Task Force (FATF) and underwent a mutual evaluation in early 2007. The results are expected to be released publicly via the FATF's website in 2008. Canada is a member of the Asia/Pacific Group on Money Laundering (APG), and also supports the Caribbean Financial Action Task Force (CFATF). Canada also belongs to the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. FINTRAC became a member of the Egmont Group in 2002. In June 2006, Toronto was selected as the permanent location of the Secretariat of the Egmont Group. The GOC will contribute approximately $5 million over a five-year period to help establish the Secretariat.

Canada has demonstrated a strong commitment to combat money laundering and terrorist financing both domestically and internationally. In 2007, the GOC made strides in enhancing its anti-money laundering and counter-terrorist financing regime, and reducing its vulnerability to money laundering and terrorist financing. The GOC should continue to implement these efforts, particularly a system for administrative monetary penalties in 2008. The GOC should also ensure that its privacy laws do not excessively prohibit provision of information to domestic and foreign law enforcement that might lead to prosecutions and convictions. Such prohibitions also should not prohibit the exchange of information between FINTRAC and its counterpart FIUs, or information sharing on the cross-border movement of currency.

Cayman Islands

The Cayman Islands, a United Kingdom (UK) Caribbean overseas territory, continues to make strides in strengthening its anti-money laundering and counter-terrorist financing regime. However, the islands remain vulnerable to money laundering due to their significant offshore sector. Most money laundering that occurs in the Cayman Islands is primarily related to fraud (particularly securities fraud), drug trafficking, and tax evasion.

The Cayman Islands is home to a well-developed offshore financial center that provides a wide range of services, including banking, structured finance, investment funds, various types of trusts, and company formation and management. There are approximately 450 banks and trust companies, 8,600 funds, 740 captive insurance companies, and 62,572 exempt companies licensed or registered in the Cayman Islands. Shell banks are prohibited, as are anonymous accounts. Bearer shares can only be issued by exempt companies and must be immobilized. Gambling is illegal; and the Cayman Islands does not permit the registration of offshore gaming entities.

The Misuse of Drugs Law and the Proceeds of Criminal Conduct Law (PCCL) criminalize money laundering related to narcotics trafficking and all other serious crimes. A revision and consolidation of these laws has been proposed for enactment before the end of 2007. The PCCL provides for the offense of money laundering where a person or business has engaged in criminal conduct or has benefited from criminal conduct; tax offenses are not included. The PCCL was amended in May 2007 to incorporate terrorist financing offenses into the definition of money laundering.

The Cayman Islands Monetary Authority (CIMA) is responsible for the licensing, regulation and supervision of the Cayman Islands' financial industry, as well as monitoring the industry for compliance with its anti-money laundering and counter-terrorist financing (AML/CTF) obligations. The financial industry includes banks, trust companies, investment funds, fund administrators, insurance companies, insurance managers, money service businesses, and corporate service providers. These institutions, as well as most designated nonfinancial businesses and professions, are subject to the AML/CTF regulations set forth in the Guidance Notes on the Prevention and Detection of Money Laundering in the Cayman Islands (Guidance Notes). The Guidance Notes are issued by the CIMA and were last amended in May 2007. With the enactment of the Money Laundering (Amendment) (No 2) Regulation 2007 on August 7, 2007, dealers in precious metals and precious stones are now included in the definition of relevant financial businesses, but have been given a transitional grace period until January 1, 2008, for compliance. The real estate industry is also subject to AML/CTF regulations, but the CIMA does not have responsibility for supervising this sector.

The CIMA conducts on-site and off-site examinations of licensees. These examinations include monitoring for compliance with the PCCL and the CIMA's Guidance Notes. The Guidance Notes require employee training, record keeping, and "know your customer" (KYC) identification requirements for financial institutions and certain financial services providers. The regulations require due diligence measures for individuals who establish a new business relationship, engage in one-time transactions over 15,000 Cayman Islands dollars (approximately $18,000), or who may be engaging in money laundering. The application of the AML/CTF measures to the financial sector and designated nonfinancial businesses is not based on risk assessment, although the CIMA does employ a risk-based approach to its on-site inspections.

The PCCL requires mandatory reporting of suspicious transactions, and makes failure to report a suspicious transaction a criminal offense that could result in fines or imprisonment. A suspicious activity report (SAR) must be reported once it is known or suspected that a transaction may be related to money laundering or terrorist financing. There is no threshold amount for the reporting of suspicious activity. It is currently not an offense to tip off the subject of a SAR; however, this should be corrected with the upcoming consolidation of the PCCL with the Misuse of Drugs Law that is currently underway.

Established under PCCL (Amendment) Law 2003, the Financial Reporting Authority (FRA) replaces the former financial intelligence unit of the Cayman Islands. The FRA is responsible for, among other things, receiving, analyzing, and disseminating SARs, including those relating to the financing of terrorism. The FRA began operations in 2004 and has a staff of six: a director, a legal advisor, a senior accountant, a senior analyst, a junior analyst, and an administrative officer. The FRA is a separate civilian authority governed by the Anti-Money Laundering Steering Group (AMLSG), which is chaired by the Attorney General and includes as its members the Financial Secretary, the Managing Director of the Cayman Islands Monetary Authority, the Commissioner of Police, the Solicitor General, and the Collector of Customs. Obligated entities currently report suspicious activities to the FRA via fax, although the FRA plans to establish an electronic reporting system. Under the PCCL, the FRA has the authority to require all obligated entities to provide additional information related to a SAR.

The majority of SARs received by the FRA are submitted by banks, with 10 percent of the total SARs received submitted by lawyers. From July 1, 2006 to June 30, 2007 (the fiscal year of the FRA), the FRA received 219 SARs. As of August, the FRA had responded to nine requests for information from foreign FIUs in 2007, and sent an additional seven disclosures to foreign law enforcement or FIUs.

The Financial Crime Unit (FCU) of the Royal Cayman Islands Police (RCIP) is responsible for investigating money laundering and terrorist financing. The FCU works in conjunction with the Joint Intelligence Unit (JIU), which gathers and disseminates intelligence to domestic and international law enforcement agencies. The Legal Department of the Portfolio of Legal Affairs is responsible for prosecuting financial crimes. As of August, the FRA had sent two cases to the FCU for further investigation in 2007. There have been five money laundering convictions in the Cayman Islands since 2003.

On August 10, 2007, the Cayman Islands enacted the Customs (Money Declarations and Disclosures) Regulations, 2007. These regulations establish a mandatory declaration system for the inbound cross-border movement of cash and a disclosure system for money that is outbound. All persons transporting money totaling 15,000 Cayman Islands dollars (approximately $18,000) or more into the Cayman Islands are required to declare such amount in writing to a Customs officer at the time of entry. Persons carrying money out of Cayman Islands are required to make a declaration upon verbal or written inquiry by a Customs officer.

The Cayman Islands has a comprehensive system in place for the confiscation, freezing, and seizure of criminal assets. In addition to criminal forfeiture, civil forfeiture is allowed in limited circumstances. Under the Misuse of Drugs Law and the PCCL, the courts can order the restraint of property upon application by a prosecutor. The FRA can also request a court order to freeze bank accounts if it suspects the account is linked to money laundering or terrorist financing. However, while the police may obtain production orders for the purposes of investigation and confidential information, there are no specific asset-tracing provisions. These will be provided for in the proposed consolidation of the PCCL and the Misuse of Drugs Law. Over $120 million in assets has been frozen or confiscated since 2003.

The Cayman Islands is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001. However, the United Kingdom has yet to extend the application of the International Convention for the Suppression of the Financing of Terrorism to the Cayman Islands. The Cayman Islands criminalized terrorist financing through the passage of the Terrorism Bill 2003, which extends criminal liability to the use of money or property for the purposes of terrorism. It also contains a specific provision on money laundering related to terrorist financing. While lists promulgated by the UN Sanctions Committee and other competent authorities are legally recognized, there is no legislative basis for independent domestic listing and delisting. The confiscation, freezing, and seizure of assets related to terrorist financing are permitted by law. Nonprofit organizations must

be licensed and registered, although there is no competent authority responsible for their supervision. There have been no terrorist financing investigations or prosecutions to date in the Cayman Islands.

In 1986, the United States and the United Kingdom signed a Treaty concerning the Cayman Islands relating to Mutual Legal Assistance in Criminal Matters. By a 1994 exchange of notes, Article 16 of that treaty has been deemed to authorize asset sharing between the United States and the Cayman Islands. The Cayman Islands is a member of the Caribbean Financial Action Task Force (CFATF). In June 2007, CFATF conducted its third mutual evaluation of the Cayman Islands. The evaluation team found the Cayman Islands to be compliant or largely compliant with 38 of the 49 Financial Action Task Force recommendations. The FRA is a member of the Egmont Group. The FRA currently has nine MOUs with FIUs in Australia, Canada, Chile, Guatemala, Indonesia, Mauritius, Nigeria, Thailand, and the United States.

The Government of the Cayman Islands should continue its efforts to implement its anti-money laundering and counter-terrorist financing regime. It should enact the proposed provisions to consolidate the Misuse of Drugs Law and the Proceeds of Criminal Conduct Law to criminalize tipping off the subjects of suspicious activity reports and to allow for asset tracing provisions. The Caymans Islands should also ensure that new provisions related to AML/CTF requirements for dealers in precious metals and stones and the disclosure/declaration system for the cross-border movement of currency are fully implemented.

Chile

Chile's has a large and well-developed banking and financial sector. The government is actively seeking to turn Chile into a global financial center and has signed 55 Free Trade Agreements with countries around the world. With the increase in legitimate trade and currency flows and the growing economy may come an increase in illicit activity and money laundering. Stringent bank secrecy laws emphasizing privacy rights have been broadly interpreted and hamper Chilean efforts to identify and investigate money laundering and terrorist financing. Chile's incomplete and still-developing regulatory oversight is an additional vulnerability.

In 2007, the Government of Chile (GOC) prosecuted its first four money laundering cases under the new penal system. In the first case, the defendant was found guilty of drug trafficking, but not money laundering. However, the sentence he received included the seizure of all his assets, not solely those tied to narcotics trafficking; thus, while not convicted of money laundering, he received the penalty associated with a money laundering conviction. The second and third cases were resulted in conviction on charges of money laundering as a result of plea bargaining, marking the first two recorded money laundering convictions under the new penal system. The fourth case, however, resulted in a conviction of money laundering by the trial judges. The accused in this case laundered money from the proceeds of drug trafficking in Europe and was sentenced to six years in prison, with all of his assets confiscated.

Chile criminalized money laundering under Law 19.366 of 1995, Law 19.913 of 2003, and Law 20.119 of 2006. Under Law 19.913, predicate offenses for money laundering include narcotics trafficking, terrorism in any form and the financing of terrorist acts or groups, illegal arms trafficking, kidnapping, fraud, corruption, child prostitution and pornography, and some instances of adult prostitution. Chile has yet to widen the scope of money laundering to apply it to other types of crimes such as trafficking in persons, intellectual property rights violations, and extortion. Detection methods, particularly when not tied to drug trafficking, are still weak. Thus, while most money laundering thus far discovered is tied to drug dealing, it is difficult to determine whether the majority of money laundering in Chile truly is tied to this crime.

Law 19.913 created Chile's financial intelligence unit, the Unidad de Análisis Financiero (UAF), as an autonomous agency affiliated with the Ministry of Finance. The UAF currently has a staff of 21, and has received approval in the budget for 2008 to expand to 31 employees. Law 19.913 requires mandatory reporting of suspicious transactions to the UAF by banks and financial institutions, financial leasing companies, general and investment funds-managing companies, pension fund administration companies, the Foreign Investment Committee, money exchange firms and other entities authorized to receive foreign currencies, firms that carry out factoring operations, credit card issuers and operators, securities companies, money transfer and transportation companies, stock exchanges, stock exchange brokers, securities agents, insurance companies, mutual funds managing companies, forwards and options markets operators, tax-free zones' legal representatives, casinos, gambling houses and horse tracks, customs general agents, auction houses, realtors and companies engaged in the land development business, notaries and registrars. Law 20.119 now also subjects pension funds and sports clubs to reporting requirements. Dealers in jewels and precious metals, and intermediaries (such as lawyers and accountants) are not subject to reporting requirements.

In addition to filing suspicious transaction reports (STRs), Law 19.913 also requires that obligated entities maintain registries of cash transactions that exceed 450 unidades de fomento (UF) (approximately $17,000). All cash transaction reports (CTRs) contained in the internal registries must be sent to the UAF at least once a year, or more frequently at the request of the UAF. The UAF requires banks to submit CTRs every month, and money exchange houses and most other obliged institutions every three months. Some specific institutions without a high amount of cash transactions (e.g. notaries) may submit CTRs every 6 months. In all cases, institutions must report CTRs dating from May 2004, when the obligation to record cash transactions over 450 UF went into effect. As of September, the UAF had received 1,839 CTRs and 301 STRs in 2007.

The Chilean tax service (Servicio de Impuestos Internos) issued a regulation, Resolution 120, requiring all banks, exchange houses and money remitters to report all transactions exceeding $10,000 sent to or received from foreign countries. Twenty-four banks joined together to appeal this regulation, claiming compliance would violate bank secrecy and expose them to lawsuits. The court of appeals ruled in favor of the banks, which are no longer subject to Resolution 120. The physical transportation of cash exceeding $10,000 into or out of Chile must be reported to Customs, which then files a report with the UAF. These reports are sent to the UAF daily. However, Customs and other law enforcement agencies are not legally empowered to seize or otherwise stop the movement of funds, and the GOC does not impose a significant penalty for failing to declare the transportation of currency in excess of the threshold amount,.

Law 20.119 authorizes the UAF to impose sanctions on obligated entities for noncompliance with requirements to establish an anti-money laundering and counter-terrorist financing (AML/CTF) system or reporting suspicious/cash transactions. In 2007, the UAF identified several cases of failure to report suspicious activity or to establish an AML/CTF system. It sanctioned some nonbank financial institutions for the first time this year by either fining the institution, or by sending it a letter stating the institution was sanctioned. If the organization is not found to be compliant within a year, it can be subject to three times the maximum fine for being sanctioned twice in a year. The UAF may also access any government information (police, taxes, etc.) not covered by secrecy or privacy laws. The UAF does not have regulatory responsibilities, but can issue general instructions on reporting obligations, such as requiring reporting entities to report any transactions by persons suspected of terrorist financing.

The Superintendence of Banks and Financial Institutions (SBIF) supervises banks in Chile, and stock brokerages, securities firms, and insurance companies are under the supervision and regulation of the Superintendence of Capital Markets. Chile's anti-money laundering laws oblige banks to abide by "know-your-customer" standards and other money laundering controls for checking accounts. However, the same compliance standards do not apply to savings accounts. Only a limited number of

banks rigorously apply money laundering controls to noncurrent accounts. Banks and financial institutions must keep records with updated background information on their clients throughout the period of their commercial relationship, and maintain records for a minimum of five years on any case reported to the UAF. The UAF has expressed concern about the quality of STRs, but is the organization responsible for working with reporting entities to improve quality. Bank compliance officers complain that, while the UAF has criticized the quality of their reports, it has provided no training to teach them how to improve. The UAF and the Banking Association have asked representatives from Colombia's FIU to provide training to the banks in 2008. None of the money laundering cases that have gone to trial in Chile to date were referred by the UAF, nor did they contain evidence provided by banks, though money passed through banks in all of the cases.

Insufficient supervision and the lack of a definition of "suspicious activity" for nonbank and nonfinancial institutions continue to be identified as deficiencies in the GOC's AML/CTF regime. Each entity independently decides what constitutes irregularities in financial transactions. Nonbank financial institutions, such as money exchange houses and cash couriers, do not fall under the supervision of any regulatory body for compliance with AML/CTF standards. In Santiago alone there are more than 60 exchange houses (approximately 114 nationwide), many of which do not record or share with other exchange houses any information about their customers. The GOC is aware of the need for regulation of these entities. As of May 2007, nonbank financial institutions must obtain contact information and a declaration of origin statement from individuals carrying out transactions of more than $5,000. These institutions must also report transactions of up to $4,999 to the UAF if they are considered to be suspicious. Nevertheless, the lack of supervision, training in the definition of "suspicious activity," and a harmonized system to keep record of daily transactions diminishes useful reporting to the UAF and undermines the effectiveness of the system. This sector appears particularly vulnerable to abuse by money launderers.

Chile's gaming industry falls under the supervision of the Superintendence of Casinos (SCJ), which is in charge of drafting regulations about casino facilities, and the administration, operation and proper development of the industry. Online gambling is prohibited except for the Internet purchase of lottery tickets from one of Chile's two lotteries. Eight casinos are currently operating throughout the country. The SCJ has oversight powers and regulatory authority over the industry but no law enforcement authority. Under Law 19.995, the SCJ granted authorization for 15 casinos to operate in Chile after participating in an international and domestic bidding process to assign permits during 2005 and 2006. One new casino opened in 2007, and nine are expected to open in 2008. By 2009, a total of 22 casinos will be fully operational and under the oversight authority of the SCJ. The SCJ screened applications for the new casino licenses with the support of domestic and international police and financial institutions. However, Chilean law limits the SCJ to 270 days for the entire background check and determination of whether to issue a license.

Law 19.913 requires casinos to keep a record of all cash transactions over UF 450 (the equivalent of approximately $17,000), and to designate a compliance officer. However, in July 2007, the UAF instructed casinos to identify, know, and maintain records on all customers—Chileans and foreigners—who carry out any transaction over $3,000. The SCJ also requires the casinos to prepare and submit for approval manuals detailing their AML/CTF plan. The SCJ is working to establish additional regulations, internal control standards, and standardized forms to improve their ability to monitor the growing number of casinos. Chile's Finance Ministry, in cooperation with the SCJ, presented to Congress a draft law addressing some of the weaknesses of Chile's gaming law. The draft law, if it passes, will provide increased regulatory authority to the SJC and prohibit individuals without licenses from operating electronic gambling games.

When the UAF determines that an account or a case requires further investigation, it passes the information to the Public Ministry (the public prosecutor's office). The Public Ministry is responsible

for receiving and investigating all cases from the UAF and has up to two years to complete an investigation and begin prosecution. In 2007, the UAF referred seven cases to the Public Ministry.

The Public Ministry's unit for money laundering and economic crimes has been proactive in investigating crimes, and pursuing training opportunities to further educate its prosecutors and other players in the criminal justice process. The money laundering unit is also developing a manual for prosecutors trying drug cases. The manual provides practical steps to investigate assets so as to identify possible money laundering as well as drug trafficking. They have also established a computer link with the tax service, SBIF, and other relevant agencies to access information that is not protected by bank and tax secrecy laws.

The Chilean investigative police (PICH) and the uniformed national police (Carabineros) work in conjunction with the Public Ministry on money laundering investigations. They also cooperate with U.S. and regional law enforcement in money laundering investigations. In 2004, Customs agents at Santiago's airport alerted the newly formed UAF of cash couriers bringing large amounts of euros to Chile from Colombia. After analysis, the UAF referred the case to the CDE (the precursor to the Public Ministry), which formally opened an investigation. The PICH's anti-money laundering unit and DEA uncovered an international money laundering scheme in which employees of some cash exchange houses carried euros and U.S. dollars from Colombia to Chile. The money was then carried by Chilean employees on commercial flights to the United States where it was deposited in banks and returned to Colombia in pesos. Through Chilean/DEA cooperation, arrests were made in Chile and the U.S. simultaneously and the money laundering ring was broken.

The police are competent and well-trained, but many are new to investigating financial crimes. Many complain of insufficient access to information. Chilean law prohibits the UAF from giving information directly to law enforcement, and allows the sharing of information only with the Public Ministry and foreign FIUs. Currently police must request financial information from the Public Ministry, which in turn requests it from the UAF. The UAF responds with all available information; however, much financial and tax information is protected through Chile's strict secrecy laws.

Bank secrecy is the most often identified obstacle to money laundering investigations identified by the police and prosecutors. Article 154 of the General Banking Law states that deposits and obligations of any kind shall be subject to banking secrecy, and information about such transactions may only be provided to the depositor or creditor (or an authorized legal representative). Law 707 also states that banks may not share information about the movement and balances in a current account with a third party. To avoid possible lawsuits, banks do not share information with prosecutors unless the prosecutors produce a judicial order. Thus, bank compliance officers are restricted to simply reporting suspicious activity and then waiting for the appropriate court authorization to release any private information. Many banks respond quickly to requests for information from the UAF, but are slow to reply to judicial court orders to provide prosecutors with additional information. When they do reply, they often provide incomplete information. Police and prosecutors complain they lose valuable time waiting at least a month (but usually more) for banks to provide incomplete information. Judges can require the detention of the bank's general manager until all information is disclosed, but this tool is rarely used. In the instances when the judge has issued the order for the general manager's detention, bank information was provided immediately.

Under Law 20.119, the Public Ministry can, with the authorization of a judge, lift bank secrecy provisions to gain account information if the account is directly related to an ongoing case. Unless a suspicious transaction report has been filed on an account, prosecutors and the UAF must get permission from a judge to examine an account. The process is often subject to the determination of judges who have received little training in financial crimes. The judges must decide if the prosecutors have presented sufficient evidence to warrant lifting bank secrecy. However, this process often prohibits prosecutors and the UAF from accessing the information they would need to convince a

judge of suspicious activity. The UAF has made approximately 10 requests per year, petitioning a judge only when confident the request would be granted. All requests have been granted within 24 hours, but the system does not yet encourage aggressive examination of suspicious activity on the part of the UAF, and time is lost in the preparation of the case for the judge.

A draft law currently under discussion in a committee of Chile's House of Representatives would facilitate easier access to bank and tax records for the UAF and prosecutors in certain instances. If passed, this law would bring Chile more into greater compliance with the Financial Action Task Force (FATF) Recommendations, and UN resolutions on terrorist financing. The draft law has been sitting in the Congressional commission since it was introduced in May 2007. Without urgent status granted to it by the President, it appears unlikely to work its way through the legislative process quickly. The Organization for Economic Cooperation and Development (OECD), to which Chile hopes to accede, criticized Chile's bank secrecy laws in October 2007. Chile's Foreign Minister used the opportunity to encourage passage of the draft law.

Law 19.913 contains provisions that allow prosecutors to request that assets be frozen only when tied to drug trafficking. No provisions have been made for freezing assets under other circumstances, including assets of individuals or companies designated by UN Security Council Resolution 1267. The Ministry of National Property currently oversees forfeited assets, and proceeds from the sale of forfeited assets are passed directly to CONACE, the National Drug Control Commission, to fund drug abuse prevention and rehabilitation programs. Under the present law, forfeiture is possible for real property and financial assets. Chilean law does not permit the seizure of substitute assets or civil forfeiture. The same draft law that would facilitate lifting bank secrecy for the UAF and Public Ministry would allow for the freezing of assets in cases of suspected terrorist financing and would enable Chile to share seized assets with other governments. The draft law would also ensure assets seized in money laundering convictions would go, at least in part, to law enforcement rather than only to drug rehabilitation programs. A total of $2 million in assets were seized in money laundering investigations in 2007.

Two free trade zones exist in Chile, in Punta Arenas and Iquique. The Iquique free trade zone, the larger of the two, also has an extension in Arica, near Chile's border with Peru. The physical borders of the free trade zone are porous and largely uncontrolled. All companies in the free trade zone are reporting entities and must report any suspicious activity to the UAF. Due to weak detection methods, determining the extent of money laundering in the free trade zones is virtually impossible. Iquique appears to be the primary conduit for counterfeit goods into Chile, and one of the main conduits of counterfeit goods moving to the Tri-Border Area between Brazil, Paraguay, and Argentina. Chilean resources to combat this issue are extremely limited. Police investigative efforts suggest possible criminal links between Iquique and the Tri-Border Area involving both terrorist financing of Hizballah and Hamas and money laundering.

Law 18.314 and Law 19.906 criminalize terrorist financing in Chile. Law 19.906 modifies Law 18.314 to more efficiently sanction terrorist financing in conformity with the UN International Convention for the Suppression of the Financing of Terrorism. Under Law 19.906, financing a terrorist act and the provision (directly or indirectly) of funds to a terrorist organization are punishable by five to ten years in prison. The Superintendence of Banks circulates the UNSCR 1267 Sanctions Committee's consolidated list to banks and financial institutions. The UAF also posts the 1267 list on its website and has instructed all reporting entities to report any transactions by those on the list. The GOC has not identified any terrorist assets belonging to individuals or groups named on the list to date in Chile. Law enforcement lacks tools to investigate terrorist financing; undercover operations, for example, are not permitted for such investigations.

The GOC does not monitor transactions outside of Chile to prevent terrorist financing, nor does it regulate nongovernmental organizations (NGOs). Nonprofit organizations must register at the Justice

Ministry, but this Ministry has no regulatory responsibility over them. In response to the evaluation of Chile by the Financial Action Task Force of South America (GAFISUD), which was released in December 2006, the Finance Ministry initiated discussions with the Superintendence of Banks and the Superintendence of Capital Markets to identify the best way to monitor NGOs; these discussions have not yet reached conclusions.

Chile is party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the Inter-American Convention on Terrorism. Chile is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and GAFISUD. The UAF is a member of the Egmont Group of financial intelligence units and serves as one of the representatives for the Americas on the Egmont Committee. The UAF has signed memoranda of understanding (MOUs) for the exchange of financial information with the United States FIU and FIUs of 32 other jurisdictions.

The GOC is proactive in pursing partnerships with other countries. It signed an agreement with Colombia in 2007 to cooperate on terrorism and economic crimes. There is no regular, formal exchange of records with the United States, but case-specific cooperation and exchange of records is very strong. Negotiations with Chile on the FBI's South American Fingerprint Exploitation (SAFE) project, whereby Chile and U.S. would share fingerprint records of criminals, are ongoing. As part of Chile's strategy to access the OECD, Chile participates, as an observer or invitee, in 18 OECD Committees and Working Groups, including the Working Group on Bribery and Transnational Crimes.

The first money laundering conviction by judges under the new judicial system demonstrates a significant step in the Government of Chile's anti-money laundering regime. However, it remains to be seen if the system will be successful in convicting money launderers without ties to drug trafficking. Issues of limited access to information for the Public Ministry, the PICH, and the Carabineros and inter-agency conflict should be resolved. Reporting entities should be adequately supervised, receive sufficient training in determining suspicious activity, and monitored for compliance with reporting requirements. The GOC should ensure the passage of the draft law currently sitting in the lower house of Congress to allow for the lifting of bank secrecy and the freezing of assets. Passage of this law would bring Chile closer to compliance with its UNSCR 1267 obligations and FATF Recommendations. The GOC should also increase government oversight of nonfinancial institutions, allow for greater access to information for the UAF and other key agencies, and enhance inter-agency cooperation to improve Chile's ability to combat money laundering and terrorist financing.

China, People's Republic of

Over the past five years, the Government of the People's Republic of China has made significant progress in developing anti-money laundering and counter-terrorist financing measures including through legislative reform, strengthening enforcement mechanisms, and international cooperation efforts. However, money laundering remains a serious concern as China restructures its economy and develops its financial system. Narcotics trafficking, smuggling, trafficking in persons, counterfeiting of trade goods, fraud, tax evasion, and other financial crimes are major sources of laundered funds. Most money laundering cases currently under investigation involve funds obtained from corruption and bribery. Chinese officials have noted that most acts of corruption in China are closely related to economic activities and accompanied by illegal money transfers. Proceeds of tax evasion, recycled through offshore companies, often return to China disguised as foreign investment and, as such, receive tax benefits. Underground banking and trade-based money laundering are an increasing concern. According to the International Monetary Fund, money laundering in China may total as much

as U.S. $24 billion per year and officials with the People's Bank of China reported a total of 1,239 cases involving illicit money flows involving 362.6 billion Chinese yuan renminbi (RMB) (approximately U.S. $45.3 billion) in 2006.

The People's Bank of China (PBC), China's central bank, maintains primary authority for anti-money laundering and counter terrorist finance coordination. The PBC also shares some anti-money laundering responsibilities with other financial regulatory agencies, including: the China Banking Regulatory Commission (CBRC), which supervises and regulates banks, asset management companies, trust and investment companies, and other deposit-taking institutions; the China Insurance Regulatory Commission (CIRC), which supervises the insurance sector; and the China Securities Regulatory Commission (CSRC), which supervises the securities sector. The Ministry of Public Security's Anti-Money Laundering Division and Anti-Terrorism Bureau lead anti-money laundering and counter-terrorist finance-related law enforcement efforts.

Within the PBC's Financial Intelligence Unit (FIU), the Anti-Money Laundering Bureau (AMLB) handles the coordination of all anti-money laundering programs and carries out administrative and policy oversight, while the China Anti-Money Laundering Monitoring and Analysis Center (CAMLMAC) collects, analyzes, and disseminates suspicious transaction reports and currency transaction reports. According to CAMLMAC, which was established in 2004, 683 reports on suspicious transactions, involving RMB 137.8 billion (approximately U.S. $18.9 billion), were identified for further investigation by the end of 2005. From July 1, 2005 to June 30, 2006, CAMLMAC received 619,962 RMB suspicious transaction reports and 2,245,267 foreign currency suspicious transactions. The 2007 FATF mutual evaluation of China noted that consideration should be given to the problem of how to effectively manage and exploit such a large volume of STRs coming directly to CAMLMAC, which has a staff of only sixty people.

Since its inception, the FIU has transferred 57 files (involving about 80,000 separate suspicious transactions) to the Ministry of Public Security (MPS) for investigation. Nine referrals have resulted in cases being filed for investigation; and one has been referred for prosecution. Since October 2005, approximately ten suspicious transaction dossiers have been transferred to other agencies, including five to the Ministry of State Security (MSS). Four of these cases are still being investigated by the MSS. The other referral was closed after investigation.

The MPS is China's main law enforcement body, responsible for following up on STRs and for guiding and coordinating public security authorities across China in investigations involving money laundering and the seizure, freezing and confiscation of proceeds of crime. Most of these responsibilities are concentrated in the AML Division of the MPS Economic Crime Investigation Department (ECID). The Anti-Terrorism Bureau of the MPS is responsible for investigating general crimes relating to terrorist financing. Crimes against state security (including terrorism and related crimes) are the responsibility of the Ministry of State Security (MSS). The Supreme People's Procuratorate (SPP) supervises and directs the approval of arrests, prosecution, and supervision of cases involving money laundering crimes. The Supreme People's Court (SPC) supervises and directs the trial of money laundering crimes. Both can issue judicial interpretations. Law enforcement agencies are authorized to use a wide range of powers, including special investigative techniques, when conducting investigations of money laundering, terrorist financing and predicate offences. These powers include seizing articles relevant to the crime, including all (customer) records held by financial institutions. Reportedly, law enforcement and prosecutorial authorities currently focus on pursuing predicate offences, to the exclusion of AML/CTF.

China has criminalized money laundering under three separate articles of the Penal Code. Article 349 of the Penal Code was introduced in December 1990 to criminalize the laundering of proceeds generated from drug-related offenses. In June 2006, Article 191 of the Penal Code was amended to expand the criminalization of money laundering to seven predicate offenses, which now include fraud,

bribery, and embezzlement, in addition to narcotics trafficking, organized crime, smuggling, and terrorism. Article 312 was also amended in June 2006 to make it an offense to launder the proceeds of any crime through a variety of means, and it criminalizes complicity in concealing the proceeds of criminal activity.

A new Anti-Money Laundering Law, which covers AML/CTF preventative measures for the entire financial system, took effect January 1, 2007. The law broadened the scope of existing anti-money laundering regulations by mandating that financial institutions maintain thorough records on accounts and transactions, and report large and suspicious transactions. These actions firmly established the PBC's authority over national anti-money laundering efforts.

The PBC executed a revised regulatory framework in early 2007 to support the new Anti-Money Laundering Law. "Rules for Anti-Money Laundering by Financial Institutions" (AML Rules) took effect January 1, 2007, and "Administrative Rules for Reporting of Large-Value and Suspicious Transactions by Financial Institutions" (LVT/STR Rules) took effect March 1, 2007. Under the revised rules, all financial institutions-including securities, insurance, trust companies and futures dealers are considered accountable for managing their own anti-money laundering mechanisms and must report large and suspicious transactions. The LVT/STR Rules were amended on June 21, 2007 to require financial institutions to report suspicious transactions related to terrorist financing.
Under the AML and LVT/STR Rules, any cash deposit or withdrawal of over RMB 200,000 or foreign-currency withdrawal of over U.S. $10,000 in one business day must be reported within five days electronically or within 10 days in writing to the PBC Financial Intelligence Unit. Money transfers between companies exceeding RMB 2 million (approximately U.S. $274,000) in one day or between an individual and a company greater than RMB 500,000 (approximately U.S. $68,500) must also be reported. The new rules also require that all financial institutions submit monthly reports outlining suspicious activities and retain transaction records for five years. Financial institutions that fail to meet reporting requirements in a timely manner are subject to a range of administrative penalties and sanctions including having their licenses or business operations suspended.

The Administrative Rules for Financial Institutions on Customer Identification and Record Keeping of Customer Identity and Transaction Information (CDD Rules) became effective on August 1, 2007. These rules require all financial institutions to identify and verify their customers, including the beneficial owner. Specific requirements relating to the identification of legal persons (e.g. requirements to verify their legal status by obtaining proof of incorporation) have been extended to all financial institutions. The CDD Rules also introduce specific requirements for financial institutions in relation to foreign Politically Exposed Persons (PEPs), including having to obtain approval from senior management before opening an account and determining the source of funds.

China has implemented a cross-border disclosure/declaration system operated by the General Customs Administration (GCA). All cross-border transportations of cash exceeding RMB 20,000 for local currency (approximately U.S. $2,740) or for foreign currency must be declared. Bearer negotiable instruments do not need to be declared, but cross-border transportation of RMB through the mail system or in vehicles is not permitted. China has also implemented a disclosure system based on a risk-based targeting system. The GCA is authorized to conduct checks of persons entering or leaving the country, seize undeclared cash, and question, detain and sanction anyone who violates any requirement. Those who carry out physical cross border transportation related to money laundering or terrorist financing are also subject to criminal sentences. New provisions allowing the use of RMB in Hong Kong have also created loopholes for money laundering activity. From January 2005 to October 2006, there were 4,926 cases involving travelers who did not disclose cash being carried, but this data is not effectively being utilized for money laundering or terrorist financing investigations. .

China's cash-based economy, combined with robust cross-border trade, contributes to a high volume of difficult-to-track large cash transactions. While China is proficient in tracing formal financial

transactions, the large size of the informal economy—estimated by the Chinese Government at approximately ten percent of the formal economy, but quite possibly much larger—means that tracing informal financial transactions presents a major obstacle to law enforcement. Anti-money laundering efforts are further hampered by the prevalence of counterfeit identity documents and underground banks, which in some regions reportedly account for over one-third of lending activities. Only banks are authorized to provide money or value transfer services in China. Banks are not allowed to have agents that could offer such services. According to Article 174 of the Penal Code, it is a criminal offense to operate an illegal financial institution or provide financial services illegally in China. Authorities have expressed concern that criminal or terrorist groups could exploit underground banking mechanisms to bypass law enforcement. According to the FATF, China has had some success at combating illegal underground banking. Authorities destroyed 47 underground banks in 2005; in 2006, Chinese police uncovered seven underground banks and seized laundered assets totaling more than 14 billion RMB (approximately U.S. $1.92 billion).

The extent of underground banking's link to the large expatriate Chinese community is not known. Traditionally, "flying money" or fei-chien networks, are operated by money changers, gold shops, and trading companies. The international Chinese underground banking system is dependent on close associations and family ties that are resistant to most law enforcement countermeasures. Value transfer via trade goods, including barter exchange, is a common component in Chinese underground finance. Many Chinese underground trading networks in Africa, Asia, the Middle East, and the Americas are involved in the trade of Chinese-manufactured counterfeit goods, in violation of intellectual property rights. There are reports that the proceeds of narcotics produced in Latin America are laundered via trade by purchasing Chinese manufactured goods (both licit and counterfeit) in an Asian version of the Black Market Peso Exchange.

To remedy information deficiencies, the PBC launched a national credit-information system in January 2006. Although still very limited, this system allows banks to have access to information on individuals as well as on corporate entities. The new Anti-Money Laundering Law also explicitly prohibits financial institutions from opening or maintaining anonymous accounts or accounts in fictitious names, and PBC rules obligate financial institutions to perform customer due diligence, regardless of the type of customer (business or individual), type of transaction, or level of risk.

To address online fraud, the PBC has tightened regulations governing electronic payments. In 2005, the PBC announced new rules prohibiting consumers from making online purchases of more than RMB 1,000 (approximately U.S. $137) in any single transaction or more than RMB 5,000 (approximately U.S. $688) in a single day. Enterprises are limited to electronic payments of no more than RMB 50,000 (approximately U.S. $6,900) in a single day. In March 2007, Chinese regulators announced additional online restrictions regarding the use "virtual money;"—online credits sold by websites to customers to pay for games and other web-based services—amidst rumors that such credits were being used to launder money.

China is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. In 2006, China became a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Corruption.

China has signed mutual legal assistance treaties with over 24 countries and has entered into some 70 MOUs and cooperation agreements with over 40 countries. The United States and China signed a mutual legal assistance agreement (MLAA) in June 2000, the first major bilateral law enforcement agreement between the countries. The MLAA entered into force in March 2001 and provides a basis for exchanging records in connection with narcotics and other criminal investigations and proceedings. The United States and China cooperate and discuss money laundering and enforcement issues under the auspices of the U.S./China Joint Liaison Group's (JLG) subgroup on law enforcement cooperation.

In addition, the United States and China have established a Working Group on Counterterrorism that meets on a regular basis. China has established similar working groups with other countries as well.

China has signed extradition agreements with 30 countries to make it more difficult for economic criminals to seek shelter abroad. According to China's Ministry of Public Security, approximately 800 Chinese economic crime suspects have reportedly fled abroad with more than 70 billion RMB (approximately U.S. $9.1 billion) involved.

In late 2004, China joined the Eurasian Group (EAG), a FATF-style regional body that includes Russia, Belarus, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. In January 2005, China became an observer to the FATF and gained full membership in June 2007. FATF published its Mutual Evaluation Report on China in June 2007. China's FIU has applied for membership to the Egmont Group.

Subsequent to the September 11, 2001, terrorist attacks in the United States, Chinese authorities began to actively participate in U.S. and international efforts to identify, track, and intercept terrorist finances, specifically through implementation of United Nations Security Council counter-terrorist financing resolutions. According to the FATF, China has not implemented UNSCR 1267 and UNSCR 1373 in a manner that meets the specific requirements of FATF Special Recommendation III. China's primary domestic concerns with terrorist financing focus on the western Xinjiang Uighur Autonomous Region. Terrorist financing is a criminal offense in China. However, the terrorist financing laws lack clarity in a number of critical areas.

The Chinese Government significantly strengthened its anti-money laundering regime through legislative and regulatory reforms, law enforcement mechanisms, and membership in international organizations, in particular the FATF. The Chinese Government should continue to build upon actions taken in recent years to develop a viable anti-money laundering/counter-terrorist financing regime consistent with international standards. Important steps include expanding the list of predicate crimes to include terrorism, including terrorist financing, as a predicate offense. China should continue to develop a regulatory and law enforcement environment designed to prevent and deter money laundering, and it should raise awareness within the judiciary of money laundering as a criminal offense. China should ensure that law enforcement and prosecutorial authorities specifically pursue money laundering and terrorist financing offenses, and not simply treat them as a subsequent byproduct of investigations into predicate offenses. China's Anti-Money Laundering Law and related regulations should also apply to a broader range of nonfinancial businesses and professions. The application of sanctions for noncompliance with requirements that financial institutions perform customer identification, due diligence, and record keeping should be assessed to ensure that they have a genuinely dissuasive effect. In addition to strengthening its counter-terrorism finance regime, Chinese law should specifically define the term "terrorist activities" to be consistent with international standards. The Penal Code should also specify the definition of "funds" and criminalize the act of collecting funds for terrorist purposes. In addition, China should strengthen its mechanisms for freezing terrorist assets. Chinese law enforcement authorities should examine domestic ties to the international network of Chinese expatriate brokers and traders that are often linked to underground finance, trade fraud, and trade-based money laundering.

Colombia

The Government of Colombia (GOC) is a regional leader in the fight against money laundering. Comprehensive anti-money laundering regulations have allowed the government to refine and improve its ability to combat financial crimes and money laundering. Nevertheless, the laundering of money from Colombia's lucrative cocaine and heroin trade continues to penetrate its economy and affect its financial institutions. Although progress has been made in recent years, a complex legal system and limited resources for anti-money laundering programs constrain improvements.

Laundering illicit funds is related to a number of criminal activities (narcotics trafficking, commercial smuggling for tax and import duty evasion, kidnapping for profit, and arms trafficking and terrorism connected to violent paramilitary groups and guerrilla organizations), and is carried out, to a large extent, by U.S. Government-designated terrorist organizations. The GOC and U.S. law enforcement agencies closely monitor transactions that could disguise terrorist finance activities. The U.S. and Colombia exchange information and cooperation based on Colombia's 1994 ratification of the United Nations Convention against Illicit Trafficking in Narcotics and Psychotropic Substances. This convention extends into most money laundering activities resulting from Colombia's drug trade.

Colombia's economy is robust and diverse and is fueled by significant export sectors that ship goods such as coal, petroleum products, textiles and apparel, flowers, and coffee to the U.S. and beyond. While Colombia is not a regional financial center, the banking sector is mature and well regulated. An increase in financial crimes not related to money laundering or terrorist financing, such as bank fraud, has not been widely seen in Colombia. However, criminal elements have used the banking sector to launder money, under the guise of licit transactions. Money laundering has occurred via trade and the nonbank financial system, especially related to transactions that support the informal or underground economy. Colombian money is also laundered through offshore centers, generally relating to transactions involving drug-related proceeds.

Casinos in Colombia lack adequate regulation and transparency. Free trade zones in some areas of the country present opportunities for smugglers to take advantage of lax customs regulations, or the corruption of low-level officials to move products into the informal economy. Although corruption of government officials remains a problem, its scope has decreased in recent years. The GOC continues to implement steps to ensure the integrity of its most sensitive institutions and senior government officials.

Money launderers in Colombia employ a wide variety of techniques, and frequently use such methods as the Black Market Peso Exchange and contraband trade to launder the proceeds of illicit activities. Colombia's financial intelligence unit (FIU), the Financial Information and Analysis Unit (Unidad de Información y Análisis Financiero or UIAF) has identified more than ten techniques alone for laundering money via contraband trade. Colombia also appears to be a significant destination and transit location for bulk shipment of narcotics-related U.S. currency and EU euros. Local currency exchangers convert narcotics currency to Colombian pesos and then ship the U.S. dollars and euros to Central America and elsewhere for deposit as legitimate exchange house funds that are then reconverted to pesos and repatriated by wire to Colombia. Other methods include the use of debit and stored value cards to draw on financial institutions outside of Colombia and the transfer of funds out of and then back into Colombia by wire through different exchange houses to create the appearance of a legal business or personal transaction. Colombian authorities have also noted increased body smuggling (carrying currency on a person) of U.S. and other foreign currencies and an increase in the number of shell companies operating in Colombia. Pre-paid debit and stored value cards, Internet banking, and the dollarization of the economy of neighboring Ecuador represent some of the growing challenges to money laundering enforcement in Colombia.

Colombia has broadly criminalized money laundering. Under legislation passed in 1995, 1997, and 2001, the GOC has established the "legalization and concealment" of criminal assets as a separate criminal offense, and criminalized the laundering of the proceeds of extortion, illicit enrichment, rebellion, narcotics trafficking, arms trafficking, crimes against the financial system or public administration, and criminal conspiracy. Under a new law approved in 2006, penalties under the criminal code for money laundering and terrorist financing range from eight to 22 years with fines from 650 to 50,000 times the current legal minimum salary. Persons who acquire proceeds from drug trafficking are subject to a potential sentence of six to fifteen years, while illicit enrichment convictions carry a sentence of six to ten years. Failure to report money laundering offenses to

authorities is itself an offense punishable under the criminal code, with penalties increased in 2002 to imprisonment of two to five years.

Financial institutions are required by law to maintain records of account holders and financial transactions for five years. Secrecy laws have not been an impediment to bank cooperation with law enforcement officials, since under Colombian law there is a legal exemption to client confidentiality when a financial institution suspects money laundering activity. Colombia's banks have strict compliance procedures, and work closely with the GOC, other foreign governments and private consultants to ensure system integrity. General negligence laws and criminal fraud provisions ensure the financial sector complies with its responsibilities while protecting consumer rights. Obligated entities are supervised by the Superintendence of Finance. In 2007, the Superintendence of Finance issued a circular requiring entities under its authority to implement a new consolidated risk monitoring system that includes risk prevention and control measures based on international standards by January 1, 2008.

Established in 1999 within the Ministry of Finance and Public Credit, the UIAF is widely viewed as a hemispheric leader in efforts to combat money laundering and supplies considerable expertise in organizational design and operations to other FIUs in Central and South America. The UIAF has broad authority to access and analyze financial information from public and private entities in Colombia. Obligated entities, which include banks, stock exchanges and brokers, mutual funds, investment funds, export and import intermediaries, credit unions, wire remitters, exchange houses, public agencies, notaries, casinos, lottery operators, car dealers, and foreign currency traders, are required to report suspicious transactions to the UIAF, and are barred from informing their clients of their reports. Most obligated entities are also required to establish "know-your-customer" provisions. With the exception of exchange houses, obligated entities must report to the UIAF cash transactions over U.S. $5,000. The UIAF requires exchange houses to provide data on all transactions above U.S. $200. In 2007, 7,136 suspicious transaction reports (STRs) were filed through the month of September, with 58 percent of STRs deemed by UIAF to merit further investigation by their analysis unit. The Fiscalia (National Prosecutor's Office) reported 48 convictions for money laundering in 2007.

In 2006, the UIAF inaugurated a new centralized data network connecting 15 governmental entities as well as the banker's association (Asobancaria). The network allows these entities to exchange information online and share their databases in a secure manner, and facilitates greater cooperation among government agencies in preventing money laundering and other financial crimes. As of October 2007, the UIAF's database contained over 525 million transaction and activity reports. Between 2000 and September 2007, the UIAF provided authorities with 610 financial intelligence reports pertaining to 32,774 individuals, 2,031 businesses, and approximately U.S. $3.5 billion in transactions.

Given concerns about bulk cash smuggling, the GOC requires individual cash transactions above U.S. $5,000 or combined monthly transactions above U.S. $50,000 to be handled through the formal financial system, which is subject to the UIAF reporting requirements. It is illegal to transport more than the equivalent of US$ 10,000 in cash across Colombian borders, and the GOC has criminalized cross-border cash smuggling and defined it as money laundering. In spite of improvements, customs officials are inadequately equipped to detect cross-border currency smuggling. Workers rotate frequently producing inadequately trained staff. In addition, the individual customs officials are held liable for any inspected article that they damage, causing hesitation in conducting thorough inspections. Reportedly, corruption is also a problem, and customs officials often lack the proper technical equipment necessary to do their job. The GOC has been slow to make needed changes in this area.

In July 2007, the Drug Enforcement Administration (DEA) and the Department of Homeland Security's Immigration and Customs Enforcement (ICE) agency seized approximately 20 million

euros and U.S. dollars at the Miami International Airport belonging to several casas de cambio. Documents seized indicated that five of the ten registered Colombian casas de cambio had sent the currency to the United States with an ultimate destination of London. News reports in the Colombian press widely reported the downward effect on the black market currency exchange rate in Colombia resulting from these seizures. One of the five implicated financial institutions was Cambios y Capitales, which was designated by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) on October 10, 2007, as one of seven individuals and 14 companies tied to Specially Designated Narcotics Trafficker Juan Carlos Ramirez Abadia (alias "Chupeta"). Chupeta was arrested in Brazil on July 3, 2007, and is awaiting extradition to the U.S.

Colombian law provides for both conviction-based and nonconviction based in rem forfeiture, giving it some of the most expansive forfeiture legislation in Latin America. Law 793 of 2002 eliminates interlocutory appeals that prolonged and impeded forfeiture proceedings in the past, imposes strict time limits on proceedings, places obligations on claimants to demonstrate their legitimate interest in property, requires expedited consideration of forfeiture actions by judicial authorities, and establishes a fund for the administration of seized and forfeited assets. The amount of time for challenges is shorter and the focus is on the seized item (cash, jewelry, boat, etc.), placing more burdens on the accused to prove the item was acquired with legitimately obtained resources. Law 785 of 2002, the National Drug Directorate (DNE) has the authority to conduct interlocutory sales of seized assets and contract with entities for the management of assets. Law 785 also permits provisional use of seized assets prior to a final forfeiture order, including assets seized prior to the enactment of the law.

In spite of improvements to the GOC's asset forfeiture capabilities, a number of problems remain. Concerns about personal liability have discouraged official action in some cases, exceptions in proceedings can still cause cases to drag on for years, and the pace of final decisions remains slow compared to new seizures. Until this year, prosecutors had limited discretion on asset seizures and had to seize all assets associated with a case, including those of minimal value or those that clearly risk loss under state administration, such as livestock. However, in November 2007, the Attorney General approved pre-seizure guidelines, applicable to forfeitures nationwide, which will require an evaluation of an asset's worth prior to seizure, and made other significant changes to the manner in which seizures for forfeiture will be conducted. The guidelines were also approved by the DNE Director. With limited resources and only 45 staff dedicated to asset management, the DNE must rely on outside contractors to store or manage assets. The GOC has established priorities for the proceeds of disposed assets; however, DNE's management task will only be reduced when the pace of judicial decisions and disposals exceeds new seizures. In 2007, the DNE and the Fiscalia concluded their work with the U.S. Department of Justice to establish regulations and guidelines that would give Colombian prosecutors authority not to seize assets of limited value. These guidelines will also aid DNE in its task of managing the assets under its control.

The GOC pursues the seizure of assets obtained by drug traffickers through their illicit activities. For the last four years, the Sensitive Investigations Unit (SIU) of the Colombian National Police (CNP), in conjunction with U.S. law enforcement and the Colombian Fiscalia have been investigating the Cali and North Valle cartels' business empires, including the Rodriguez Orejuela brothers, the Grajales family, and Juan Carlos Ramirez Abadia ("Chupeta"). The Cali and Norte Valle cartels, as well as their leaders and associated businesses, are on the OFAC list of Specially Designated Narcotics Traffickers (SDNTs), pursuant to Executive Order 12978. The Executive Order imposes economic sanctions authorities to attack the financial empires built by Colombian narcotics traffickers.

Colombian and U.S. law enforcement agencies have cooperated in a series of investigations designed to identify and seize assets either purchased by money gained through illegal drug activity or assets used to launder drug proceeds. In August 2007, OFAC added dozens of businesses and front men tied to Chupeta's financial empire to its list of SDNTs. In September 2007, the Colombian National Police and Colombian Fiscalia seized 332 business entities and assets tied to Chupeta, which were valued at

approximately U.S. $400 million. These entities and assets included office buildings, a resort hotel, night clubs, and an amusement park. In October 2007, OFAC added additional businesses and front men tied to Chupeta's financial empire to its list of SDNTs. These joint actions to apply economic sanctions have affected the Colombian drug cartels' abilities to use many of the financial assets they derived from their narcotics trafficking activities and have assisted the Colombian government in creating cases to seize narcotics-related assets.

In 2007, several major investigations by DEA and the SIU of the Department of Administrative Security (DAS) resulted in arrests and seizures of major money laundering organizations operating between the countries. These included Operation Rock Salt, which resulted in 60 arrests for money laundering in Italy and Colombia, and the seizure of $39 million in business entities and assets in Colombia. An additional $10 million was seized under Operation Plata Sucia, which led to the arrests of 28 money launderers in Colombia and the United States, and the seizure of $5 million, 65 kilograms of heroin, and 60 kilograms of cocaine in the United States in 2006. Extradition requests to the United States are pending in many of the arrests for Operation Plata Sucia. In January 2007, the Colombian National Police in cooperation with the DEA recovered approximately $80 million in primarily U.S. currency and gold on raids on houses used to stash drug proceeds. Reportedly, the total value is probably the most ever seized by law enforcement in a single operation anywhere in the world.

ICE has also worked closely with Colombian authorities. In 2002, ICE supported the CNP establishment of a financial investigative unit within the organization's intelligence and investigations unit (DIJIN). The DIJIN has successfully initiated investigations against money laundering organizations in Colombia as well as pursued leads received from on-going U.S. investigations which have resulted in significant arrests and seizures. These include Operation Goldmine, which targeted an organization utilizing textiles as a means to launder narcotics proceeds between the U.S. and Colombia. This investigation led to 32 indictments in the U.S. and the seizure of over $9 million. The DIJIN also successfully targeted the money-laundering infrastructure of Norte Valle Cartel leader Luis Hernando Gomez Bustamante. Coordinating actions with ICE domestic and foreign offices lead to the arrest of high-level members of this organization, which have been extradited to the U.S. from Colombia and other countries, to include its leader.

ICE has also helped Colombia establish a Trade Transparency Unit (TTU) with the GOC to aggressively target trade-based money laundering organizations that facilitate the movement of criminal proceeds across borders. TTUs provide a mechanism for the GOC and the USG to identify existing vulnerabilities in both U.S. and foreign financial and trade systems, and to jointly work associated criminal investigations. Colombia's TTU is one of four established foreign TTUs, and includes members from the Directorate of Customs and Revenue (DIAN), UIAF, and DIJIN.

Terrorist financing is now an autonomous crime in Colombia. A new law entered into effect in 2007 which amended the penal code to define and criminalize direct and indirect financing of terrorism, of both national and international terrorist groups, in accordance with the Financial Action Task Force of South America (GAFISUD) and Egmont Group recommendations. The new law allows the UIAF to receive STRs regarding terrorist financing, and freeze terrorists' assets immediately after their designation. In addition, banks are now held responsible for their client base and must immediately inform the UIAF of any accounts held by newly designated terrorists. Banks also have to screen new clients against the current list of designated terrorists before the banks are allowed to provide prospective clients with services. To fulfill increased monitoring requirements, the GOC increased the size of UIAF staff to 65 positions and authorized the creation of new subdivisions for Information Management and Legal Affairs.

Colombian law is unclear on the government's authority to block assets of individuals and entities on the UN 1267 Sanctions Committee consolidated list. The government circulates the list widely among financial sector participants, and banks are able to close accounts but not seize assets. Banks also

monitor other lists, such as OFAC's publication of Specially Designated Terrorists. Charities and nongovernmental organizations (NGOs) are regulated to ensure compliance with Colombian law and to guard against their involvement in terrorist activity. This regulation consists of several layers of scrutiny, including the regulation of incorporation and the tracing of suspicious financial flows through the collection of intelligence or STR reporting.

The GOC is a member of GAFISUD. However, as a result of the GOC's failure to pay its membership dues dating back to 2004 (totaling approximately $87,000), GAFISUD placed sanctions on Colombia in July and suspended its membership on December 1. According to GOC officials, legislation must be passed to authorize the GOC to pay its membership dues; past dues had been paid without legal authorization. At its December plenary meeting, GAFISUD agreed to reinstate Colombia's membership, but the GOC's participation in GAFISUD-sponsored events is limited, and the GOC does not have a voice at GAFISUD plenary meetings. The GAFISUD Secretariat will send a letter to the President of Colombia outlining its concerns and a high-level delegation from various GAFISUD member countries will meet with GOC officials in 2008.

Colombia is a member the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group. The UIAF is a member of the Egmont Group, and has signed memoranda of understanding with 27 FIUs around the world. The GOC is a party to the1988 UN Drug Convention, the International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. The GOC has signed, but not yet ratified, the Inter-American Convention against Terrorism.

In 2007, the Government of Colombia made additional progress in the development of its financial intelligence unit, regulatory framework and interagency cooperation within the government. The implementation of a formal terrorist finance law is another development in fighting terrorism and financial crime. International cooperation with the U.S. and other countries has led to several high-profile seizures and prosecutions. However, weaknesses remain. The growth in contraband trade to launder illicit drug proceeds will require even greater interagency cooperation within the GOC, including coordination between the UIAF and DIAN, the tax and customs authority. Congestion in the court system, procedural impediments and corruption remain problems. Limited resources for prosecutors, investigators, and the judiciary hamper their ability to close cases and dispose of seized assets. Further, streamlined procedures for the liquidation and sale of seized assets under state management could help provide funds available for Colombia's anti-money laundering and counter-terrorist financing regime. The GOC is also strongly encouraged to enact legislation to permit the use of proceeds from confiscated assets to support its law enforcement efforts. In addition, the GOC should ensure that the necessary legislation is passed to allow it to pay its GAFISUD dues and become active in GAFISUD once again.

Comoros

The Union of the Comoros (Comoros) consists of three islands: Grande Comore, Anjouan and Moheli. An ongoing struggle for influence continues between the Union and island presidents. Comoros is not a principal financial center for the region. An anti-money laundering (AML) law, which addresses many of the primary AML issues of concern, was passed by Presidential Decree in 2004. However, Comoran authorities lack the capacity to effectively implement and enforce the legislation, especially on the island of Anjouan.

In May 2006, Muslim cleric Ahmed Abdallah Mohamed Sambi was elected President in the first peaceful and democratic transfer of power in Comoros' post-independence history. He won the election with 58 percent of the vote after campaigning on promises to fight corruption and unemployment. The presidency of the union rotates between the three islands. The former incumbent,

Azali Assoumani, represented Grand Comore; Sambi is from Anjouan. The three islands in the Comoros continue to retain much of their autonomy, particularly with respect to their security services, economies, and banking sectors.

One year after Sambi's election, Island president (governor) elections were scheduled on Grande Comore, Moheli, and Anjouan. The first two held free and fair elections. In Anjouan, Colonel Bacar refused elections and de facto seceded from the Union. In October 2007, the African Union applied financial and travel sanctions on Bacar and his illegitimate government. Union President Sambi and his cabinet are unable to travel to, or govern, the island of Anjouan.

Union Vice President Idi Nadhoim hosted a seminar in early 2007 on policies to combat money laundering and terrorist finance. The event was sponsored by the World Bank and the Bank of France. Union Central Bank officials, commercial banks, and operators participated, with a focus on Union policies with regard to Anjouan's illicit banking license activities. Marc Lantieri, Head of the Franc Zone at the Bank of France, made a keynote presentation on financial risk management and money laundering.

At the same seminar, Vice President Nadhoim emphasized that a stable and healthy financial system was a prerequisite for economic development. Jean Pierre Michau, an advisor to the Governor of the Bank of France, stated firmly that the Anjouan government's Internet-based banking license sales were against Comoran law and facilitated fraudulent banking activity. Vice President Nadhoim publicly accused Mr. F. LeCler of La Réunion as an accomplice of Anjouan in setting up money laundering operations. The Vice President also said Mr. Ronnie Dvorkin of "Anjouan Corporate Services" based in London was accused of violating Union Laws in his dealings with Anjouan.

Soon thereafter, Central Bank Governor Abdoulbastoi sent the United States Embassy a comprehensive report on Union Government policies and actions with regard to illicit Anjouan banking activities. Citing the 2003 law that conferred sole authority for granting banking licenses on the Union Central Bank, the Governor reported he had informed financial authorities in France, Brussels, and the United States to prohibit all activities by Anjouan-registered entities. The Governor repeated an earlier request that U.S. or European authorities help the Comoros by closing down all websites associated with Anjouan, including National Bank of Anjouan, International Company Office, Wall Street Bank, anjouan.net, anjouan.com, anjouan.org and numerous others.

The Union Central Bank has for years corresponded with French commercial banking authorities to request action against Anjouan entities. The Union Government has also issued numerous public announcements warning the public against all Anjouan financial entities. A regularly-updated circular lists the six banks properly accredited by the Union Central Bank in the Comoros: Central Bank of Comoros, Commerce and Industry Bank, Comoros Development Bank, National Post Office and Financial Services Company, Meck Union, and Sanduk Union.

The 2004 federal-level AML law is based on the French model. The main features of the law are that it: requires financial and related records to be maintained for five years; permits assets generated or related to money laundering activities to be frozen, seized and forfeited; requires residents to declare all currency or financial instruments upon arrival and departure, and nonresidents to declare all financial instruments upon arrival and all financial instruments above Comoran francs 500,000 (approximately U.S. $1,250) on departure; permits provision and receipt of mutual legal assistance with another jurisdiction where a reciprocity agreement is in existence and confidentiality of financial records is respected; requires nonbank financial institutions to meet the same customer identification standards and reporting requirements as banks; requires banks, casinos and money exchangers to report unusual and suspicious transactions (by amount or origin) to the Central Bank and prohibits cash transactions over Comorian francs 5 million (approximately U.S. $12,500); and criminalizes the provision of material support to terrorists and terrorist organizations. Although there is a suspicious activity filing requirement in the Union's AML law, there does not appear to be an independent

financial intelligence unit in either Anjouan or the Union. As of February 2006, no suspicious transaction reports had been filed with the Comorian Central Bank in Grand Comore as required under the existing Union law, and the branch of the Central Bank located in Anjouan had no knowledge of the shell bank entities that have been licensed by Anjouan's Offshore Finance Authority, which apparently operates independently from the Union's Central Bank and has licensed some 300 offshore banks, many of which appear to be shell banks.

Foreign remittances from Comorans abroad in France, Mayotte (claimed by France) and elsewhere remain the most important influx of funds for most Comorons. Until recently most remittances came via informal channels, but in 2006 Western Union established a presence to capture part of this market.

Union authorities have limited ability to implement AML laws in Anjouan and Moheli. Similarly, the island governments of Anjouan and Moheli may have limited control over AML matters. Although Moheli has its own AML law in effect (the Anti-Money Laundering Act of 2002), the law itself has some serious shortcomings and authorities lack the resources and expertise to enforce its provisions. Comprehensive information on Anjouan's laws and regulations is difficult to obtain, but it appears Anjouan does have an AML law (the Money Laundering Prevention Act, Government Notice 008 of 2005) but reportedly the law applies to Anjouan and not to the offshore entities it licenses. Little is known about: (i) the procedures that have been established to review and approve offshore licenses issued before the enactment of the AML law; (ii) the procedures that have been established to review and approve ongoing bank license applications and to supervise and monitor institutions for compliance with Anjouan laws; and (iii) the efforts and resources available to implement these procedures and enforce compliance.

President Sambi has reiterated Union Government support for efforts made under former President Azali to bring AML enforcement under Union government jurisdiction. All banking and financial institutions operating within the jurisdiction of the Union of the Comoros, whether offshore or onshore, must abide by the provisions of legislation No. 80-7 of May 3, 1980. According to article 7 of this legislation, a bank or any other financial institution cannot operate in the Union of the Comoros without prior authorization from the Union Finance Minister upon recommendation from the Comoros Central Bank. Thus, offshore banks operating in the autonomous islands of the Union of the Comoros without prior authorization from the Union Finance Minister contravene the May 3, 1980 legislation. Since taking office, President Sambi has sought to have corrupt former officials prosecuted. A grossly inadequate budget, dysfunctional ministries, and a nonfunctioning judiciary limit Sambi. Throughout 2006 there were reports that Sambi's authority in Anjouan is limited. There are reports that high-ranking Comoran officials tolerate and possibly benefit from money laundering. The lack of political will is exacerbated by the lack of capacity. Under the Constitution, the Union AML applies to all three islands, but is not enforced in Anjouan.

While the Comoros is not a principal financial center for the region, Moheli and Anjouan may have attempted or may be attempting to develop an offshore financial services sector as a means to finance government expenditures. The Anjouan island government's claim that unrelated companies are presenting themselves as licensed by the government of Anjouan makes authoritative information on Anjouan's offshore sector difficult to establish. Both Moheli, pursuant to the International Bank Act of 2001, and Anjouan, pursuant to the Regulation of Banks and Comparable Establishments of 1999, license off-shore banks. Together, the islands have licensed more than 300 banks. Applicants for banking licenses in either jurisdiction are not required to appear in person to obtain their licenses. In Anjouan, only two documents (a copy of the applicant's passport and a certificate from a local police department certifying the lack of a criminal record) are required to obtain an offshore license and fax copies of these documents are acceptable. Even if additional information was to be required, it is doubtful that either jurisdiction has the ability or resources to authenticate and verify the information. Neither jurisdiction is capable, in terms of expertise or resources, of effectively regulating an offshore

banking center. Anjouan, and probably Moheli as well, has delegated much of its authority to operate and regulate the offshore business to private, nonComoran domiciled parties. In November 2004 and again in December 2005, Anjouan island government officials denied island government involvement in the offshore sector. They said the Union of the Comoros Central Bank was the only authority for the offshore banking sector in the country and insisted the Anjouan island government had not established its own central bank. They admitted that several years earlier the government of Anjouan considered starting an offshore banking sector, but they had not pursued it. Substantial concern remains that Anjouan, and possibly Moheli, allows shell banking activity. Union President Sambi has repeatedly requested international assistance in closing any shell banks or illicit financial entities that operate within the Comoros without legitimate approval.

France, the former colonial power, maintains substantial influence and activity in Comoros, and has bypassed the Union and island governments to, where possible, prosecute suspects in money laundering or shell banks under French law. Although Comoros lacks homegrown narcotics, the islands are used as a transit site for drugs coming mainly from Madagascar. In view of international concern about drug trafficking, in 1993 France began providing technical expertise in this field to Comoros.

In addition to offshore banks, both Moheli, pursuant to the International Companies Act of 2001, and Anjouan, pursuant to Ordinance Number 1 of 1 March 1999, license insurance companies, Internet casinos, and international business companies (IBC's). Moheli claims to have licensed over 1200 IBC's. Bearer shares of IBC's are permitted under Moheli law. Anjouan also forms trusts, and registers aircraft and ships (without requiring an inspection of the aircraft or ship in Anjouan).

Comoros is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism.

Comoros has become the 12th member of the free-trade area of the Common Market for Eastern and Southern Africa (Comesa). The U.S. Export-Import Bank (ExIm Bank) has added Comoros to its Short-Term Insurance Pilot Program for Africa (STIPP), while renewing the program for three years, beginning March 31, 2006.

The Government of the Union of the Comoros (GOC) should harmonize anti-money legislation for the three islands that comprise the federal entity. The legislation should adhere to world standards. A unified financial intelligence unit should be established and the unregulated offshore financial sectors in Moheli and Anjouan should either be regulated by federal authorities or be shut down. In either case, bearer shares should be prohibited. The list of individuals and entities that are included on the United Nations 1267 Sanctions Committee's consolidated list should be circulated to banks in the Comoros. The deficiencies in the anti-money laundering/terrorist financing regimes in the Comoros and the inability to implement existing legislation make it vulnerable to traditional money laundering and to the financing of terrorism. Comoros should make every effort to comport to international standards. The total annual operating budget of the Union Finance Ministry is less than U.S. $100,000. Combined with the lack of political strength, it is highly unlikely that the needed reforms in Moheli and Anjouan will be successfully implemented without significant outside assistance.

Cook Islands

The Cook Islands is a self-governing parliamentary democracy in free association with New Zealand and a member of the British Commonwealth. Cook Islanders are citizens of New Zealand. The Cook Islands' offshore sector makes it vulnerable to money laundering. The sector offers banking, insurance, international trusts, and formation of international business companies and trusts. However,

due to recent legislative and regulatory changes, the Cook Islands complies with current international standards.

The domestic banking system is comprised of branches of two major Australian banks and the local Bank of the Cook Islands (BCI). Domestic banks are primarily involved in traditional deposit taking and lending. The BCI operates as a stand-alone institution competing against the two Australian banks and is no longer engaged in development lending. Legislation allows for development lending to be undertaken in the future by a separate company not subject to supervision by the Financial Supervisory Commission (FSC). In addition, nonperforming loans made by the Cook Islands Development Bank have been transferred to another affiliated company. In addition to the three domestic banks, the Cook Islands financial sector also consists of four international banks, seven trustee companies, and six offshore and three domestic insurance companies. The domestic insurance companies are not regulated by the FSC, but legislation is being drafted to allow regulation to take place in 2008.

The Cook Islands has an offshore financial sector that licenses international banks and offshore insurance companies and registers international business companies (IBCs). The offshore sector also consists of company services and trusts, including asset protection trusts (APTs). APTs protect the assets of individuals from civil judgments in their home countries and are able to contain a "flee clause." One of the purposes of a "flee clause," is to evade law enforcement. If a foreign law enforcement agency makes an inquiry regarding the trust, the trust will be transferred automatically to another offshore center. According to officials of the Government of the Cook Islands (GOCI), the "flee clause" exists to transfer APTs in times of emergency, such as a natural disaster, but they may also incorporate clauses designed to avoid the courts of the jurisdiction they are in or investigations by regulatory authorities. In practice they are rarely used as they are difficult to implement without the trustee finding itself in breach of the law.

The Cook Islands was placed on the Financial Action Task Force (FATF) list of Non-Cooperative Countries and Territories (NCCT) in 2000. After the GOCI addressed deficiencies in its anti-money laundering regime by enacting legislative reforms, the FATF removed the Cook Islands from its NCCT list in February 2005. The FATF conducted a year-long monitoring program, which concluded in June 2006, to closely monitor the islands.

The Banking Act 2003 and the Financial Supervisory Commission Act (FSCA) 2004 established a new framework for licensing and prudential supervision of domestic and offshore financial institutions in the Cook Islands. The legislation requires international offshore banks to have a physical presence in the Cook Islands, transparent financial statements, and adequate records prepared in accordance with consistent accounting systems. The physical presence requirement is intended to prohibit shell banks. All banks are subject to a vigorous and comprehensive regulatory process, including on-site examinations and supervision of activities.

The FSCA established the Financial Supervisory Commission as the licensed financial sector's sole regulator. The FSC is empowered to license, regulate, and supervise the business of banking. It serves as the administrator of the legislation that regulates the offshore financial sector. The FSC can license international banks and offshore insurance companies and register international companies. It also supervises trust and company service providers. Its policy is to respond to requests from overseas counterparts to the utmost extent possible. The FSC has taken a broad interpretation of the concept of "counterpart" and does not need to establish general equivalence of function before being able to cooperate.

Licensing requirements, as set out in the legislation, are comprehensive. The Banking Act 2003 and a Prudential Statement on Licensing issued in February 2004 contain detailed licensing criteria for both locally incorporated and foreign banks, including "fit and proper" criteria for shareholders and officers, satisfactory risk management, accounting and management control systems, and minimum

capital requirements. The Banking Act 2003 defines banking business, prohibits the unauthorized use of the word "bank" in a company name, and requires prior approval for changes in significant shareholding.

By enacting the Financial Transactions Reporting Act (FTRA) 2003, which replaced a similar Act passed a year earlier, the Cook Islands authorities strengthened its anti-money laundering and counter-terrorist financing (AML/CTF) legal and institutional framework. Reviews are underway to consider how the AML/CTF legislation affects other domestic laws. The Financial Supervisory Commission (FSC), regulator of the licensed financial sector is drafting new insurance legislation. The legislation will regulate the small domestic insurance sector and update supervision of the offshore insurance sector. Insurance intermediaries will also be regulated under the proposed legislation.

The FTRA imposes certain reporting obligations on 26 different types of institutions, including banks, offshore banking businesses, offshore insurance businesses, casinos, gambling services, insurers, financial advisors, solicitors/attorneys, accountants, financial regulators, lotteries and money remitters. The Minister of Finance can extend the reporting obligation to other businesses when required. Reporting institutions are required to retain all records related to the opening of accounts and financial transactions for a minimum of six years. The records must include sufficient documentary evidence to verify the customer's identity. In addition, reporting institutions are required to develop and apply internal policies, procedures, and controls to combat money laundering and to develop audit functions to evaluate such policies, procedures, and controls. Reporting institutions must comply with any guidelines and training requirements issued under the FTRA, as amended, and must provide internal training on all anti-money laundering matters. The FTRA provides for administrative and financial sanctions on institutions for noncompliance.

The FTRA requires the FSC to assess the compliance by licensed financial institutions with customer due diligence and record keeping requirements. Resulting reports and documentation from annual inspections are provided to the Cook Islands Financial Intelligence Unit (CIFIU). The CIFIU is also responsible for assessing compliance by nonlicensed institutions.

The CIFIU is the central unit responsible for processing disclosures of financial information in accordance with anti-money laundering and antiterrorist financing legislation. It became fully operational with the assistance of a Government of New Zealand technical advisor. The FTRA grants supervisory authority to the CIFIU, allowing it to cooperate with other regulators and supervisors, require reporting institutions to supplement reports, and obtain information from any law enforcement agency and supervisory body.

Obligated institutions are required to report any attempted or completed large currency transactions and suspicious transactions to the CIFIU. The currency reporting requirements apply to all currency transactions of NZ $10,000 (approximately U.S. $6870) and above, electronic funds transfers of NZ$10,000 and above, and transfers of currency in excess of NZ $10,000 into and out of the Cook Islands. Failure to declare such transactions could incur penalties. The CIFIU is required to destroy a suspicious transaction report if there has been no activity or information related to the report or to a person named in the report for six years. The CIFIU does not have an investigative mandate. If it determines that a money laundering offense, serious offense or terrorist financing offense has been or is being committed, it must refer the matter to law enforcement for investigation. The Minister of Finance, who is responsible for administrative oversight, appoints the head of the CIFIU.

The CIFIU is participating in the Pacific FIU database project (PFIUDP) provided by AUSTRAC, the Australian FIU. The CIFIU received a prototype of the database and is now testing the reporting and analysis capacity. The Pacific FIU Database Project includes other jurisdictions that will receive versions of the same database framework.

Since June 2004 the Cook Islands had made further progress in implementing its AML/CTF regime. The head of the CIFIU chairs the Coordinating Committee of Agencies and Ministries, which promotes, formalizes and maintains coordination among relevant government agencies; assists the GOCI in the formulation of policies related to AML/CTF issues; and enables government agencies to share information and training resources gathered from their regional and international networks. The AML/CTF consultative group of stakeholders facilitates consultation between government and the private sector, and ensures all financial sector players are involved in the decision making and problem solving process regarding AML/CTF regulations and reporting. The CIFIU is also a member of the Anti-Corruption Committee, along with the Office of the Prime Minister, Police, Crown Law, Audit Office, and the Financial Secretary.

The Terrorism Suppression Act 2004, based on the model law drafted by an expert group established under the auspices of the Pacific Islands Forum Secretariat, criminalizes the commission and financing of terrorism. The United Nations (Security Council Resolutions) Act 2003 allows the Cook Islands, by way of regulations, to give effect to the Security Council resolutions concerning international peace and security.

The GOCI is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. The Cook Islands is an active member of the Asia/Pacific Group on Money Laundering (APG), an associate member of the FATF. The CIFIU became a member of the Egmont Group in June 2004, has bilateral agreements allowing the exchange of financial intelligence with Australia, and is negotiating a memorandum of understanding (MOU) with Thailand. The Cook Islands plans to become a member of the Offshore Group of Banking Supervisors (OGBS), once it has qualified by undergoing further evaluation. The GOCI is also an active member of the Association of Financial Supervisors of Pacific Countries and draws on the resources of this association and Pacific Financial Technical Assistance Centre for capacity building for FSC staff. The Cook Islands has received nine requests for mutual legal assistance since the Mutual Assistance in Criminal Matters Act came into force in 2003. Five have been answered, and four are pending. The Cook Islands has not received any extradition requests from foreign countries, but successfully extradited one person from New Zealand.

The Cook Islands should continue to implement legislation designed to strengthen its nascent AML/CTF institutions. The Government of the Cook Islands should maintain vigilant regulation of its offshore financial sector, including its asset protection trusts, to ensure that its offshore sector comports with international standards.

Costa Rica

Although Costa Rica is not a major regional financial center, it remains vulnerable to money laundering and other financial crimes. Narcotics trafficking (mainly cocaine) continues to be a primary motive for money laundering, but fraud, trafficking in persons, arms trafficking, corruption, and the presence of Internet gaming companies all contribute to money laundering activity. While local criminals are active, the majority of criminal proceeds laundered derive primarily from foreign criminal activity. Reforms in 2002 to the Costa Rican counternarcotics law expanded the scope of anti-money laundering regulations, but also, unintentionally, created an opportunity to launder funds by eliminating the government's licensing and supervision of casinos, jewelers, realtors, attorneys, cash couriers, and other nonbank financial institutions. While these loopholes have not yet been closed, these weaknesses should be addressed as part of a legal reform bill on money laundering that may be passed in 2008. Bank fraud and counterfeit currency, though they do exist, do not seem to be on the rise.

Gambling is legal in Costa Rica, and there is no requirement that the currency used in Internet gaming operations be transferred to Costa Rica. There are well over 250 sports-book companies registered to

operate in Costa Rica. One U.S. citizen, who had been running a sports-book company in Costa Rica, was arrested in the Dominican Republic in 2007.

Costa Rica is not considered an offshore financial center. While the formal banking industry in Costa Rica is tightly regulated, the offshore banking sector, which offers banking, corporate and trust formation services, remains an area of concern. Foreign-domiciled offshore banks can only conduct transactions under a service contract with a domestic bank, and they do not engage directly in financial operations in Costa Rica. They must also have a license to operate in their country of origin. Furthermore, they must comply with Article 126 of the Costa Rican Central Bank's Organic Law, which requires offshore banks to have assets of at least U.S. $3 million, a physical presence in Costa Rica, and be subject to supervision by the banking authorities of their registered country. Shell banks are not allowed in Costa Rica and regulated institutions are forbidden from having any direct or indirect relationships with institutions that may be described as shell banks or fictitious banks. Bearer shares are not permitted in Costa Rica.

Currently, six offshore banks maintain correspondent operations in Costa Rica: three from The Bahamas and three from Panama. The Government of Costa Rica (GOCR) has supervision agreements with its counterparts in both countries, permitting the review of correspondent banking operations. However, these counterpart regulatory authorities occasionally interpret the agreements in ways that limit review by Costa Rican officials. In 2005, the Attorney General ruled that the Superintendent General of Financial Entities (SUGEF) lacked authority to regulate offshore operations due to an apparent contradiction between the 1995 Organic Law of the Costa Rican Central Bank and Law 8204. Draft legislation to correct the contradiction and reassert the SUGEF's regulatory power is under review in the Legislative Assembly and is expected to pass in 2008. Costa Rican authorities acknowledge that they are currently unable to adequately assess risk.

The GOCR reports that Costa Rica is primarily used as a bridge to send funds to and from other jurisdictions using, in many cases, companies or established banks in offshore financial centers. Alternative remittance systems exist in Costa Rica, mainly as a result of Costa Rican immigration to the United States, or Nicaraguans to Costa Rica. However, there is no confirmation that these remittance systems are used for money laundering.

There are 287 free trade zones (FTZs) within Costa Rica. The Promotora del Comercio Exterior de Costa Rica (PROCOMER) manages the FTZ regime and has responsibility for registering all qualifying companies. PROCOMER's qualification process consists of conducting due diligence on a candidate company's finances and assessing the total cost of ownership. PROCOMER annually audits all of the firms within the FTZ regime and touts its system of tight controls. The four major types of firms operating in Costa Rica's FTZ regime are manufacturing, services, trading, and administrative organizations. PROCOMER reports that there has been no evidence of money laundering activity in the FTZs in 2007.

In 2002, the GOCR enacted Law 8204. Law 8204 criminalizes the laundering of proceeds from all serious crimes (not only drug-related money laundering), which are defined as crimes carrying a sentence of four years or more. Law 8204 obligates financial institutions and other businesses to identify their clients, report currency transactions over U.S. $10,000 and suspicious transactions to the financial intelligence unit (FIU), the Unidad de Analisis Financiero (UAF). Law 8204 also requires that financial records be retained for at least five years, and that the beneficial owners of accounts and funds involved in transactions be identified. While Law 8204, in theory, applies to the movement of all capital, current regulations are narrowly interpreted so that the law applies only to those entities that are involved in the transfer of funds as a primary business purpose, such as exchange houses and stock brokerages. Therefore, the law does not cover such entities as casinos, dealers in jewels and precious metals, insurance companies, intermediaries such as lawyers, accountants or broker/dealers, or Internet gambling operations, as their primary business is not the transfer of funds.

Costa Rican financial institutions are regulated by the Office of the Superintendent General of Financial Entities (SUGEF), the Superintendent General of Securities (SUGEVAL), and the Superintendent of Pensions (SUPEN). All three of these entities fall under the National Council of Supervision of the Financial System (CONASSIF). All financial entities subject to the jurisdiction of SUGEF, SUGEVAL and SUPEN are obligated to submit suspicious transaction reports (STRs), regardless of the amount involved or transaction reported. Law 8204 does not establish any protection for reporting individuals with respect to their cooperation with law enforcement entities. Nevertheless, this does not exempt them from reporting; if they do not file STRs, they may be subject to pecuniary sanctions established in Article 81 of Law 8204.

The UAF, which is located within the Costa Rican Drug Institute (ICD), became operational in 1998. Article 123 of Law 8204 empowers the UAF to request, collect and analyze STRs and cash transaction reports (CTRs) submitted by obligated entities. The Money Laundering, Financial, and Economic Crimes Unit of the Judicial Investigative Organization (OIJ), under the Public Ministry (Prosecutor's Office), receives a copy of the information sent to the UAF. This practice gives rise to the possibility of duplication of information and waste of time and resources, and the risk of contamination or leakage of information. Each superintendence holds the CTRs until the UAF requests them. All requests and reports from the UAF must be signed by the Director of the ICD. Approval and authorization is therefore given by the Director of the ICD, not the Director of the UAF. This practice may interfere with the UAF's operational autonomy.

The UAF has no regulatory responsibilities. The UAF has access to the records and databases of financial institutions and other government entities, but must obtain a court order if the information collected is to be used as evidence in court. Additionally, there are formal mechanisms in place to share information domestically and with other countries' FIUs.

In spite of its broad access to government information and high levels of cooperation with the financial sector, the UAF remains ill-equipped and under-funded to provide information needed by investigators. Additionally, in 2007, the UAF had a 40 percent turnover in personnel, including one of their most senior analysts. Nevertheless, in 2007, the UAF continued to increase the quality of its analysis and forwarded more thoroughly analyzed cases to prosecutors. The UAF received 280 STRs in 2007, 92 of which are still under review.

The GOCR body responsible for investigating financial crimes is the OIJ. The OIJ is assisted by the UAF and has adequately trained staff. In 2007, there were two prosecutions for financial crimes.

All persons carrying entering or exiting Costa Rica are required to declare any amount over U.S. $10,000 to Costa Rican officials at ports of entry. Declaration forms are required. Cash smuggling reports are entered into a database maintained by ICD and is shared with appropriate government agencies, including the UAF.

Articles 33 and 34 of Law 8204 cover asset forfeiture and stipulate that all movable or immovable property used in the commission of crimes covered by this act shall be subject to preventative seizure. When seizure or freezing takes place, the property is placed in a legal deposit under the control of ICD. The banking industry closely cooperates with law enforcement efforts to trace funds and seize or freeze bank accounts. During 2007, officials seized over U.S. $9.6 million (an increase over the U.S. $5.2 million seized in 2006) in narcotics-related assets, much of it in undeclared cash. Seized assets are processed by the ICD and if judicially forfeited, are divided among drug treatment agencies (60 percent), law enforcement agencies (30 percent), and the ICD (10 percent).

Although the GOCR has ratified the major UN counterterrorism conventions, terrorist financing is not a crime in Costa Rica. In 2002, a government task force drafted a comprehensive counterterrorism law with specific terrorist financing provisions. The draft law, when passed, would expand existing conspiracy laws to include the financing of terrorism and enhance existing narcotics laws by

incorporating the prevention of terrorist financing into the mandate of the ICD. In 2007, Costa Rica was notified that if its terrorist financing law was not passed by May 2008, it risks being expelled from the Egmont Group of financial intelligence units. The GOCR expects the legislation to be passed by the May 2008 deadline.

Costa Rican authorities receive and circulate to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. However, these authorities cannot block, seize, or freeze property without prior judicial approval. Thus, Costa Rica lacks the ability to expeditiously freeze assets connected to terrorism. No assets related to designated individuals or entities were identified in Costa Rica in 2007.

Costa Rica fully cooperates with appropriate USG law enforcement agencies and other governments investigating financial crimes related to narcotics and other crimes. Articles 30 and 31 of Law 8204 grant authority to the UAF to cooperate with other countries in investigations, proceedings, and operations concerning financial and other crimes covered under that law.

Costa Rica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. On March 21, 2007, the GOCR ratified the UN Convention against Corruption. The GOCR has also signed, but not yet ratified, the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, and has ratified the Inter-American Convention against Terrorism. Costa Rica is a member of the Caribbean Financial Action Task Force (CFATF), and assumed the CFATF presidency in 2007. The most recent mutual evaluation of Costa Rica was conducted by the CFATF in July 2006. The GOCR is a member of the Money Laundering Experts Working Group of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD). The UAF is a member of the Egmont Group.

Even though the Government of Costa Rica convicted a handful of individuals for money laundering over the last several years, further efforts are required to bring Costa Rica into compliance with international anti-money laundering and counter-terrorist financing standards. The GOCR should criminalize terrorist financing prior to the Egmont Group deadline for expulsion. The GOCR should also pass legislation that reconciles contradictions regarding the supervision of its offshore banking sector, and should extend its anti-money laundering legislation and regulations to cover the Internet gaming sector, dealers in jewelry and precious metals, attorneys, casinos, and other nonbank financial institutions. Costa Rica should ensure that its financial intelligence unit and other GOCR authorities are adequately equipped to combat financial crime.

Côte d'Ivoire

The Republic of Cote d'Ivoire is an important West African regional financial hub. Money laundering and terrorist financing in Cote d'Ivoire are not primarily related to narcotics proceeds. Criminal proceeds that are laundered are reportedly derived from regional criminal activity, such as the smuggling of consumer goods and agricultural products. Reportedly, most of the smuggling networks are organized chiefly by nationals from Nigeria and the Democratic Republic of the Congo. Due to the ongoing political and economic turmoil in Cote d'Ivoire, respect for the rule of law continues to deteriorate. As a result, Ivorian and some other West African nationals are becoming more and more involved in criminal activities and the subsequent laundering of funds. Cote d'Ivoire is ranked 150 out of 179 countries in Transparency International's 2007 Corruption Perceptions Index. The extent to which Ivorian territory is used in the growing use of West Africa as a transshipment point for drugs from South America to Europe is largely unknown. The de facto ongoing division of the country makes such an assessment, as well as that of Cote d'Ivoire's possible associated role as a drug laundering center, difficult.

The outbreak of the rebellion in 2002 increased the amount of smuggling of goods across the northern borders, including cocoa, timber, textiles, tobacco products, and light motorcycles. There have also been reports of an increase in the processing and smuggling of diamonds from mines located in the north. Ivorian law enforcement authorities have, until the mid-2007, had very little control over the northern half of the country. While national authority is slowly being redeployed, the government's control over borders in the formerly rebel-controlled regions of the country remains very weak. The relationship between revenues associated with smuggled goods and narcotics proceeds remains unclear due to the lack of effective border controls in the north. Smuggling of sugar, cotton, cocoa, cars, and pirated DVDs occurs in the government-controlled south and is motivated by a desire to avoid the payment of taxes. According to the Office of the Customs Financial Enquiries, the cross-border trade of diamond and cocoa over Cote d'Ivoire's porous borders generates contraband funds that are laundered into the banking system via informal moneychangers. Criminal enterprises use both the formal and informal financial sector to launder funds. Cash is moved both via the formal banking sector and by cash couriers. Cash earned by immigrant or migrant workers generally flows out of Cote d'Ivoire, going to extended families outside the region.

Banks have begun to resume operations, but because banking services were largely absent from the northern part of Côte d'Ivoire until the end of 2007, informal money couriers, money transfer organizations similar to hawaladars and, increasingly, goods transportation companies transferred funds domestically, as well as within the sub-region. Domestic informal value transfer systems are not regulated. Informal remittance transfers from outside Cote d'Ivoire violate West African Central Bank (BCEAO) money transfer regulations. The standard fee for informal money transfer services is approximately ten percent. In addition to transferring funds, criminal enterprises have been known to launder illicit funds by investing in real estate and consumer goods such as used cars in an effort to conceal the source of funding.

Hizballah is present in Côte d'Ivoire and conducts fundraising activities, mostly among the large Lebanese expatriate community. The Ivorian government has taken no legal action to prevent the misuse of charitable and or other nonprofit entities that can be used as conduits for the financing of terrorism. Reportedly, the Ministry of Interior Security is addressing this problem.

There are no free trade zones in Cote d'Ivoire. In August 2004, the Ivorian government adopted a plan for the creation of a free trade zone for information technology and for biotechnology. This project remains dormant.

The Economic and Financial Police report an ongoing rise in financial crimes related to credit card theft and foreign bank account fraud, which includes wire transfers of large sums of money primarily involving British and American account holders who are the victims of Internet based advance fee scams. The Ministry of Finance remains concerned by the high levels of tax fraud, particularly VAT tax fraud, by merchants. The country has the largest bank network in the region. French financial interests account for the majority of retail and other banking and insurance services. The banking law was recently changed to require banks be capitalized with U.S. $10 million and nonbank financial institutions (mortgage firms, insurance companies, etc.) with U.S. $5 million.

The Ivorian banking law, enacted in 1990, prevents disclosure of client and ownership information, but does allow the banks to provide information to judicial authorities such as investigative magistrates. The law also permits the use of client and ownership information as evidence in legal proceedings or during criminal investigations. The Tax and Economic police can request information from the banks.

Until recently, the penal code criminalized only money laundering related to drug trafficking, fraud, and arms trafficking. On November 29, 2005, the National Assembly adopted the l'Union Economique et Monetaire Ouest Africaine/West African Economic and Monetary Union

(l'UEMOA/WAEMU), common law on money laundering, making all forms of money laundering a criminal offense.

The law focuses on the prevention of money laundering and also expands the definition to include the laundering of funds from all serious crimes. The law does not set a minimum threshold. It includes standard "know your customer" requirements for banks and other financial institutions, and establishes procedures and a suspicious transaction reporting obligation which covered institutions must follow to assist in the detection of money laundering. The law provides for the creation of an Ivorian financial intelligence unit (FIU), as well as a legal basis for international cooperation. The new law includes both criminal and civil penalties, and permits the freezing and seizure of assets, which can be instruments for and proceeds of crime. Legitimate businesses are among the assets which can be seized if used to launder money or support terrorist or other illegal activities. Substitute assets cannot be seized if there is no relationship with the offense.

The money laundering law provides for the establishment of a financial intelligence unit (FIU) known as "Cellule Nationale de Traitement des Informations Financieres" (CENTIF). Participants at the September 2007 L'UEMOA/WAEMU meeting of finance ministers had urged Cote d'Ivoire to accelerate the start of CENTIF operations. CENTIF members were nominated on December 20, 2007. The government of Cote d'Ivoire announced on January 8, 2008 that CENTIF is now operational, and its members were sworn in on January 16, 2008. It reports to the Finance Minister. On a reciprocal basis and with the permission of the Ministry of Finance, CENTIF can share information with other FIUs in L'UEMOA/WAEMU and with those of nonL'UEMOA/WAEMU countries, as long as those institutions keep the information confidential.

Once established, the FIU will continue to work with previously established investigative units such as the Centre de Recherche Financiere (CRF) at the Department of Customs and the Agence Nationale de Strategie et d'Intelligence (ANSI) at the presidency. The CRF and the ANSI will still continue their missions, which include fiscal and customs fraud and counterfeiting. The Economic and Financial police, the criminal police unit (Police Judiciaire), the Department of Territorial Surveillance, the CRF and ANSI all are responsible for investigating financial crimes, including money laundering and terrorist financing.

The Ministry of Finance, the BCEAO, and the West African Banking Commission, headquartered in Cote d'Ivoire, supervise and examine compliance with anti-money laundering/counter-terrorist financing (AML/CTF) laws and regulations. All Ivorian financial institutions are required to maintain customer identification and transaction records for ten years. Additionally, as in all BCEAO member countries, all bank deposits over CFA 5,000,000 (approximately U.S. $10,000) must be reported to the BCEAO, along with customer identification information. Law enforcement authorities can request access to these records to investigate financial crimes through a public prosecutor. In 2007, there were no arrests or prosecutions for money laundering or terrorist financing.

The new legislation imposes a ten-year retention requirement on financial institutions to retain records of all "significant transactions," which are transactions with a minimum value of CFA 50,000,000 (approximately U.S. $100,000) for known customers. New money laundering controls apply to nonbank financial institutions such as exchange houses, stock brokerage firms, insurance companies, casinos, cash couriers, national lotteries, nongovernment organizations, travel agencies, art dealers, gem dealers, accountants, attorneys, and real estate agents. The law also imposes certain customer identification and record maintenance requirements on casinos and exchange houses. The tax office (Ministry of Finance) supervises these entities. All Ivorian financial institutions, nonfinancial businesses, and professions subject to the scope of the money laundering law are required to report suspicious transactions. The Ivorian banking code protects reporting individuals. Their identities are not divulged with respect to cooperation with law enforcement authorities.

Cote d'Ivoire monitors and limits the international transport of currency and monetary instruments under L'UEMOA/WAEMU administrative regulation R/09/98/CM/L'UEMOA/WAEMU. There is no separate domestic law or regulation. When traveling to another L'UEMOA/WAEMU country, Ivorian and expatriate residents must declare the amount of currency being carried out of the country. When traveling to a destination other than another L'UEMOA/WAEMU country, Ivorian and expatriate residents are prohibited from carrying an amount of currency greater than the equivalent of 500,000 CFA francs (approximately U.S. $1,000) for tourists, and two million CFA francs (approximately U.S. $4,000) for business operators, without prior approval from the Department of External Finance of the Ministry of Economy and Finance. If additional amounts are approved, they must be in the form of travelers' checks.

Cote d'Ivoire does not have a specific law that criminalizes terrorist financing, as required under UNSCR 1373, although financing of all "serious crimes" falls under the domain of the law. Until the passage of the 2005 money laundering law, the Government of Cote d'Ivoire (GOCI) relied on several L'UEMOA/WAEMU directives on terrorist financing, which provided a legal basis for administrative action by the GOCI to implement the asset freeze provisions of UNSCR 1373. The BCEAO and the government report that they promptly circulate to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's Consolidated List and those on the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. To date, no assets related to terrorist entities or individuals have been discovered, frozen or seized.

The GOCI participates in the Intergovernmental Group for Action against Money Laundering (GIABA) based in Dakar, which is the Financial Action Task Force-style regional body (FSRB) for West Africa. GIABA has scheduled a mutual evaluation scheduled for Cote d'Ivoire for November 2008. Other than the authority granted to CENTIF by the AML law, the GOCI has neither adopted laws nor promulgated regulations that specifically allow for the exchange of records with United States on money laundering and terrorist financing.

Cote d'Ivoire has demonstrated a willingness to cooperate with the United States in investigating financial or other crimes. For example, in a 2007 case, a prominent American government official based in the UK was defrauded by a party based in Cote d'Ivoire who was using the individual's credit card information to purchase expensive medical equipment and ship it to Cote d'Ivoire. While the perpetrator(s) were not apprehended, Ivorian authorities worked cooperatively with U.S. law enforcement.

Cote d'Ivoire is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. The GOCI has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

The Government of Cote d'Ivoire should specifically criminalize terrorist financing and become a party to the relevant UN Conventions. The Ministry of Finance should work to build capacity at CENTIF to maximize effectiveness in FIU functions, especially analysis, outreach and information sharing. CENTIF should work toward becoming a member of the Egmont Group. The GOCI's law enforcement and customs authorities need to implement measures to diminish smuggling, trade-based money laundering and informal value transfer systems. The GOCI should also enact legislation criminalizing terrorist financing and facilitating information sharing with other countries. Authorities should also take steps to halt the spread of corruption that permeates both commerce and government and facilitates the continued growth of the underground economy and money laundering. Cote d'Ivoire should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Cyprus

Cyprus has been divided since the Turkish military intervention of 1974, following an unsuccessful coup d'etat directed from Greece. Since then, the Republic of Cyprus (ROC) has controlled the southern two-thirds of the country, while a Turkish Cypriot administration calling itself the "Turkish Republic of Northern Cyprus (TRNC)" controls the northern part. Only Turkey recognizes the "TRNC." The U.S. Government recognizes only the Republic of Cyprus This report primarily discusses the area controlled by the ROC but also includes a separate section on the area administered by Turkish Cypriots.

Cyprus is a major regional financial center with a robust financial services industry and a significant amount of nonresident businesses. As with all such centers, Cyprus remains vulnerable to international money laundering activities. Fraud along with other financial crimes and narcotics trafficking are the major sources of illicit proceeds laundered in Cyprus.

A number of factors have contributed to the development of Cyprus as a financial center: the island's central location; a preferential tax regime, double tax treaties with 40 countries (including the United States, several European Union (EU) nations, and former Soviet Union nations); a labor force well trained in legal and accounting skills; a sophisticated telecommunications infrastructure; and EU membership.

Four authorities regulate and supervise financial institutions in Cyprus: the Central Bank of Cyprus, responsible for supervising locally incorporated banks and money transfer businesses; the Cooperative Societies Supervision and Development Authority (CSSDA), supervising cooperative credit institutions; the Superintendent for Insurance Control; and the Cyprus Securities and Exchange Commission. Three entities act as regulators for designated nonfinancial businesses and professions (DNFBPs): the Council of the Bar Association supervises attorneys; the Institute of Certified Public Accountants supervises accountants; and the financial intelligence unit (FIU) supervises real estate agents and dealers in precious metals and stones. The supervisory authorities may impose administrative sanctions if the legal entities or persons they supervise fail to meet their obligations as prescribed in Cyprus' anti-money laundering (AML) laws and regulations.

Cyprus currently hosts a total of 43 banks, 17 of which are incorporated locally. The remaining 26 banks are branches of foreign-incorporated banks and conduct their operations mainly with nonresidents. At the end of August 2007, the cumulative assets of all banks were U.S. $112 billion. Under the EU's "single passport" policy, banks licensed by competent authorities in EU countries could establish branches in Cyprus or provide banking services on a cross-border basis without obtaining a license from the Central Bank of Cyprus,. By the end of 2007, nine foreign banks were operating a branch in Cyprus under this arrangement.

Cyprus hosts seven licensed money transfer companies, 65 investment firms, two management firms handling "undertakings for collective investment in transferable securities" (UCITS), 40 licensed insurance companies, 400 licensed real estate agents, 2,311 registered accountants, 1,810 practicing lawyers, and around 165 cooperative credit institutions, controlling about 32 percent of total deposits. Stricter EU requirements on credit institutions have pushed cooperative credit institutions to merge on a large scale over the last three years. Their number shrank from 359 to the current 165 in less than three years, and authorities expect it to drop to just over 100 by the middle of 2008.

In recent years, Cyprus has introduced tax and legislative changes effectively abolishing all legal and substantive distinctions between domestic and offshore companies. All Cypriot companies now pay taxes at a uniform rate of 10 percent, irrespective of the permanent residence of their owners or whether they do business internationally or in Cyprus. Cyprus has lifted the prohibition from doing business domestically and companies formerly classified as offshore are now free to engage in business locally. In March 2007, Cyprus withdrew from the Offshore Group of Banking Supervisors.

The Cypriot government made this move specifically to change the focus and impression of its foreign business from "offshore" to "international." By removing any distinction between resident and nonresident or on-shore and offshore companies, the same disclosure, reporting, tax and other laws and regulations apply equally to all registered companies. Despite these stricter standards, few of the estimated 54,000 nonresident companies established in Cyprus as of 2006 have taken themselves off the company register and the number of new nonresident companies registering in Cyprus continues to increase as a result of the low tax rate and high service quality.

Cyprus continues to revise its anti-money laundering (AML) framework to meet evolving international standards. The Prevention and Suppression of Money Laundering Activities Law criminalizes all money laundering, establishes a customer identification requirement and obligations for suspicious transaction reporting, provides for the confiscation of proceeds from serious crimes, and codifies the actions that banks, nonbank financial institutions, and obligated nonfinancial businesses must take, The AML law establishes the financial intelligence unit (FIU) and authorizes criminal (but not civil) seizure and forfeiture of assets. The definition of predicate offense is any criminal offense punishable by a prison term exceeding one year. Cypriot AML legislation addresses government corruption, provides for the sharing of assets with other governments, and facilitates the exchange of financial information with other FIUs. Cypriot authorities reportedly have full access to information concerning the beneficial owners of every company registered in Cyprus. This includes companies doing business abroad and companies with foreign beneficial owners and shareholders. Due diligence and reporting requirements extend to auditors, tax advisors, accountants, and, in certain cases, attorneys, real estate agents, and dealers in precious stones and gems. Although the professional organizations for accountants and lawyers publicize strict "know your customer" regulations, the regulatory oversight of these sectors is reportedly nearly nonexistent. Violations result in administrative fines of up to Cyprus Pounds (CP) 3,000 (approximately U.S. $7,500). The FIU can instruct banks, financial institutions and other obligated entities to delay or prevent execution of customers' transactions. Casinos and Internet gaming sites are not permitted, although sports betting halls are allowed.

ROC law requires all persons entering or leaving Cyprus to declare all currency, Cypriot or foreign, and gold bullion worth CP 7,300 (approximately U.S. $18,250) or more. The Central Bank has the authority to revise this amount. On June 15 2007, EU Directive 1889/2005, went into effect. As a result, for currency worth €10,000 (U.S. $14,620) or more, Cyprus regulates cash transactions for travelers entering its borders from countries outside the EU.

Cyprus is currently in the process of passing legislation entitled "Law for the Prevention and Suppression of Money Laundering Activities," which was expected to pass without significant changes before the end of 2007. This legislation will consolidate and supersede existing legislation. When enacted, the draft law will encompass all recent FATF and MONEYVAL recommendations, and revises Cyprus' AML legislation, to harmonize it with the EU's Third AML Directive. This Directive mandated implementation by December 15, 2007. The new law provides much stricter administrative fines for noncompliance, i.e., from the current €5,130 (U.S. $7,500) to €200,000 (U.S. $292,400) and generally raises Cyprus' AML standards.

The draft law also addresses: enhanced due diligence extending coverage of "politically-exposed persons" (PEPs), cross-border transactions, and transactions with customers not physically present or on behalf of third parties. The law introduces simplified due diligence for certain persons or entities deemed to be low risk as well as requirements for Unit for Combating Money Laundering (MOKAS), the Cypriot financial intelligence unit (FIU), and other supervisory authorities to collect statistical data. MOKAS must provide banks and other obligated entities with feedback in response to any STR submission. The law criminalizes the general collection of funds with the knowledge that terrorists or terrorist groups would use them for any purpose (i.e., not just for violent acts); and terrorism finance is explicitly covered by the new law (although already considered a predicate offense under existing legislation).

A second draft law, expected to pass by early 2008, regulates trust and company service providers (other than accountants and lawyers), bringing them under the supervisory authority of the Central Bank. As soon as these laws go into effect, the supervisory authorities will issue revised directives.

In October 2006, the IMF released a detailed assessment of the "Observance of Standards and Codes for Banking Supervision, Insurance Supervision and Securities Regulation." The report noted that the Cyprus Securities and Exchange Commission (SEC) was legally unable to cooperate with foreign regulators if the SEC did not have a direct interest and that the SEC had difficulty obtaining information regarding the beneficial owners of Cypriot-registered companies. The report also noted that commitments emerging from EU accession had "placed stress on the skills and resources" of the staff of the Co-operative Societies Supervision and Development Authority (CSSDA) and the Insurance Superintendent. The SEC has drafted amending legislation to resolve these issues, expected to pass by early 2008.

In recent years the Central Bank has introduced regulations aimed at strengthening AML vigilance in the banking sector. Among other requirements, banks must ascertain the identities of the natural persons who are the "principal/ultimate" beneficial owners of all legal entities; adhere to the October 2001 paper of the Basel Committee on Banking Supervision on "Customer Due Diligence for Banks"; and pay special attention to business relationships and transactions involving persons from jurisdictions identified by the Financial Action Task Force (FATF) as deficient in their AML regime, particularly concerning counter-terror financing (CTF).

All banks must report to the Central Bank, on a monthly basis, individual cash deposits exceeding 10,000 Cypriot pounds (approximately U.S. $22,000 in local currency) or approximately U.S. $10,000 in foreign currency. Bank employees must report all suspicious transactions to the bank's compliance officer, who determines whether to forward a report to the Cypriot FIU for investigation. Banks retain reports not forwarded to the FIU, which the Central Bank audits as part of its regular on-site examinations. Banks must file monthly reports with the Central Bank indicating the total number of suspicious transaction reports (STRs) submitted to the compliance officer and the number forwarded by the compliance officer to the FIU. Bank officials may be held personally liable if their institutions launder money. Cypriot law partially protects reporting individuals with respect to their cooperation with law enforcement but does not clearly absolve a reporting institution or its personnel from complete criminal or civil liability. Banks must retain client identification data, transaction records, and business correspondence for five years.

Central Bank money laundering directives place additional obligations on banks, including requirements on customer acceptance policy; and updating customers' identification data and business profiles. Banks must have computerized risk management systems to verify whether a customer constitutes a PEP; provide full details on any customer sending an electronic transfer in excess of U.S. $1,000; and have adequate management information systems for on-line monitoring of customers' accounts and transactions. Cypriot banks typically use electronic risk management systems to target transactions to and from high-risk countries, as well as high-risk customers. Since the expiration of Cyprus' Exchange Control Law, the Central Bank no longer reviews foreign investment applications for nonEU residents. Since January 1, 2007, Cyprus has begun implementing EU Directive 1781/2006 ("Information on the Payer Accompanying Transfers of Funds"), which requires full disclosure of details for electronic fund transfers in excess of €1,000 (U.S. $1,462).

The Central Bank also requires compliance officers to file annual reports outlining measures taken to prevent money laundering and to comply with its guidance notes and relevant laws. In addition, the Central Bank has the authority to conduct unannounced inspections of bank compliance records. In July 2002, the U.S. Internal Revenue Service (IRS) officially approved Cyprus' "know-your-customer" rules, which form the basic part of Cyprus' AML system. As a result of the approval, banks

in Cyprus that acquire United States securities on behalf of their customers may enter into a "withholding agreement" with the IRS and become qualified intermediaries.

The Prevention and Suppression of Money Laundering Activities Law mandated the establishment of the Unit for Combating Money Laundering (MOKAS), the Cypriot financial intelligence unit (FIU). MOKAS is responsible for receiving and analyzing STRs and for conducting money laundering investigations. A representative of the Attorney General's Office heads the unit. All banks and nonbank financial institutions, insurance companies, the stock exchange, cooperative banks, lawyers, accountants, and other financial intermediaries must report suspicious transactions to MOKAS. Sustained efforts by the Central Bank and MOKAS to strengthen reporting have resulted in a significant increase in the number of STRs being filed. Between January 1 and November 19, 2007, MOKAS received 160 STRs. In the same interval, MOKAS received 261 information requests from foreign FIUs, other foreign authorities, and INTERPOL. MOKAS cooperates closely with the U.S. in money laundering investigations.

Money laundering is an autonomous crime in Cyprus. MOKAS evaluates evidence generated by its member organizations and other sources to determine if an investigation is necessary. MOKAS has the power to administratively suspend financial transactions for an unspecified period of time. MOKAS also has the power to apply for freezing or restraint orders affecting any kind of property at a preliminary stage of an investigation. MOKAS has issued several warning notices, based on its own analysis, identifying possible trends in criminal financial activity. These notices have resulted in the closure of dormant bank accounts. MOKAS conducts AML training for Cypriot police officers, bankers, accountants, and other financial professionals, and, in conjunction with the Central Bank of Cyprus, for bankers.

During the interval from January 1 through November 19, 2007, MOKAS opened 447 cases and closed 150. Since 2000, there have been 13 prosecutions for money laundering, one of which took place in 2007. Of the 13 prosecutions, eight have resulted in convictions. In 2007, MOKAS issued one confiscation order for a total of approximately $10.5 million. A number of other cases are pending.

Sections 4 and 8 of the Ratification Law 29 (III) of 2001 criminalize terrorist financing. The implementing legislation amends the AML law to criminalize the collection of funds in the knowledge that these would be used by terrorists or terrorist groups for violent acts. The parliament passed an amendment to the implementing legislation in July 2005 eliminating a loophole that had inadvertently excused Cypriot nationals operating in Cyprus from prosecution for terrorism finance offenses. MOKAS routinely asks banks to check their records for any transactions by any person or organization designated by foreign FIUs or the U.S. Treasury Department as a terrorist or a terrorist organization.

Under a standing instruction, the Central Bank automatically issues a "search and freeze" order for accounts matching the name of any entity or group designated by the UN 1267 Sanctions Committee or the EU Clearinghouse as a terrorist or terrorist organization. If a financial institution finds matching accounts, it will immediately freeze the accounts and inform the Central Bank. As of November 2007, no bank has reported holding a matching account. When FIUs or governments—not the UN or the EU Clearinghouse—designate and circulate the names of suspected terrorists, MOKAS has the authority to block funds and contacts commercial banks directly to investigate. To date, none of these checks have revealed anything suspicious. The lawyers' and accountants' associations cooperate closely with MOKAS and the Central Bank. Cyprus cooperates with the United States to investigate terrorist financing. MOKAS reports that no terrorist assets have been found in Cyprus to date and thus there have been no terrorist finance prosecutions or freezing of terrorist assets. In 2006, there was one investigation for terrorist financing involving four persons.

Cyprus believes that its existing legal structure is adequate to address money laundering through alternative remittance systems such as hawala. Cypriot authorities maintain that there is no evidence

that alternative remittance systems such as hawala operate in Cyprus. Cyprus licenses charitable organizations, which must submit copies of their organizing documents and annual statements of account to the government. The majority of charities registered in Cyprus are reportedly domestic organizations.

Cyprus is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Cyprus has signed, but not ratified, the UN Convention Against Corruption. Cyprus is a member of MONEYVAL the FATF-style regional body for Council of Europe member states. MOKAS is a member of the Egmont Group and has signed memoranda of understanding (MOUs) with 17 FIUs, although Cypriot law allows MOKAS to share information with other FIUs without benefit of an MOU. A mutual legal assistance treaty between Cyprus and the United States entered into force September 18, 2002.

Cyprus has put in place a comprehensive AML/CTF regime, which it continues to upgrade. Cyprus should ensure not only the passage, but also the full implementation, of the two laws that will tighten the current regime requirements. Cyprus should ensure that it is able to implement the law criminalizing the collection of funds with the knowledge that they will be used by terrorists or terrorist groups for any purpose, not only to commit terrorist or violent acts. Cyprus should enact provisions that allow for civil forfeiture of assets in the future.

Area Administered by Turkish Cypriots. The Turkish Cypriot community continues to lack the legal and institutional framework necessary to provide effective protection against the risks of money laundering. There are currently 24 domestic banks in the area administered by Turkish Cypriots. Internet banking is available. The offshore sector consists of 14 banks and approximately 50 companies. The offshore banks may not conduct business with residents of the area administered by Turkish Cypriots and may not deal in cash. The "Central Bank" audits the offshore entities, which must submit an annual report on their activities. However, the "Central Bank" has no regulatory authority over the offshore banks and can neither grant nor revoke licenses. Instead, the "Ministry of Finance" performs this function. A new law restricts the granting of new bank licenses to only those banks with licenses in an OECD country or a country with "friendly relations" with the "TRNC." A new law to more closely regulate offshore banks is pending in "parliament."

It is thought that the 18 essentially unregulated and primarily Turkish-mainland owned casinos and the 14 offshore banks are the primary vehicles through which money laundering occurs. Casino licenses are fairly easy to obtain, and background checks on applicants are minimal. A significant portion of the funds generated by these casinos reportedly change hands in Turkey without ever entering the Turkish Cypriot banking system, and there are few safeguards to prevent the large-scale transfer of cash to Turkey. Another area of concern is the approximately five hundred "finance institutions" operating in the area that extend credit and give loans. Although they must register with the "Office of the Registrar of Companies," they remain unregulated. Some of these companies are owned by banks and others by auto dealers. Recent years have seen a large increase in the number of sport betting halls, which are licensed by the "Office of the Prime Minister." There are currently five companies operating in this sector, with a total of 30 outlets. Four of the companies also accept bets over the Internet. Turkish Cypriot authorities deported one prominent Turkish organized crime figure, Yasar Oz, following a December 19, 2006 shootout at the Grand Ruby Casino that left two dead. As a result of this incident, the Turkish Cypriot authorities arrested seven individuals, closed the Grand Ruby and Denizkizi Casinos and deported much of their staff. Nevertheless, several other casinos are still believed to have significant links to organized crime groups in Turkey.

The fact that the "TRNC" is recognized only by Turkey limits the ability of Turkish Cypriot authorities to receive training or funding from international organizations with experience in combating money laundering. The Turkish Cypriot community is not part of any regional FATF-style

organization and thus is not subject to any peer evaluations. In 2007, FATF conducted an informal review and found numerous shortcomings in AML laws and regulations as well as insufficient resources devoted to the effort. Turkish Cypriot officials objected to the conclusions.

The offshore banking sector remains a concern. In August 2004, the U.S. Department of the Treasury's FinCEN, pursuant to Section 311 of the USA PATRIOT Act, found First Merchant Bank to be of primary money laundering concern based on a number of factors. These factors, included that it is licensed as an offshore bank in a jurisdiction with inadequate AML controls, particularly those applicable to its offshore sector; and that it is involved in the marketing and sale of fraudulent financial products and services. Other factors point to its use as a conduit for the laundering of fraudulently obtained funds; and its apparent use to launder criminal proceeds by the individuals who own, control, and operate First Merchant Bank—individuals with links to organized crime. In December 2006, the Turkish Cypriot administration ordered First Merchant Bank to cease its operations due to violations of the Turkish Cypriot "Offshore Banking Law." The bank is now only permitted to perform activities associated with closing the Bank such as the payment and collection of outstanding debts.

Turkish Cypriot authorities have begun taking limited steps to address the risk of financial crime, including enacting an anti-money laundering law (AMLL) for the area. The law aims to reduce the number of cash transactions in the area administered by Turkish Cypriots. as well as improve the tracking of any transactions above U.S. $10,000. Under the AMLL, banks must report to the "Central Bank" any electronic transfers of funds in excess of U.S. $100,000. Such reports must include information identifying the person transferring the money, the source of the money, and its destination. Banks, nonbank financial institutions, and foreign exchange dealers must report all currency transactions over U.S. $20,000 and suspicious transactions in any amount. Banks must follow a know-your-customer policy and require customer identification. Banks must also submit suspicious transaction reports (STRs) to a five-member "Anti-Money Laundering Committee (AMLC)" which decides whether to refer suspicious cases to the "police" and the "attorney general's office" for further investigation. The five-member committee is composed of representatives of the "police," "customs," the "Central Bank," and the "Ministry of Finance." However, the AMLL has never been fully implemented or enforced.

In 2005, the "AMLC," which had been largely dormant for several years, began meeting on a regular basis and encouraging banks to meet their obligations to file STRs. The committee has reportedly referred several cases of possible money laundering to law enforcement for further investigation, but no cases have been brought to court and no individuals have been charged. There have been no successful prosecutions of individuals for money laundering, although one foreign bank owner suspected of having ties to organized crime was successfully extradited. There are significant concerns that law enforcement and judicial authorities lack the technical skills needed to investigate and prosecute financial crimes. The "AMLC" also complains that since foreign jurisdictions will not cooperate with them by providing evidence or appearing to testify, they have difficulty presenting cases to their court system.

Although the AMLL prohibits individuals entering or leaving the area administered by Turkish Cypriots from transporting more than U.S. $10,000 in currency without prior "Central Bank" authorization, "Central Bank" officials note that this law is difficult to enforce. This is particularly true given the large volume of travelers to and from Turkey, especially since Turkish Cypriot authorities relaxed restrictions that limited travel across the UN-patrolled buffer zone. There is also a relatively large British population in the area administered by Turkish Cypriots and a significant number of British tourists. As a result, an informal currency exchange market has developed.

The "Ministries of Finance, Economy and Tourism" are drafting several new AML laws that they claim will, among other things, establish an FIU and provide for better regulation of casinos, currency

exchange houses, and both onshore and offshore banks. Turkish Cypriot authorities have committed to ensuring that the new legislation meets international standards. However, it is unclear if or when the new legislation will be adopted, and if it is adopted, whether it will ever be fully implemented and enforced. Work on the new bills has been ongoing for more than three years. Turkish Cypriot officials have promised FATF that the laws will pass in 2007, after which the European Commission plans to help with their implementation through selected training and funding.

The Turkish Cypriot AMLL provides better banking regulations than were previously in force, but as an AML tool it is far from adequate, and without ongoing enforcement, cannot meet its objectives. A major weakness continues to be the many casinos, where a lack of resources and expertise leave that area essentially unregulated and therefore especially vulnerable to money laundering abuse. The largely unregulated finance institutions, currency exchange houses, and offshore banking sector are also of concern. The Turkish Cypriot authorities should move quickly to enact a new anti-money laundering law, establish a strong, functioning "financial intelligence unit", and adopt and implement a strong regulatory environment for all obliged institutions, in particular casinos, money exchange houses, and entities in the offshore sector. Turkish Cypriot authorities should take steps to enhance the expertise of members of the enforcement, regulatory, and financial communities with an objective of better regulatory guidance, the more efficient STR reporting, better analysis of reports, and enhanced use of legal tools available for prosecutions. Passage of new laws and willingness to cooperate with foreign experts for implementation will be the early tests of a change in approach to these issues.

Czech Republic

The Czech Republic is one of the most stable and prosperous of the post-Communist states of Central and Eastern Europe. However, the Czech Republic's central location in Europe and its relatively new status as a functional market economy have left it vulnerable to money laundering. While various forms of organized crime (narcotics trafficking, trafficking in persons, fraud, counterfeit goods, embezzlement and smuggling) remain the primary source of laundered assets in the country, Czech officials and media outlets have voiced increasing concern about the ability of extremist groups and terrorists to launder or remit money within the country. Domestic and foreign organized crime groups target Czech financial institutions for laundering activity, most commonly by means of financial transfers through the Czech Republic. Banks, currency exchanges, casinos and other gaming establishments, investment companies, and real estate agencies have all been used to launder criminal proceeds. Currency exchanges in the capital and border regions are also considered to be a major problem.

The growth of the Czech Republic economy between 2000 and 2007 was supported by exports to the European Union (EU), primarily to Germany. However, despite the progressive development of modern payments techniques, the economy is still heavily cashed-based. The Czech Republic decided to adopt the single European currency (euro) in connection with its accession to the EU in 2004, and in July 2007 the Organizational Committee of National Coordination Group published "The National Changeover Plan for the Czech Republic," which covers the technical, legislative and organizational preparation for the future introduction of the euro in Czech Republic.

Major sources of criminal proceeds include criminal offenses against property, insurance fraud, and credit fraud. Connections between organized crime and money laundering have been observed mainly in relation to activities of foreign groups, in particular from the former Soviet republics, the Balkan region, and Asia. The Czech Republic is also vulnerable to other illicit financial activities conducted through credit and loan services, money remittances (particularly in connection with the Asian community), and illegal foreign exchange business.

The Government of the Czech Republic (GOCR) first criminalized money laundering in September 1995 through additions to its Criminal Code. Although the Criminal Code does not explicitly mention

money laundering, its provisions apply to financial transactions involving the proceeds of all serious crimes. A July 2002 amendment to the Criminal Code introduces a new independent offense called "Legalization of Proceeds from Crime." This offense has a wider scope than previous provisions and enables prosecution for laundering one's own illegal proceeds (as opposed to those of other parties). The 2002 amendment also stipulates punishments of five to eight years imprisonment for the legalization of proceeds from all serious criminal activity and calls for the forfeiture of assets associated with money laundering. Despite some improvements, the criminalization of money laundering under Section 252a ("Legalization of Proceeds from Criminal Activity") of the Criminal Code still does not contain a broad definition and coverage of money laundering. To date, Section 252a has mostly been applied to criminal offenses that have more to do with stolen goods than with the laundering proceeds.

The Czech anti-money laundering legislation (Act No. 61/1996, Measures Against Legalization of Proceeds from Criminal Activity) became effective in July 1996. The Anti-Money Laundering (AML) Act, which provides for the general preventive framework, was adopted in 1996 and covered only the banking sector. It has been amended several times and to comply with EU requirements. The law now requires a wide range of financial institutions, as well as attorneys, casinos, realtors, notaries, accountants, tax auditors, and entrepreneurs engaging in financial transactions, to report all suspicious transactions to the Ministry of Finance's financial intelligence unit (FIU), known as the Financial Analytical Unit (FAU). Suspicious transactions exceeding 15,000 euros (approximately U.S. $22,140) must be reported, and those exceeding 1,000 euros (approximately U.S. $1,476) must be identified internally.

The GOCR recently approved a new draft law on "Measures against Legalization of Proceeds from Criminal Activity and Terrorism Financing." This proposal implements the EU's Third Money Laundering Directive. Legislative approval by December 15, 2007, as requested by the EU, is expected. In connection with this effort, the Czech National Bank is preparing an amendment to the foreign currency law that would introduce new regulations and licensing requirements for currency exchanges.

The Law on International Sanctions that came into force in April 2006 also represents progress by the GOCR. Under this law, the Ministry of Finance has the authority to fine institutions for failure to report accounts or other assets belonging to individuals, organizations, or countries, on which international sanctions have been imposed, or those not fulfilling other obligations set by international regulations. Earlier laws restricting financial cooperation with the Taliban (2000) and Iraq (2005) were replaced by the Law on International Sanctions.

The Czech Republic still has more than 2.6 million anonymous deposit passbooks containing 3.9 billion crowns (approximately U.S. $200 million). Due to ongoing criticism, the Czech Republic introduced legislation in 2000 prohibiting new anonymous passbook accounts. In 2002 the Act on Banks was amended to abolish all existing bearer passbooks by December 31, 2002. In principle, bearer passbooks will be completely phased out by 2012. While account holders can still withdraw money from the accounts for another few years, the accounts do not earn interest and cannot accept deposits. In 2007, approximately 350 million crowns (approximately $18 million) were withdrawn from these accounts. Although in general the customer identification procedures are mostly in place, full customer due diligence (CDD) requirements should be introduced in the AML Act with appropriate guidance.

Czech authorities require that financial institutions maintain transaction records for a period of ten years. Reporting requirements also apply to persons or entities seeking to enter the Czech Republic. Under the provisions of the AML Act, anyone entering or leaving the Czech Republic with more than 10,000 euros (approximately U.S. $14,750) in cash, traveler's checks, or other monetary instruments must make a declaration to customs officials, who are required to forward the information to the FAU.

Similar reporting requirements apply to anyone seeking to mail the same amount in cash to or from the country. In practice, the effectiveness of these procedures is difficult to assess. With the accession of the Czech Republic to the EU, nearly all customs stations on the borders were closed. Although the customs station at the Prague Airport remains operational, detecting the smuggling or transport of large sums of currency by highway is difficult.

The FAU was established in July 1996 as an administrative FIU under the umbrella of the Ministry of Finance. It has overall supervisory competence to ensure the implementation of the AML Act by all obliged entities Since 2000 financial institutions have been required to report all suspicious transactions to the FAU. The FAU is authorized to share all information with the Czech Intelligence Service (BIS) and Czech National Security Bureau (NBU) in addition to its ongoing cooperation with the Czech Police, Customs, and counterparts abroad. The GOCR expects that this type of information sharing will improve the timeliness and nature of exchanges between the different agencies within the Czech government.

The FAU is charged with reviewing suspicious transaction reports (STRs) filed by police agencies, financial, and other institutions. It is also charged with uncovering cases of tax evasion, which is a widespread problem in the Czech Republic The FAU has neither the mandate nor the capacity to initiate or conduct criminal investigations. Investigative responsibilities remain with the Czech National Police Unit for Combating Corruption and Financial Crimes (UOKFK) or other Czech National Police bodies. The FAU's work covers only a relatively small segment of total financial activity within the Czech Republic. Since April 2006, the FAU has had the power to fine financial institutions that fail to report accounts or other assets belonging to individuals, organizations, or countries on which international sanctions have been imposed.

The UOKFK has primary responsibility for all financial crime and corruption cases. Following the dissolution of the specialized Financial Police on January 1, 2007, the unit became the main law enforcement counterpart to the FAU and is responsible for investigations of terrorist financing cases. Following the abolition of the Financial Police, the UOKFK took over all of its ongoing cases, but the pace of investigations has slowed.

The number of STRs transmitted to the FAU has been growing. There were 3,404 suspicious transactions reported in 2005 and 3,480 in 2006. From January through October 2007, there were 1,729 reports of suspicious transactions. This upward trend is interpreted as evidence of the active participation of concerned entities in the anti-money laundering regime. Conversely, the number of inquiries evaluated and forwarded to law enforcement bodies have decreased compared to 2005. In 2005, the FAU forwarded 208 reports to the police and only 137 in 2006. From January through October 2007, the number of reports forwarded to the police was 82; in 25 cases, the payments were temporarily frozen. The abolition of the Financial Police and the transfer of its cases to the Unit Combating Corruption and Financial Crimes caused temporary difficulties in communication between the FAU and the Police. It is not clear whether every case transferred to law enforcement was investigated. Cooperation with foreign counterparts remains good. In 2005, the FAU received 130 assistance requests from abroad and sent 69 requests abroad. In 2006, it received 128 and sent 77. During the first nine months of 2007, the FAU received 102 requests and sent out 49 requests.

From January to June 2007, the Police investigated eight individuals, but did not seize any related funds. This is a significant decrease from 2006, when the police investigated 11 offenders and seized 373 million crowns (approximately $20 million). The decrease can be partially explained by the abolition of the specialized Financial Police.

The Czech Republic saw its first convictions of individuals attempting to legalize proceeds from crime only in 2004. In 2005, there were 23 alleged offenders prosecuted and three were convicted. In 2006, there were 33 were prosecuted, and five convicted. In the first half of 2007, only six people were prosecuted and two convicted. The sentences were low and included suspended sentences or fines. An

ongoing issue in criminal prosecutions is that law enforcement agencies must prove that the assets in question were derived from criminal activity. The accused is not obligated to prove that the property or assets were acquired legitimately.

While the institutional capacity to detect, investigate, and prosecute money laundering and financial offenses has increased in recent years, both the FAU and the Police face staffing challenges. The Financial Action Task Force (FATF) and the Council of Europe's FATF-style regional body (MONEYVAL) have both emphasized the need for the Czech Republic to increase the FAU's staff. Given the scope of its responsibilities, the FAU remains a relatively small organization. The Police face even bigger challenges due to recent changes in police retirement rules and the perceived lack of political support for independent police work. Many senior and experienced police officers are reportedly leaving or are considering early retirement. These departures will affect not only the UOKFK, but the Organized Crime Unit and other critical police organizations as well. The dissolution of the Financial Police, which was created in 2004 in response to EU recommendations and had a good track record of investigating and prosecuting money laundering and terrorist finance cases, has also had a negative impact on police work on financial crimes.

Czech laws facilitate the seizure and forfeiture of bank accounts. A financial institution that reports a suspicious transaction has the authority to freeze the suspect account for up to 24 hours. However, for investigative purposes, this time limit can be extended to 72 hours to give the FAU sufficient time to investigate whether there is evidence of criminal activity. Currently, the FAU is authorized to freeze accounts for 72 hours. If sufficient evidence of criminal activity exists, the case is forwarded to UOKFK, which has another three days to gather the necessary evidence. If the UOKFK is able to gather enough evidence to start prosecution procedures, then the account can stay frozen for the duration of the investigation and prosecution. If, within the 72-hour time limit, the UOKFK fails to gather sufficient evidence to convince a judge to begin prosecution, the frozen funds must be released. These time limits do not apply to accounts owned by suspected terrorists and terrorist organizations, or by other individuals and organizations covered under the Law on International Sanctions.

Although Czech law authorizes officials to use asset forfeiture, it is still not widely used. It was introduced into the criminal system in 2002 and allows judges, prosecutors, or the police (with the prosecutor's consent) to freeze an account or assets if evidence indicates that the contents were used or will be used to commit a crime, or if the contents are proceeds of criminal activity. In urgent cases, the police can freeze the account without the previous consent of the prosecutor, but within 48 hours must inform the prosecutor, who then confirms the freeze or releases the funds. An amendment to the 2004 Law on the Administration of Asset Forfeiture in Criminal Procedure implemented provisions and responsibilities overseeing the administration and storage of seized property and appoints the police as administrators of seized assets.

A 2006 amendment to the Czech Criminal Procedure Code and Penal Code brought several positive changes to the asset forfeiture and seizure law. The law, as amended, now allows for the freezing and confiscation of the value of any asset (including immovable assets) and is not limited to property. These provisions allow the police and prosecutors to seize assets gained in illicit activity previously shielded by family members. The law allows for the seizure of substitute asset values as well as asset values not belonging to the criminal.

The National Drug Headquarters (NDH) cooperates with the UOKFK on drug-related cases. However, as a result of the abolition of the Financial Police the NDH conducts its basic financial investigations alone and, if needed, contacts the UOKFK. In the first ten months of 2007, the NDH confiscated 1.9 million crowns (approximately U.S. $108,000), 44 thousand euros (approximately U.S. $65,000), and other assets valued at 1.8 million crowns (approximately U.S. $103,000).

In November 2004, the Czech Government amended the Criminal Code and enacted new definitions for terrorist attacks and terrorist financing. A penalty of up to 15 years' imprisonment can be imposed

on those who support terrorists financially, materially, or by other means. In addition to reporting all suspicious transactions possibly linked to money laundering, concerned institutions are now required to report all transactions suspected of being tied to terrorist financing. An amendment to the anti-money laundering law in 2000 requires financial institutions to freeze assets that belong to suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committees consolidated list.

The Czech Republic ratified the UN International Convention for the Suppression of the Financing of Terrorism in October 2005. Subsequently, the GOCR adopted the National Action Plan for the Fight against Terrorism for 2005-2007. This document covers topics such as police work and cooperation, protection of security interests, enhancement of security standards, and customs issues. The fight against terrorist financing is one of the major priorities contained in the plan.

Although the terrorist finance threat in the Czech Republic is considered to be modest, some law enforcement officials believe that the presence of third-country remuneration networks operating in the country ("hawala" shops) could translate into a greater possibility of financing terrorist activities. The Czech Republic has specific laws criminalizing terrorist financing and legislation permitting rapid implementation of UN and EU financial sanctions, including action against accounts held by suspected terrorists or terrorist organizations. A governmental body called the Clearinghouse was established in 2002 to streamline the collection of information from institutions to enhance cooperation and response to a terrorist threat. The Clearinghouse meets only in cases of necessity. It has not met thus far in 2007. The FAU is currently distributing lists of designated terrorists to relevant financial and governmental bodies. Czech authorities have been cooperative in the global effort to identify suspect terrorist accounts, and adoption of the Law International Sanctions has made their work easier. Several cases have been detected, and payments to suspected organizations were not permitted. No sanctions have been imposed.

The Czech Republic has signed memoranda of understanding on information exchange with 23 countries, and, most recently, signed a new agreement with Paraguay. The Czech Republic formalized an agreement with Europol in 2002. The FAU has been a member of the Egmont Group since 1997 and is authorized to cooperate and share information with all of its international counterparts, including those that are not part of the Egmont Group. The Czech Republic participates in MONEYVAL. The most recent mutual evaluation of Czech Republic was conducted by the MONEVAL in 2006. The mutual evaluation report (MER) was adopted by the MONEYVAL at its 24th plenary meeting in December 2007.

The Czech Republic is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The Czech Republic is also a party to the World Customs Organization's Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offenses as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

The United States and the Czech Republic have a Mutual Legal Assistance Treaty (MLAT), which entered into force on May 7, 2000, as well as an extradition treaty that has been in effect since 1925. In May 2006, the United States and the Czech Republic signed a supplemental extradition treaty and a supplemental MLAT to implement the U.S.-EU Agreements on these subjects; however, these instruments have not yet been ratified.

The Government of the Czech Republic has made progress in its efforts to strengthen its money laundering regime. The GOCR cooperates to a large extent with foreign counterparts in the field of anti-money laundering and counter-terrorist financing. However, the incomplete Czech legal framework on seizure and confiscation is a major limitation to its international cooperation, and its staffing problems could be an obstacle to timely and effective collaboration. Czech authorities are using a risk-based approach when determining priorities and imposing obligations on obliged entities.

However, there is a tendency to rely on assumptions rather than on assessments, and as a result there is a lack of unanimity on sectors exposed to and used for money laundering purposes. The Czech Republic should approve already-drafted amendments to its existing money laundering legislation by to implement the European Union's Third Money Laundering Directive. The GOCR should also ratify the UN Convention against Transnational Organized Crime and UN Convention against Corruption.

Dominica

The Commonwealth of Dominica initially sought to attract offshore dollars by offering a wide range of confidential financial services, low fees, and minimal government oversight. A rapid expansion of Dominica's offshore sector without proper supervision made it attractive to international criminals and vulnerable to official corruption. In response to international criticism, Dominica enacted legislation to address many of the deficiencies in its anti-money laundering and counter-terrorist financing regime.

Dominica's financial sector includes one offshore bank, approximately 12,787 international business companies (IBCs) (an increase from 11,452 in 2006), 20 insurance agencies, six money remitters, one building and loan society, and three operational Internet gaming companies. However, reports indicate more Internet gaming sites may exist. There are no free trade zones in Dominica.

Under Dominica's Economic Citizenship Program, individuals can purchase citizenship and obtain passports for approximately U.S. $75,000 for an individual and U.S. $100,000 for a family of up to four persons. There is no residency requirement and passport holders may travel to Commonwealth countries without a visa. An application for economic citizenship must be made through a government approved local agent and requires a fee for due diligence or background check purposes. An in-person interview is also required. Dominica's Economic Citizenship Program does not appear to be adequately regulated. In the past, subjects of United States criminal investigations have been identified as exploiting this program. In 2007, 15 individuals acquired economic citizenship.

Under common banking legislation enacted by its eight member jurisdictions, the Eastern Caribbean Central Bank (ECCB) acts as the primary supervisor and regulator of onshore banks in Dominica. The ECCB, in conjunction with the Financial Services Unit (FSU), supervises Dominica's offshore bank. The ECCB assesses applications for offshore banking licenses, conducts due diligence checks on applicants, and provides a recommendation to the Minister of Finance. Offshore banks are required to have a physical presence and are forbidden from opening client accounts before verifying the beneficial owner of the bearer shares and/or companies. The Minister of Finance is required to seek advice from the ECCB before exercising his powers with respect to licensing and enforcement.

The ECCB also conducts on-site inspections for anti-money laundering compliance of onshore and offshore banks in Dominica. Inspections of offshore banks are conducted by the ECCB in collaboration with the FSU. The Offshore Banking (Amendment) Act No. 16 of 2000 prohibits the opening of anonymous accounts, prohibits IBCs from direct or indirect ownership of an offshore bank, and requires disclosure of beneficial owners and prior authorization to changes in beneficial ownership of banks. All offshore banks are required to have available for review on-site books and records of transactions. Per the Banking Act, which went into effect in Dominica in 2006, the ECCB is able to share information directly with foreign regulators through a memorandum of understanding (MOU).

The International Business Companies Act (IBCA) enacted in 1996 and amended in 2000, requires that bearer shares be kept with an approved fiduciary, who is required to maintain a register with the names and addresses of beneficial owners. Additional amendments to the Act in September 2001 require previously issued bearer shares to be registered. Dominica permits "shelf companies" or ready made offshore companies. Shelf companies have already been incorporated with a nominee director and nominee shareholder, and are for sale for immediate use. IBCs are not required to have a physical

presence and are restricted from conducting local business activities. Internet gaming entities must register as IBCs.

The IBCA empowers the FSU to perform regulatory, investigatory, and enforcement functions over IBCs. The FSU also supervises, regulates, and inspects Dominica's registered agents and conducts on-site visits to ensure that the companies are operating in compliance with requirements imposed by law. The FSU staff consists of a manager, two professional staff (supervisors/examiners), and one administrative assistant.

Amendments to the Money Laundering Prevention Act (MLPA) No. 20 of December 2000 adopted in 2001 criminalize the laundering of proceeds from any indictable offense. The law applies to narcotics-related money laundering and all hybrid or indictable offenses as predicate offenses for money laundering, whether committed in Dominica or elsewhere. The MLPA overrides secrecy provisions in other legislation and requires financial institutions to keep records of transactions for at least seven years. The MLPA also requires persons to report cross-border movements of currency that exceed U.S. $10,000 to the financial intelligence unit (FIU). The MLPA requires a wide range of financial institutions and businesses, including any offshore institutions, to report suspicious transactions simultaneously to the MLSA and the FIU. Additionally, financial institutions are required to report any transaction over U.S. $5,000.

The MLPA establishes the Money Laundering Supervisory Authority (MLSA) and authorizes it to inspect and supervise nonbank financial institutions and regulated businesses for compliance with anti-money laundering legislation. The MLSA is also responsible for developing anti-money laundering policies, issuing guidance notes, and conducting training. The MLSA consists of five members: a former bank manager, the FSU manager, the Deputy Commissioner of Police, a senior State Attorney, and the Deputy Comptroller of Customs.

The 2001 Money Laundering Prevention Regulations apply to all onshore and offshore financial institutions including banks, trusts, insurance companies, money transmitters, regulated businesses, and securities companies. The regulations specify know-your-customer requirements, record keeping, and suspicious transaction reporting procedures, and require compliance officers and training programs for financial institutions. The regulations require that the true identity of the beneficial interests in accounts be established, and mandate the verification of the nature of the business and the source of the funds of the account holders and beneficiaries. Reporting entities are protected by law with respect to their cooperation with law enforcement entities. Anti-Money Laundering Guidance Notes, also issued in 2001, provide further instructions for complying with the MLPA and provide examples of suspicious transactions to be reported to the MLSA and the FIU.

The FIU, established under the MLPA, became operational in August 2001. The FIU's staff consists of a certified financial investigator and a director. The FIU analyzes suspicious transaction reports (STRs) and cross-border currency transactions reports, forwards appropriate information to the Director of Public Prosecutions, and works with foreign counterparts on financial crimes cases. The FIU has access to records of financial institutions and other government agencies with the exception of the Inland Revenue Division. In 2007, the FIU received 17 STRs. The FIU is closely examining the relationship between narcotics proceeds and money laundering in Dominican financial institutions. However, Dominica believes most of the money laundering cases under investigation involves external proceeds from fraudulent investment schemes.

The MLPA provides for the freezing of assets for seven days by the FIU, after which time a suspect must be charged with money laundering or the assets released. All assets that can be linked to any individual or legitimate business under investigation can be seized or forfeited, providing that the amount seized or forfeited does not exceed the total benefit gained by the subject from the crime committed. The court can order the confiscation of frozen assets. Pursuant to the MLPA, tangible confiscated assets such as vehicles or boats are forfeited to the state. Intangible assets such as cash or

bank accounts are split between the forfeiture fund and the government-consolidated fund by 80 and 20 percent, respectively. In 2006, $55,481 was frozen but subsequently the matter was discontinued by the Director of Public Prosecutions and the funds returned. No statistics are currently available on the amount of assets frozen or seized in 2007.

There are no known convictions on money laundering charges in Dominica and there were no arrests or prosecutions for money laundering or terrorist financing in 2007. In 2006, a French national was arrested for attempting to obtain a line of credit through fraudulent wire transfers; he had been under investigation since 2004 for misappropriation of funds from Guadeloupe nationals. Since 2003, Dominica has collaborated closely with U.S. and foreign law enforcement agencies in a widespread money laundering case involving a European fraudulent investment scheme proceeds in one of the now closed offshore banks in Dominica.

In 2003, Dominica enacted the Suppression of Financing of Terrorism Act (No. 3 of 2003), which provides authority to identify, freeze, and seize terrorist assets, and to revoke the registration of charities providing resources to terrorists. The MLSA and the Office of the Attorney General supervise and examine financial institutions for compliance with anti-money laundering and counter-terrorist financing laws and regulations. The Government of the Commonwealth of Dominica (GOCD) circulates pertinent terrorist lists to financial institutions. To date, no accounts associated with terrorists or terrorist entities have been found in Dominica. There were no terrorist-related assets frozen, forfeited, or seized in 2007. The GOCD has not taken any specific initiatives focused on alternative remittance systems.

In 2000, a Mutual Legal Assistance Treaty between Dominica and the United States entered into force. However, in 2007, Dominica has not been cooperative in meeting mutual legal assistance requests. The GOCD also has a Tax Information Exchange Agreement with the United States but Dominica has not responded to more than two dozen requests from the USG for information regarding a potential money laundering case involving both countries. The MLPA authorizes the FIU to exchange information with foreign counterparts. Cash smuggling reports are not shared with foreign governments.

Dominica is a member of the Caribbean Financial Action Task Force (CFATF). The GOCD is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Dominica's FIU became a member of the Egmont Group in June 2003. Dominica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and to the Inter-American Convention against Terrorism. The GOCD has neither signed nor ratified the UN Convention against Corruption or the UN Convention against Transnational Organized Crime.

The Government of the Commonwealth of Dominica should fully implement and enforce the provisions of its legislation and provide additional resources for regulating offshore entities, including immobilizing the bearer shares of current "shell companies". It should stringently regulate Internet gaming entities. Dominica should take measures to update its anti-money laundering regulations and guidance notes to reflect current international standards. In addition, Dominica should conduct awareness training for financial institutions, specifically banks, to ensure their understanding and compliance of STR reporting requirements. The GOCD should either commit to engage in scrupulous due diligence on Economic Citizenship applicants, or eliminate the program. Per its agreements with the United States Government (USG), Dominica should make efforts to share information with the USG in an effective and timely manner as stipulated under the terms of its MLAT and Tax information Exchange Agreement. The GOCD should also become a party to the UN Convention against Corruption and the UN Convention against Transnational Organized Crime.

Dominican Republic

As a major transit country for drug trafficking, the Dominican Republic remains vulnerable to money laundering. Financial institutions in the Dominican Republic engage in currency transactions involving international narcotics trafficking proceeds that include significant amounts of U.S. currency or currency derived from illegal drug sales in the United States. The smuggling of bulk cash by couriers and the use of wire transfer remittances are the primary methods for moving illicit funds from the United States into the Dominican Republic. Once in the Dominican Republic, currency exchange houses, money remittance companies, real estate and construction companies, and casinos facilitate the laundering of these illicit funds.

Money laundering in the Dominican Republic is criminalized under Act 17 of 1995 (the 1995 Narcotics Law) and Law No. 72-02 of 2002. Under these laws, the predicate offenses for money laundering include illegal drug activity, trafficking in human beings or human organs, arms trafficking, kidnapping, extortion related to recordings and electronic tapes, theft of vehicles, counterfeiting of currency, fraud against the state, embezzlement, and extortion and bribery related to drug trafficking. Law 183-02 also imposes financial penalties on institutions that engage in money laundering, although the Government of the Dominican Republic (GODR) is in the process of amending the law to add a parallel structure of criminal penalties. Law No. 78-03 permits the seizure, conservation and administration of assets that are the product or instrument of criminal acts pending judgment and sentencing. The 1995 Narcotics Law allows preventive seizures and criminal forfeiture of drug-related assets, and authorizes international cooperation in forfeiture cases.

While narcotics-related investigations have been initiated under the 1995 Narcotics Law, and substantial currency and other assets have been confiscated, there have been only four successful money laundering prosecutions under this law. In August 2006, the Attorney General's office created a financial crimes unit to actively pursue financial crimes and money laundering investigations to aid in prosecutors' ability to obtain money laundering convictions. Since 2006, there have been 25 investigations and seven cases brought to court, one of which is the Banco Intercontinental (BANINTER) case.

The 2003 collapse of BANINTER revealed 14 years of double-bookkeeping designed to hide sweetheart loans, embezzlement, and money laundering. Subsequent state reimbursement of depositors resulted in costs of approximately 2.3 billion dollars. With the fraud-based collapse of Banco Mercantil and Banco Nacional de Credito (BANCREDITO) that same year, total bank fraud-based losses to the Dominican government approached $3 billion in 2003. These frauds gutted the Dominican economy, almost tripled national indebtedness, and caused a massive devaluation of the Dominican peso. The GODR negotiated an International Monetary Fund (IMF) standby loan in August 2003 to help cover the costs of the failures. The IMF insisted on extensive changes in laws and procedures to improve banking supervision. Though legislative changes have been made, full implementation of IMF requirements lags.

By the end of 2007, the prosecutor's investigations were essentially completed in the BANCREDITO case, although none of the convictions—which are currently under appeal—were for money laundering. Preparations for a case against Banco Mercantil officials have been hampered since February as the Supreme Court has not yet resolved related jurisdictional issues. In the BANINTER case, which concluded in November 2007, convictions and significant sentences were entered for bank president Ramon Baez Figueroa and bank vice-president Marcos Baez Coco for violation of banking and monetary laws, although both were acquitted of money laundering. Dominican economist and entrepreneur Luis Alvarez Renta, a U.S. citizen, was convicted of criminal money laundering in connection with the collapse and sentenced to ten years in prison. These convictions, criticized by civil society, the media, and jurists as internally inconsistent, are nevertheless a significant challenge to impunity for the country's elite. The convictions are currently under appeal.

Under Law No. 72-02 and Decree No. 288-1996, numerous financial and nonfinancial institutions are subject to anti-money laundering provisions. Obligated entities include banks, currency exchange houses, stockbrokers, securities brokers, the Central Bank, cashers of checks or other types of negotiable instruments, issuers/sellers/cashers of travelers checks or money orders, credit and debit card companies, remittance companies, offshore financial service providers, casinos, real estate agents, automobile dealerships, insurance companies, and certain commercial entities such as those dealing in firearms, metals, archeological artifacts, jewelry, boats, and airplanes. The law mandates that these entities must report suspicious transactions as well as all currency transactions exceeding U.S. $10,000, and maintain records for a minimum of five years. Moreover, the legislation requires individuals to declare cross-border movements of currency that are equal to or greater than the equivalent of U.S. $10,000 in domestic or foreign currency.

In 1997 the Unidad de Inteligencia Financiera (UIF) was established as the financial intelligence unit (FIU) of the Dominican Republic, with the responsibility of receiving financial disclosures and suspicious transaction reports (STRs) from reporting entities in the financial sector. In 2002, Law 72-02 created the Unidad de Análisis Financiero (Financial Analysis Unit, or UAF) that reports to the National Anti-Money Laundering Committee, and has the mandate to receive financial disclosures and STRs from both financial and nonfinancial reporting entities, as well as present leads to the prosecutors' office. According to the GODR, the UAF, which became operational in 2005, has replaced the UIF as the FIU of the Dominican Republic. As a result, the UIF, which became a member of the Egmont Group in 2000, lost its membership in November 2006 as it is no longer the legally recognized FIU of the Dominican Republic. The UAF anticipates applying for Egmont membership once a full transition of FIU functions and responsibilities are complete and the GODR has formally criminalized terrorist financing, as the criminalization of terrorist financing is now a requirement for all new members of the Egmont Group.

Although the UAF is now recognized as the GODR's financial intelligence unit, it appears that there is still confusion among obligated entities regarding their reporting requirements. In 2007, rather than reporting directly to the UAF, reporting entities filed 824 STRs with the UIF. The UIF then reported the STRs to the UAF. The majority of the reports the UAF received in 2007 are believed to have been transferred from the UIF.

Further confounding the duality of FIU functions in the Dominican Republic is the proposed creation of an offshore financial center with its own agency equivalent to an FIU. In 2006, legislation was introduced by the GODR to allow for the creation of an Independent Financial Center of the Americas (IFCA), which would not be subject to the regulatory authority of GODR banking supervisors. To reassure international concerns regarding the IFCA's susceptibility to abuse by money launderers and terrorist financiers, as well as the GODR's inability to ensure that the IFCA complies with anti-money laundering and counter-terrorist financing standards, the creators of the IFCA have proposed establishing their own FIU to report to the UAF and exchange information with other FIUs. However, an FIU must by definition be a single, national entity. Although proposed amendments to the draft legislation suggest changing the name of the IFCA's FIU-equivalent agency to avoid confusion, it would still serve as a filter for STRs that should be sent to the UAF, which is not permissible under the international standards of the Egmont Group and Financial Action Task Force.

Although terrorist financing is not a crime in the Dominican Republic, the GODR continues to support U.S. Government efforts to identify and block terrorist-related funds. While no assets have been identified or frozen, the GODR 's efforts to identify and block terrorist-related funds continue through orders and circulars issued by the Ministry of Finance and the Superintendence of Banks that instruct all financial institutions to continually monitor accounts. The GODR has not enacted specific legislation that would criminalize the financing of terrorism and provide reporting entities with a legal basis to carry out counter-terrorist financing prevention programs.

According to U.S. law enforcement officials, cooperation between law enforcement agencies on drug cases, human trafficking, and extradition matters remains strong. In 2007, GODR and U.S. law enforcement were able to work together to intercept and disrupt bulk cash smuggling organizations operating in the airports and seaports of the Dominican Republic. Law enforcement in the Dominican Republic is also actively targeting commercial flights and vessels that operate to drug source countries to disrupt the illicit money flow back to narcotics traffickers.

The United States continues to encourage the GODR to join a mutual legal assistance treaty with the Organization of American States (OAS) and sign related money laundering conventions. The Dominican Republic is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The Dominican Republic is a party to the1988 UN Drug Convention, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. The GODR has signed, but has not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism.

The GODR is enhancing its anti-money laundering regime; however, additional improvements are needed, particularly with regard to combating terrorist financing. Legislative and oversight provisions are being put in place in the formal financial sector, but there exists a lack of coordination among the various entities tasked with anti-money laundering activities. Weak implementation of anti-money laundering legislation leaves the Dominican Republic vulnerable to criminal financial activity. The Government of the Dominican Republic should enhance supervision of the nonfinancial sector, and ensure this sector's compliance with reporting requirements. The GODR should bolster the operational capacity of the fledgling UAF and ensure a full transition of FIU functions. Provisions should be put in place to ensure that the International Financial Center of the Americas is not susceptible to money laundering and terrorist financing activity, and the establishment of a FIU-equivalent within the IFCA should be prohibited. The GODR should formally criminalize the financing of terrorism and ratify the International Convention for the Suppression of the Financing of Terrorism.

Ecuador

With a dollar economy geographically situated between two major drug producing countries, Ecuador is highly vulnerable to money laundering, although it is not an important regional financial center. Because thus far only a few major banks have active money laundering controls in place, and because a large number of transactions take place through unregulated money exchange and remittance companies, there is no reliable way to judge the magnitude of such activity in the country. In addition to concerns about illicit transactions through financial institutions, there is evidence that money laundering is taking place through trade and commercial activity. Large amounts of unexplained currency entering and leaving Ecuador indicate that transit and laundering of illicit cash are also significant activities. Though smuggled goods are regularly brought into the country, there is no evidence that they are significantly funded by drug proceeds.

Ecuador's financial sector consists of 29 banks, 13 investment companies, two formal exchange houses, 28 cooperatives, 39 insurance companies, two stock exchanges, and eight mutual funds. Several Ecuadorian banks maintain offshore offices. The Superintendence of Banks and Insurance is responsible for oversight of both offshore and onshore financial institutions. Regulations are essentially the same for onshore and offshore banks, with the exception that offshore deposits no longer qualify for the government's deposit guarantee. Anonymous directors are not permitted. Licensing requirements are the same for offshore and onshore financial institutions. However, offshore banks are required to contract external auditors pre-qualified by the Superintendence of Banks. These private accounting firms perform the standard audits on offshore banks that would generally be undertaken by the Superintendence in Ecuador. Bearer shares are not permitted for banks or

companies in Ecuador. Small local credit unions are numerous and are regulated only by the Ministry of Social Affairs

Law 2005-13 of October 2005 criminalizes money laundering in Ecuador. The law criminalizes the laundering of illicit funds from any source and penalizes the undeclared entry of more than $10,000 in cash or other convertible assets. Prior to the passage of Law 2005-13, the Narcotics and Psychotropic Substance Act of 1990 (Law 108) criminalized money laundering activities only in connection with illicit drug trafficking. The new law criminalizes money laundering in relation to any illegal activity, including drug trafficking, trafficking in persons and prostitution. Money laundering is penalized by a prison term of one to nine years, depending upon the amount laundered, as well as a monetary fine. However, it is unclear if a conviction is required for the predicate offense to prosecute for money laundering, and money laundering is only considered to be a crime if the amount of funds laundered exceeds U.S. $5,000.

Law 2005-13 established the National Council Against Money Laundering, headed by the Procurador General (solicitor general) and includes representatives of all government entities involved in fighting money laundering, such as the Superintendence of Banks and the National Police. Law 2005-13 also establishes Ecuador's financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), under the purview of the Council. Regulations for application of the law and establishment of the FIU were published in April 2006 under Decree 1328. The first UIF director was appointed in November 2006 but quickly resigned. A second director was appointed in December 2006 and currently leads the UIF. During 2007, the UIF acquired office space, hired 17 personnel, and set up computer systems. The UIF became operational on December 1, 2007. In the month of December, the UIF received 61 suspicious transaction reports (STRs) from obligated entities, and referred 20 suspicious transactions to the judicial police and Attorney General's Office for review. Although now operational, the director is still seeking technical support and improved software to improve the analytical capacity of the unit.

All entities that fall under the 1994 Financial System Law, including banks, savings and credit institutions, investment companies, stock exchanges, mutual funds, exchange houses, credit card administrators, money transmitters, mortgage companies, insurance companies and reinsurance companies, are required to report all "unusual and unjustified" transactions to the UIF within 48 hours. Financial institutions under the supervision of the Superintendence of Banks and Insurance currently report suspicious transactions to the Superintendence. Obligated entities are also required to establish "know-your-client" provisions, report cash transactions over $10,000, and maintain financial transaction records for ten years. Any person entering Ecuador with $10,000 or more in cash must file a report with the customs service; however, this requirement is currently not being enforced. Entities or persons who fail to file the required reports or declarations may be sanctioned by the Superintendence of Banks. The UIF may request information from any of the obligated entities to assist in its analysis of suspicious transactions, and cases that are deemed to warrant further investigation will be sent to the Public Ministry. The UIF is also empowered to exchange information with other financial intelligence units on the basis of reciprocity.

Some existing laws may conflict with the detection and prosecution of money laundering. For example, the Bank Secrecy Law severely limits the information that can be released by a financial institution directly to the police as part of any investigation, and the Banking Procedures Law reserves information on private bank accounts to the Superintendence of Banks. In addition, the Criminal Defamation Law includes sanctions for banks and other financial institutions that provide information about accounts to police or advise the police of suspicious transactions if no criminal activity is ultimately proven. The law also does not provide safe harbor provisions for bank compliance officers.

Many of these obstacles can be overcome by a judge properly issuing an appropriate warrant. Also, the UIF is entitled by law to obtain information from the Superintendence of Banks and individual financial institutions, as an exception to the Banking Secrecy Law, and can provide this information to

the judicial police when part of an investigation. However, this contradictory legal framework may impede cooperation between other Government of Ecuador (GOE) agencies and the police, and cooperation to date has fallen short of the level needed for effective enforcement of money laundering statutes.

Ecuador's first major money laundering case began in August 2006 with the arrest of approximately a dozen alleged members of a Colombian money laundering operation and the seizure of a large number of assets in Ecuador. The suspects were linked to accused drug trafficker Hernan Prada Cortes, who had acquired many Ecuadorian businesses and real properties in the names of other persons since 2000, and was recently extradited to the United States from Colombia. Two of the ten individuals detained in 2006 were released due to insufficient evidence, while the other eight remain in detention and pending trial. The prosecution of this case has been delayed, in part, pending additional evidence that is expected from the Prada trial in the United States. There have been a total of three money laundering cases initiated by prosecutors since the passage of Law 2005-13, and no convictions to date.

Ecuador's legal system provides for asset forfeiture upon conviction; however, civil forfeiture is not permitted. The National Council Against Money Laundering is responsible for administering the freezing and seizure of funds that are identified as originating from illicit sources. A special fund for forfeited assets will be set up in the Central Bank, and these assets will be distributed among government entities responsible for combating money laundering. No statistics are available on the amount of assets seized or frozen by the GOE in 2007.

Terrorist financing has not been criminalized in Ecuador. The Ministry of Foreign Affairs, Superintendence of Banks and the Association of Private Banks formed a working group in December 2004 to draft a law against terrorist financing. In 2006, the draft law passed its first debate in Congress, but since then the draft has seen no revisions and is awaiting further debate. With the Congress in recess and the transition to a Constituent Assembly, there has been little opportunity to address the issue.

The Superintendence of Banks has cooperated with the U.S. Government in requesting financial institutions to report transactions involving known terrorists, as designated by the United States as Specially Designated Global Terrorists pursuant to Executive Order 13224, or as named on the consolidated list maintained by the United Nations 1267 Sanctions Committee. No terrorist finance assets have been identified to date in Ecuador. The Superintendence would have to obtain a court order to freeze or seize such assets, in the event they were identified in Ecuador. No steps have been taken to prevent the use of gold and precious metals to launder terrorist assets. Currently, there are no measures in place to prevent the misuse of charitable or nonprofit entities to finance terrorist activities.

Ecuador is a member of the Financial Action Task Force for South America (GAFISUD), and held the GAFISUD presidency in 2007. The GOE underwent a mutual evaluation by GAFISUD in September 2007, and the mutual evaluation report was accepted by the GAFISUD plenary in December 2007. The evaluation team found the GOE to be noncompliant or only partially compliant with 48 of the 49 Financial Action Task Force Recommendations on money laundering and terrorist financing. The mutual evaluation report noted the lack of a counter-terrorist financing law and the lack of successfully prosecuted money laundering cases, but recognized that the UIF is making some progress.

Ecuador is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. The GOE is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Ecuador and the United States are parties to a bilateral Agreement for the Prevention and Control of Narcotics Related Money Laundering that entered into

force in 1993 and a 1994 Agreement to Implement the United Nations Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances of December 1988, as it relates to the transfer of confiscated property, securities and instrumentalities. There is also a Financial Information Exchange Agreement (FIEA) between the GOE and the U.S. to share information on currency transactions. The UIF has signed memoranda of understanding with the FIUs of Argentina, Brazil, Bolivia, Chile, Colombia, Panama, and Peru for the exchange of information.

The Government of Ecuador has made progress in combating money laundering in recent years with the passage of anti-money laundering legislation and the establishment of an operational financial intelligence unit. However, the GOE should fully implement the existing legislation and ensure that reporting requirements are enforced. Ecuador is one of only two countries in South America that is not a member of the Egmont Group of FIUs, and the GOE should ensure that the UIF becomes fully functional and meets the standards of the Egmont Group and the Financial Action Task Force. Ecuador still needs to criminalize the financing of terrorism, which is a prerequisite for membership in the Egmont Group and is necessary to fully comply with international anti-money laundering and counter-terrorist financing standards. The GOE should address items that were not accounted for in its money laundering legislation, including the abolition of strict bank secrecy limitations and any potential sanctions for financial institutions that report suspicious transactions. The GOE should also amend its current legislation so that the laundering of funds under U.S. $5,000 is considered to be a money laundering offense, and clarify whether a conviction for a predicate offense is required before prosecutors may charge an individual with money laundering.

Egypt, The Arab Republic of

Egypt is not considered a regional financial center or a major hub for money laundering. Egypt still has a large informal cash economy, and many financial transactions do not enter the banking system. As part of its on-going economic reform plan, the Government of Egypt (GOE) continued financial sector reform in 2007. Few money laundering cases have made it to court in the last several years. Illegal dealings in antiquities, corruption, misappropriation of public funds, smuggling, and the use alternative remittance systems, such as hawala, increase Egypt's vulnerability to money laundering.

While there is no significant market for illicit or smuggled goods in Egypt, there is evidence that arms are being smuggled across Egypt's border with Gaza. The funding source is unclear, as is the destination of the proceeds. Other than arms smuggling, authorities say that the under-invoicing of imports and exports by Egyptian businessmen is still a relatively common practice. The primary goal for businessmen who engage in such activity is reportedly to avoid taxes and customs fees. Customs fraud and invoice manipulation are also found in regional value transfer schemes. The number of businesses and individuals filing tax returns as a result of June 2005 tax cuts continue to rise. Nevertheless, a large portion of Egyptian economy remains undocumented and tax evasion is commonplace

At present, money laundering and terrorist financing are officially reported as not widespread. The few cases of money laundering that have been detected involved laundering of money through the formal banking sector. However, informal remittance systems are widespread in Egypt, and are a potential means for laundering funds. Nevertheless, Egyptian authorities claim these systems do not operate in Egypt, and therefore make no effort to detect, monitor and regulate them. Due to lack of regulation and investigations, it is unclear if and to what extent money laundering is actually occurring through these systems. Expatriate Egyptian workers frequently use informal underground remittance systems due to cost and unfamiliarity with official banking procedures. Western Union and Moneygram, the two formal cash transfer operators in Egypt, are also widely used and managers have petitioned the Central Bank to expand their operations. The Central Bank has not yet approved the requests. Reports on the number of Egyptian expatriate workers are contradictory, but the figure generally stated is 5

million. The latest figures from the Central Bank indicate that overseas workers remitted U.S. $6.321 billion in fiscal year 2006-2007.

Egypt does not have a high prevalence of financial crimes, such as counterfeiting or bank fraud. There is no evidence that Egyptian financial institutions engage in currency transactions involving international narcotics-trafficking proceeds. The Anti-Money Laundering (AML) Law No. 80 of 2002 criminalizes laundering of funds from narcotics trafficking, prostitution and other immoral acts, terrorism, antiquities theft, arms dealing, organized crime, and numerous other activities. The law did not repeal Egypt's existing law on bank secrecy, but it did provide the legal justification for providing account information to responsible civil and criminal authorities. The law established the Egyptian Money Laundering Combating Unit (EMLCU) as Egypt's financial intelligence unit (FIU), which officially began operating on March 1, 2003, as an independent entity within the Central Bank. The administrative regulations of the EMLCU provide the legal basis by which the EMLCU derives its authority, spelled out the predicate crimes associated with money laundering, established a Council of Trustees to govern the EMLCU, defined the role of supervisory authorities and financial institutions, and allowed for the exchange of information with foreign competent authorities.

The Central Bank's Supervision Unit shares responsibility with the EMLCU for regulating banks and other financial institutions and ensuring compliance with AML law. Under the AML law, banks are required to keep all records for five years, and numbered or anonymous financial accounts are prohibited. The Central Bank also requires banks to maintain internal systems enabling them to comply with the AML law and has issued an instruction to banks requiring them to examine large transactions. In addition, banks are required to submit quarterly reports demonstrating compliance with AML regulations. Reporting of suspicious transactions is required by banks and nonbank financial institutions.

The Central Bank and EMLCU undertook frequent compliance assessments of all banks operating in Egypt. The assessments consisted of questionnaires and on-site visits to check AML compliance systems. Where deficiencies were found, banks were notified of corrective measures to be undertaken with a deadline for making the necessary changes and follow-up visits to reassess compliance. Sanctions for noncompliance include issuing a warning letter; imposing financial penalties; forbidding banks to undertake certain activities; replacing the board of directors; and revoking the bank's license. The Central Bank also monitors bureaux de change and money transmission companies for foreign exchange control purposes, giving special attention to those accounts with transactions above certain limits. The Capital Market Authority (CMA), which is responsible for regulating the securities markets, also conducts inspections of firms and independent brokers and dealers under its jurisdiction. Inspections are aimed at explaining and discussing AML regulations and obligations, as well as evaluating the implementation of systems and procedures, including checking for an internal procedures manual and ensuring the appointment of compliance officers.

In 2006, an independent insurance regulatory authority was established and charged with supervising insurance companies for compliance with AML laws and regulations. The General Authority for Free Zones and Investment (GAFI) regulates activity in free zones and Special Economic Zones (SEZ). The Ministry of Communication and Information Technology regulates the Postal Authority and the financial services it offers. Egypt allows gambling in casinos located in international hotels, but only foreigners are allowed to enter the casinos. All cash transactions at casinos are performed by licensed banks subject to AML controls. Individuals acting as financial intermediaries, such as lawyers, accountants, and cash couriers, are not currently subject to AML controls, although EMLCU officials have indicated that the law will soon be amended to cover the activities of these individuals. The AML law protects institutions and individuals who cooperate with law enforcement officials.

The executive regulations of the AML law lowered the threshold for declaring foreign currency at borders from the equivalent of U.S. $20,000 to U.S. $10,000. The declaration requirement was also

extended to travelers leaving as well as entering the country. However, enforcement of this provision is not consistent. The Customs Authority also signed an agreement with the EMLCU to share information on currency declarations. Authorities claim that the terrorist attacks of the past several years have given extra impetus to law enforcement agencies to thoroughly scrutinize currency imports/exports. As an example, there have been reports that Hamas ministers in the last Palestinian cabinet were crossing the Egypt-Gaza border with large amounts of cash. Egyptian Customs Authorities now pass all reports of foreign currency declarations at the border to the EMLCU and also alert the European Union border guards of individuals crossing the border with large amounts of cash.

Egypt is not an offshore financial center. Offshore banks, international business companies, and other forms of exempt or shell companies are not permitted in the country. Egypt has nine public free zones, 250 private free zones, and one SEZ. Public free zones are outside of Egypt's customs boundaries, so firms operating within them have significant freedom with regard to transactions and exchanges. The firms may be foreign or domestic, may operate in foreign currency, and are exempt from customs duties, taxes, and fees. Private free zones are usually limited to a single project such as mixing, repackaging, assembling and/or manufacturing for re-export. The SEZs allow firms operating in them to import capital equipment, raw materials, and intermediate goods duty-free and to operate tax-free. All banks and nonfinancial institutions operating in such zones are subject to Egypt's AML law provisions (AML).

The EMLCU, Egypt's FIU, is an independent entity within the Central Bank. The EMLCU has its own budget and staff and also has the full legal authority to examine and analyze all Suspicious Transaction Reports (STRs). Investigations are conducted by law enforcement agencies, including the Ministry of Interior, the National Security Agency, and the Administrative Control Authority. The EMLCU shares information with these agencies. The unit handles implementation of the AML law, which includes publishing the executive directives. The EMLCU takes its direction from a six-member council, the Council of Trustees, which is chaired by the Assistant Minister of Justice for Legislative Affairs. Other members of the Council include the Chairman of the CMA, the Deputy Governor of the Central Bank, a Sub-Minister (Under Secretary) from the Ministry of Social Solidarity, a representative from the Egyptian Banking Federation, and an expert in financial and banking affairs. In June 2004, the EMLCU was admitted to the Egmont Group of FIUs.

The Executive Director of the EMLCU is responsible for the operation of the FIU and the implementation of the policies drafted by the Council of Trustees. His responsibilities include: proposing procedures and rules to be observed by different entities involved in combating money laundering; presenting these rules and procedures to the Chairman of the Council of Trustees; reviewing the regulations issued by supervisory authorities for consistency with legal obligations and ensuring that they are up to date; ensuring the capability and readiness of the unit's database; exchanging information with supervisory entities abroad; acting as a point of contact within the GOE; preparing periodic and annual reports on the operational status of the unit; and taking necessary action on STRs recommended to be reported to the Office of Public Prosecution.

In 2002, the GOE passed the Law on Civil Associations and Establishments (Law No. 84 of 2002), which governs the procedures for establishing nongovernmental organizations (NGOs), including their internal regulations, activities, and financial records. The Law places restrictions on accepting foreign donations without prior permission from the proper authorities. Both the Ministry of Social Solidarity and the Central Bank continually monitor the operations of domestic NGOs and charities to prevent the funding of domestic and foreign terrorist groups.

Although the AML law does not specifically allow for seizure and confiscation of assets from money laundering, the Penal Code authorizes seizure of assets related to predicate crimes, including terrorism. All assets are subject to seizure, including moveable and immoveable property, rights and businesses. Assets can only be seized with an order from the Public Prosecutor, and the agency responsible for

seizing the assets depends on the predicate crime. Typically, the Central Bank seizes cash and the Ministry of Justice seizes real assets. Confiscated assets are given to the Ministry of Finance, and the executive regulations of the AML law allow for sharing of confiscated assets with other governments. The Public Prosecutor's office is currently engaged in negotiations to enhance cooperation with other governments on asset seizure and confiscation.

Because of its own historical problems with domestic terrorism, the GOE has sought closer international cooperation to counter terrorism and terrorist financing. The GOE has shown a willingness to cooperate with foreign authorities in criminal investigations, whether they are related to terrorism or narcotics.

In January 2005, the National Committee for Combating Money Laundering and Terrorist Financing was established to formulate general strategy and coordinate policy implementation among the various responsible agencies of the GOE. The committee includes representatives from the Ministries of Interior, Foreign Affairs, Social Affairs, Justice, and the National Security Agency, in addition to the EMCLU. The same agencies sit on a National Committee for International Cooperation in Combating Terrorism, which was established in 1998.

The GOE is in the process of replacing its original counter-terrorism law, an emergency law enacted in 1981 that is due to expire in spring of 2008, with a new comprehensive law. It will reportedly include specific measures against terrorist financing. Currently, article 86 of the Egyptian Penal Code criminalizes the financing of terrorism.

The United States and Egypt have a Mutual Legal Assistance Treaty. Egyptian authorities have cooperated with U.S. efforts to seek and freeze terrorist assets. Egypt also has agreements for cooperation on AML issues with the UK, Romania, Zimbabwe, and Peru. The Central Bank circulates to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. No related assets were identified, frozen, seized, or forfeited in 2007

Egypt is a founding member of the Middle East and North Africa Financial Action Task Force (MENAFATF) and follows that organization's recommendations on anti-money laundering and counter-terrorist financing. There is no information available on Egypt's mutual evaluation by MENAFATF. Egypt is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption.

The Government of Egypt will not have a successful anti-money laundering and terrorist finance regime until it has successful prosecutions and convictions. Improved investigative capacity in financial crimes is a prerequisite. Egypt should consider ways of improving the EMLCU's feedback on STRs to reporting institutions. It should improve its enforcement of cross-border currency controls, specifically allowing for seizure of suspicious cross-border currency transfers. Egyptian law enforcement and customs authorities should examine and investigate trade-based money laundering, informal value transfer systems, and customs fraud. The GOE should ensure that its updated law against terrorism specifically addresses the threat of terrorist financing, including asset identification, seizure and forfeiture.

El Salvador

Located on the Pacific coast of the Central American isthmus, El Salvador has one of the largest and most developed banking systems in Central America. Its most significant financial contacts are with neighboring Central American countries, as well as with the United States, Mexico, and the Dominican Republic. The growth of El Salvador's financial sector, the increase in narcotics

trafficking, the large volume of remittances through the formal financial sector and alternative remittance systems, and the use of the U.S. dollar as legal tender make El Salvador vulnerable to money laundering. In 2007, approximately $3.5 billion in remittances were sent to El Salvador through the financial system. Most were sent from Salvadorans working in the United States to family members. The quantity of additional remittances that flow back to El Salvador via other methods such as visiting relatives, regular mail and alternative remittance systems is not known.

Most money laundering is conducted by international criminal organizations. These organizations use bank and wire fund transfers from the United States to disguise criminal revenues as legitimate remittances to El Salvador. The false remittances are collected and transferred to other financial institutions until sufficiently laundered for use by the source of the criminal enterprise, usually a narcotics trafficking organization. One such case was investigated jointly by the Drug Enforcement Administration (DEA) and the Government of El Salvador (GOES) beginning in 2005. Two individuals were arrested. One Panamanian national was subsequently found guilty of money laundering in 2006, and a Salvadoran pled guilty in 2007. It is estimated that between U.S. $7 million and U.S. $11 million were laundered through local Western Union branch remittances.

Decree 498 of 1998, the "Law Against the Laundering of Money and Assets," criminalizes money laundering related to narcotics trafficking and other serious crimes, including trafficking in persons, kidnapping, extortion, illicit enrichment, embezzlement and contraband. The law also establishes the financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), within the Attorney General's Office. The UIF has been operational since January 2000. The National Civilian Police (PNC) and the Central Bank also have their own anti-money laundering units.

Under Decree 498, financial institutions must identify their customers, maintain records for a minimum of five years, train personnel in identification of money and asset laundering, establish internal auditing procedures, and report all suspicious transactions and transactions that exceed approximately U.S. $57,000 to the UIF. Entities obligated to comply with these requirements include banks, finance companies, exchange houses, stock exchanges and exchange brokers, commodity exchanges, insurance companies, credit card companies, casinos, dealers in precious metals and stones, real estate agents, travel agencies, the postal service, construction companies, and the hotel industry. The law includes a safe harbor provision to protect all persons who report transactions and cooperate with law enforcement authorities, and also contains banker negligence provisions that make individual bankers responsible for money laundering at their institutions. Bank secrecy laws do not apply to money laundering investigations.

In 2007, the GOES investigated 27 cases of suspected money laundering. GOES law enforcement arrested five individuals suspected of engaging in money laundering and financial crime, and prosecutors obtained convictions for four of those individuals in 2007. There were also two notable high-profile financial crime cases in 2007. In the first, a former National Legislative Assembly Deputy facing public corruption and money laundering charges fled to the United States and was later apprehended in Anaheim, California, and held on immigration charges. In the second high-profile case, a fugitive financier wanted on charges of defrauding Salvadoran investors in a case dating back to 2005 was arrested in Miami, Florida, and held pending resolution of a Salvadoran government extradition request.

The GOES has begun to more aggressively investigate private companies and financial service providers involved in suspicious financial activities. Despite demonstrating a greater commitment to pursue financial crimes, the GOES still lacks sufficient prosecutorial and police resources to adequately investigate and prosecute financial crimes. The GOES has established a secure computerized communication link between the Attorney General's office and the financial crimes division of the National Civilian Police. In addition to providing communication, the system has a software component that filters, sorts, and connects financial and other information vital to money

laundering investigations. The system, which became operational in 2006, is expected to enhance investigative capabilities. The UIF recently undertook an effort to establish a closer information sharing relationship with the Superintendent of the Salvadoran Financial System (SSF), as well as to formally incorporate the SSF into the existing secure computerized communication link.

To address the problem of international transportation of criminal proceeds, Decree 498 requires all incoming travelers to declare the value of goods, cash, or monetary instruments they are carrying in excess of approximately U.S. $11,400. Falsehood, omission, or inaccuracy on such a declaration is grounds for retention of the goods, cash, or monetary instruments, and the initiation of criminal proceedings. If, following the end of a 30-day period, the traveler has not proved the legal origin of said property, the Salvadoran authorities have the authority to confiscate the assets. In 2007, eight individuals were detected carrying undeclared cash at the international airport or at international border crossings, and a total of U.S. $1.2 million was confiscated from these individuals.

The GOES has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related and other assets of serious crimes. Forfeited money laundering proceeds are deposited in a special fund used to support law enforcement, drug treatment and prevention, and other related government programs, while funds forfeited as the result of other criminal activity are deposited into general government revenues. Law enforcement agencies are allowed to use certain seized assets while a final sentence is pending. In practice, however, forfeited funds are rarely channeled to counternarcotics operations. There exists no legal mechanism to share seized assets with other countries. Salvadoran law currently provides only for the judicial forfeiture of assets upon conviction, and not for civil or administrative forfeiture. A draft law to reform Decree 498 to provide for civil forfeiture of assets, currently in the national legislature, has run into resistance from businessmen and others who are fearful that a civil asset forfeiture regime could lead to a crackdown on tax evaders, or possibly be misused for political purposes. In 2007, the GOES froze U.S. $57,853 in bank deposits related to money laundering and financial crime investigations.

The GOES passed counterterrorism legislation, Decree No. 108, in September 2006. Decree No. 108 further defines acts of terrorism and establishes tougher penalties for the execution of those acts. Article 29 of Decree No. 108 establishes the financing of terrorism as a criminal offense, punishable by a prison term of 20 to 30 years and a monetary fine ranging from $100,000 to $500,000. The law also granted the GOES the legal authority to freeze and seize suspected assets associated with terrorists and terrorism. However, provisions to improve supervision of cash couriers, wire transfers, and financing of nongovernmental organizations (NGOs) that were included in an early draft were not included in the final law.

The GOES has circulated the names of suspected terrorists and terrorist organizations listed on the United Nations (UN) 1267 Sanctions Committee consolidated list to financial institutions. These institutions are required to search for any assets related to the individuals and entities on the consolidated list. There is no evidence that any charitable or nonprofit entity in El Salvador has been used as a conduit for terrorist financing.

El Salvador has signed several agreements of cooperation and understanding with financial supervisors from other countries to facilitate the exchange of supervisory information, including permitting on-site examinations of banks and trust companies operating in El Salvador. El Salvador is also a party to the Treaty of Mutual Legal Assistance in Criminal Matters signed by the Republics of Costa Rica, Honduras, Guatemala, Nicaragua, and Panama. Salvadoran law does not require the UIF to sign agreements to share or provide information to other countries. The GOES is party to the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, which provides for parties to cooperate in tracking and seizing assets. The UIF is also legally authorized to access the databases of public or private entities. The GOES has cooperated with foreign

governments in financial investigations related to narcotics, money laundering, terrorism, terrorist financing and other serious crimes.

El Salvador is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). The UIF has been a member of the Egmont Group since 2000. The GOES is party to the OAS Inter-American Convention against Terrorism, the UN International Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. El Salvador is also a signatory to the Central American Convention for the Prevention and Repression of Money Laundering Crimes Related to Illicit Drug Trafficking and Related Crimes.

The Government of El Salvador made advances in 2007 in terms of improvements in the operational capabilities of the UIF. To build upon this progress, however, El Salvador should continue to expand and enhance its anti-money laundering and counter-terrorist financing policies, and strengthen its ability to seize and share assets. The GOES should ensure the passage of the civil forfeiture legislation that is currently under consideration by the legislature. Remittances remain an important sector of the Salvadoran economy, and as such should be carefully supervised. The GOES should improve supervision of cash couriers and wire transfers as outlined in the Financial Action Task Force Nine Special Recommendations on terrorist financing. The GOES should also ensure that sufficient resources are provided to the overburdened Attorney General's office, as well as to the financial crime and narcotics divisions of the National Civilian Police.

France

France remains an attractive venue for money laundering because of its sizable economy, political stability, and sophisticated financial system. Narcotics trafficking, human trafficking, smuggling, and other crimes associated with organized crime are among its vulnerabilities.

The Government of France (GOF) first criminalized money laundering related to narcotics trafficking in 1987. Law 96-392 criminalizes the laundering of proceeds of all crimes. In 2004, the French Supreme Court ruled that joint prosecution of individuals was possible on both money laundering charges and the underlying predicate offense. Prior to this judgment, the money laundering charge and the predicate offense were considered the same offense and could only be prosecuted as one offense. French law has obliged institutions to combat money laundering since 1990. Entities obliged to file suspicious transaction reports (STRs) include those within a variety of financial and nonfinancial sectors, including banks, insurance companies, casinos, and lawyers.

Under Article 324 of the Penal Code, money laundering carries a penalty of five years imprisonment and a fine of 375,000 euros (approximately U.S. $547,500). With aggravating circumstances such as habitual or organized activity or connection with narcotics trafficking (Article 222-38), the penalty increases to ten years imprisonment and a fine of 750,000 euros (approximately U.S. $1,095,000). Legal procedure for criminal conspiracy applies to money laundering crimes.

As a member of the European Union (EU), France is obligated to implement all three EU money laundering directives. In late 2005, the EU adopted the Third Money Laundering Directive (2005/60/EC), which mandated an implementation deadline of December 15, 2007.

France has developed the Liaison Committee against the Laundering of the Proceeds of Crime, which is comprised of representatives from reporting professions and institutions, regulators, and law enforcement authorities. The Committee's purpose is to share information with regulated entities and to make proposals to improve the anti-money laundering (AML) system. The Justice Ministry and the French financial intelligence unit (FIU), known as the Unit for Treatment of Intelligence and Action Against Clandestine Financial Circuits or TRACFIN, co-chair this group.

The Banking Commission supervises fiduciary institutions and conducts regular audits of credit institutions. The Insurance and Provident Institutions Supervision Commission reviews insurance brokers. The Financial Market Authority monitors the reporting compliance of the stock exchange and other nonbank financial institutions. The Central Bank (Banque de France) oversees management of the records required to monitor banking transactions. Bank regulators and law enforcement can access the French Tax Administration's database to obtain information on the opening and closing of accounts. Information is available for depository accounts, transferable securities, and other properties, including cash assets. These records are important tools in the French arsenal for combating money laundering and terrorist financing.

France's FIU, TRACFIN, is responsible for analyzing suspicious transaction reports (STRs) filed by obliged entities. TRACFIN may exchange information with foreign counterparts that observe similar rules regarding reciprocity and confidentiality of information. TRACFIN works closely with the Ministry of Interior's Central Office for Major Financial Crimes (OCRGDF), which is the main point of contact for Interpol and Europol in France. TRACFIN can obtain information from senior police officers and central or local governments. The State Prosecutor informs the FIU of final court orders relating to suspicious transactions that have been reported.

TRACFIN received 12,047 STRs in 2006. The banking sector submits approximately 81 percent of STRs. The FIU referred 411 cases to the judicial authorities in 2006.

French law requires two types of reports, in addition to STRs, to be submitted to the FIU. An entity must file a report with TRACFIN when the identity of the principal or beneficiary remains unclear despite due diligence. There is no threshold limit for such reporting. Entities must also file reports when a financial entity acting in the form, or on behalf, of any asset management instrument, when legal or beneficial owners are unknown, carries out a transaction on a third party's behalf. The reporting obligation can also be extended by decree to transactions carried out by financial entities, on their own behalf or on behalf of third parties, with natural or legal persons, including their subsidiaries or establishments that are domiciled, registered, or established in any country or territory included on the Financial Action Task Force (FATF) list of noncooperative countries or territories.

Law No. 96-392 of 1996 instituted procedures for seizure and confiscation of the proceeds of crime. French law permits seizure of all or part of property. In cases of terrorist financing, France has promulgated an additional penalty of confiscation of the total assets of the terrorist offender. Authorities can freeze accounts and financial assets through both administrative and judicial measures.

Since 1986, French counter-terrorism legislation has provided for the prosecution of those involved in terrorist financing under the more severe offense of complicity in the act of terrorism. To strengthen this provision, France introduced several new characterizations of offenses, pointedly including terrorist financing. The offense of financing terrorist activities (Article 421-2-2 of the Penal Code) is defined according to the UN International Convention for the Suppression of the Financing of Terrorism and can result in ten years' imprisonment and a fine of 225,000 euros (approximately U.S. $328,500). Since 2001, TRACFIN has referred 92 cases of suspected terrorist financing to the judicial authorities for prosecution. TRACFIN participates in the "Cell for the fight against the financing of terrorism," an informal group created within the French Ministry of the Economy, Finance, and Industry to gather information to fight terrorist financing.

The Government of France (GOF) moved to strengthen France's anti-terrorism legal arsenal with the Act of 23 January 2006, authorizing video surveillance of public places, including nuclear and industrial sites, airports, and railway stations. The Act requires telephone operators and Internet café owners to keep extensive records, allows greater government access to e-communications, and opens flight passenger lists and identification information to access by counter-terrorism officials. The Act stiffens prison sentences for directing a terrorist enterprise to 30 years and extends the possible period of detention without charge. The Act permits increased surveillance of potential targets of terrorism. It

empowers the Minister of the Economy to freeze the funds, financial instruments and economic resources belonging to individuals committing or attempting to commit acts of terrorism, and belonging to companies directly or indirectly controlled by these individuals. By granting explicit national authority to freeze assets, the Act closes a potential loophole concerning the freezing of a citizen's assets as oppose to a resident EU-member citizen's assets. Adopted in January 2006, it entered into force by presidential decree in April 2007.

French authorities have moved rapidly to identify and freeze financial assets of organizations associated with Al-Qaida and the Taliban under United Nations Security Council Resolution 1267. France takes actions against other terrorist groups through the EU-wide "clearinghouse" procedure. Within the Group of Eight, France has sought to support and expand efforts targeting terrorist financing. France has worked to engage and improve the AML and counter-terrorist financing (CTF) capabilities of some African countries by offering technical assistance. On the operational level, French law enforcement cooperation targeting terrorist financing continues to be strong.

The United States and France entered into a mutual legal assistance treaty (MLAT) in 2001. Through MLAT requests and by other means, the French have provided large amounts of data to the United States in connection with terrorist financing. TRACFIN is a member of the Egmont Group and Egmont Committee and has information-sharing agreements with 30 foreign FIUs.

France is a member of the Financial Action Task Force (FATF). It is a Cooperating and Supporting Nation to the Caribbean Financial Action Task Force (CFATF) and an Observer to the Financial Action Task Force of South America (GAFISUD). France is a party to the 1988 UN Drug Convention; the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the UN Convention against Transnational Organized Crime; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention against Corruption.

The Government of France has established a comprehensive anti-money laundering regime and is an active partner in international efforts to control money laundering and the financing of terrorism. France should continue its active participation in international organizations, and its outreach to lower-capacity recipient countries, to combat the domestic and global threats of money laundering and terrorist financing. France should ensure that the promulgating regulations for compliance with the Third Money Laundering Directive are fully effective, and that the supervisory authorities are well-equipped to handle their new duties. The GOF should enact a compulsory written cash declaration regime at its airports to ensure that travelers entering and exiting France and the EU provide, in writing, a record of their conveyance of currency or monetary instruments that can be saved and shared.

Germany

Germany is one of the largest financial centers in Europe. Most of the money laundering that occurs in Germany relates to white-collar crime. Although not a major drug producing country, Germany continues to be a consumer and a major transit hub for narcotics. Organized criminal groups involved in drug trafficking and other illegal activities are an additional source of money laundering in Germany. Germany is not an offshore financial center.

In 2002, the Federal Republic of Germany (FRG) enacted a number of laws to improve law enforcement's ability to combat money laundering and terrorist financing. The measures brought German laws into line with the first and second European Union (EU) Money Laundering Directives, which mandate suspicious activity reporting by a variety of entities, including notaries, accountants, tax consultants, casinos, luxury item retailers, and attorneys.

In May 2002, the German banking, securities, and insurance industry regulators merged into a single financial sector regulator known as the Federal Financial Supervisory Authority (BaFIN). Germany's anti-money laundering (AML) legislation requires that BaFIN maintain a centralized register of all bank accounts with electronic access to all key account data held by banks in Germany. Banks cooperate with German authorities. Many have independently developed risk assessment software to screen potential and existing clients and their financial activity, and to monitor transactions for suspicious activity.

Germany's Money Laundering Act, amended by the Act on the Improvement of the Suppression of Money Laundering and Combating the Financing of Terrorism of August 8, 2002, criminalizes money laundering related to narcotics trafficking, fraud, forgery, embezzlement, and membership in a terrorist organization. It also increases due diligence and reporting requirements for banks and financial institutions and requires financial institutions to obtain customer identification for transactions conducted in cash or precious metals exceeding 15,000 euros (approximately U.S. $22,000). The legislation mandates more comprehensive background checks for owners of financial institutions and tighter rules for credit card companies. Banks must report suspected money laundering to the FIU as well as to the State Attorney (Staatsanwaltschaft).

The Federal Interior Ministry has drafted new legislation to implement the third EU Money Laundering Directive. The legislation is expected to be adopted in mid-2008. In addition to requiring that EU member states implement the Financial Action Task Force's (FATF) 40 Recommendations, the directive contains further provisions on customer due diligence and other internal risk-management measures to prevent money laundering and terrorist financing. The new regulations will apply to banks, insurance companies, and a number of professional groups (e.g., financial services providers, lawyers, notaries public, tax advisors, and other business operators). The directive calls for improved integrity and transparency to help prevent financial crime and improve information exchange between the public and private sectors. According to the draft legislation, suitable control structures must ensure that proper, accurate and current information is available about the contracting party, to ensure transparency. The EU requirement also expands reporting requirements to encompass transactions that support the financing of terrorism. The EU regulation on wire transfers (EC 1781/2006) entered into force on January 1, 2007.

As of June 15, 2007, travelers entering Germany from a nonEU country or traveling to a nonEU country with 10,000 euros (approximately U.S. $14,500) or more in cash must declare their cash in writing. The definition of "cash" includes currency, checks, traveler's checks, money orders, bills of exchange, promissory notes, shares, debentures, and due interest warrants (coupons). The written declaration must also include personal data, travel itinerary and means of transport as well as the total amount of money being transported, where the money originated from, what it is to be used for, who the owner of the money is and who is the payee. If authorities doubt the information given, or if there are other grounds to suspect money laundering or the funding of a terrorist organization, the cash will be placed under customs custody until the matter has been investigated. Penalties for nondeclaration or false declaration include a fine of up to one million euros (U.S. $1.46 million). During the period between January and September 2007 the Federal Customs Criminal Office identified 998 cases of individual cross-border cash movements that required further clarification and review. In December 2007 the new Schengen countries were enveloped within EU borders, making it possible to travel across Europe from Estonia through Germany to Portugal without border controls.

Germany established a single, centralized, federal financial intelligence unit (FIU) within the Federal Office of Criminal Investigation (Bundeskriminalamt or BKA). Staffed with financial market supervision, customs, and legal experts, the FIU is responsible for analyzing cases, responding to reports of suspicious transactions, and developing and maintaining a central database of this information. Another unit under the BKA, the Federal Financial Crimes Investigation Task Force, houses twenty BKA officers and customs agents.

Information for 2007 was unavailable, but in 2006, obligated entities filed 10,051 suspicious transaction reports (STRs) pursuant to the Money Laundering Act. According to the German Financial Intelligence Unit's (FIU's) 2006 annual report, 80 percent of the STRs filed pursuant to the Money Laundering Act and other notifications of money laundering activity forwarded to the FIU in 2006 cited fraud, including "phishing" and the use of "financial agents", as a possible criminal offense from the perspective of the reporting party. The individuals recruited in phishing schemes may be liable for money laundering penalties as well as for the illegal provision of financial services. Document forgery and tax offenses were the next most frequently cited offenses.

In 2006, approximately fifty-seven percent of the persons cited in German STRs were German nationals. Of the forty-three percent of the STRs that referenced nonGerman nationals, suspects with Turkish citizenship comprised the greatest proportion followed by Russian, Chinese, Italian and Kazakh. The 2006 statistics on STRs concerning transfers of assets to and from foreign countries displayed a number of significant trends. Russia and the Ukraine were the top two destinations for asset transfers that generated STRs. The United States is the eighth most frequently listed destination for asset transfers that are cited by STRs. When entities file STRs on transfers of assets from foreign countries, the USA is the most frequently cited source nation.

As with other crimes, actual enforcement of money laundering laws under the German federal system takes place at the state (sub-federal) level. Each state has a joint customs/police/financial investigations unit (GFG), which works closely with the federal FIU. The State Attorney can order a freeze of accounts when warranted.

As an EU member, Germany complies with a recent EU regulation requiring accurate originator information on funds transfers for transfers into or out of the EU. However, this does not place Germany into compliance with FATF Special Recommendation Seven (SR VII) on Terrorist Financing, which governs wire transfers. SR VII requires such information on all cross-border transfers, including transfers between EU member countries.

Germany moved quickly after September 11, 2001, to identify and correct the weaknesses in its laws that had permitted terrorists to live and study in Germany. One reform package closed loopholes that had permitted members of foreign terrorist organizations to engage in fundraising in Germany (e.g., through charitable organizations), which extremists had exploited to advocate violence. Subsequently, Germany increased its law enforcement efforts to prevent misuse of charitable entities. Germany has used its Vereingesetz, or Law on Associations, to take administrative action to ban extremist associations that "threaten the democratic constitutional order."

A second reform package enhances the capabilities of federal law enforcement agencies and improves the ability of intelligence and law enforcement authorities to coordinate efforts and to share information on suspected terrorists. The law also provides Germany's internal intelligence service with access to information from banks and financial institutions, postal service providers, airlines, and telecommunication and Internet service providers. Another proposed counterterrorism reform, will further streamline and simplify security agencies' access to German financial, travel, and telephone records. In 2002, the FRG also added terrorism and terrorist financing to its list of predicate offenses for money laundering, as defined by Section 261 of the Federal Criminal Code. The Criminal Code allows prosecution of members in terrorist organizations based outside Germany.

An amendment to the Banking Act institutes a broad legal basis for BaFIN to order frozen assets of EU residents suspected as terrorists. Authorities primarily concentrate on financial assets. BaFIN's system allows immediate identification of financial assets that can be potentially frozen, and German law enforcement authorities can freeze accounts for up to nine months. However, unless the assets belong to an individual or entity designated by the UNSCR 1267 Sanctions Committee, the FRG cannot seize money until authorities prove in court that the funds were derived from criminal activity or intended for terrorist activity.

Germany participates in United Nations and EU processes to monitor and freeze the assets of terrorists. The names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanctions Committee's consolidated list and those designated by EU or German authorities are regularly disseminated to German financial institutions. A court can order the freezing of nonfinancial assets. Germany and several other EU member states have taken the view that the EU Council Common Position requires, at a minimum, a criminal investigation to establish a sufficient legal basis for freezes under the EU Clearinghouse process. Proceeds from asset seizures and forfeitures go into the federal government treasury.

Since 1998, the FRG has licensed and supervised money transmitters, shut down thousands of unlicensed money remitters, and issued AML guidelines to the industry. German law considers the activities of alternative remittance systems such as hawala to be banking activities. Accordingly, German authorities require bank licenses for money transfer services, thus allowing authorities to prosecute unlicensed operations and maintain close surveillance over authorized transfer agents.

German law enforcement authorities cooperate closely at the EU level, such as through Europol. Germany has mutual legal assistance treaties (MLATs) with numerous countries. Germany exchanges law enforcement information with the United States through bilateral law enforcement agreements and informal mechanisms. United States and German authorities have conducted joint investigations. The U.S. and Germany signed a Mutual Legal Assistance Treaty in Criminal Matters on October 14, 2003. On July 27, 2006, the U.S. Senate ratified the MLAT and the German legislative bodies approved the implementing legislation in July and September 2007. Germany published the implementing legislation in the Federal Gazette on November 2, 2007, and the MLAT will come into effect once the parties formally exchange the instruments of ratification. Additionally, the U.S. and Germany signed bilateral instruments to implement the U.S.-EU Extradition and Mutual Legal Assistance Agreements on April 18, 2006. These instruments, as well as the underlying U.S.-EU Agreements, have not yet been ratified. German authorities cooperate with U.S. authorities to trace and seize assets to the full extent allowed under German laws. German law does not currently permit the sharing of forfeited assets with other countries.

Germany is a member of the FATF, the EU and the Council of Europe. The FIU is a member of the Egmont Group. Germany is party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Germany has signed, but not yet ratified, the UN Convention against Corruption.

The Government of Germany's AML laws and its ratification of international instruments underline Germany's continued efforts to combat money laundering and terrorist finance. Germany should amend its wire transfer legislation to ensure that origination information applies to all cross-border transfers, including those within the EU. It should also amend legislation to waive the asset freezing restrictions in the EU Clearinghouse for financial crime and terrorist financing, so that the freezing process does not require a criminal investigation as well as amend its legislation to allow asset sharing with other countries. Germany should ratify the UN Convention against Corruption.

Ghana

Ghana is not a regional financial center, but due to continuing turmoil in the region, Ghana's financial sector is likely to become more important regionally as it develops. Most of the money laundering found in Ghana involves narcotics and public corruption. Ghana is a significant transshipment point for cocaine and heroin. Police suspect that criminals use nonbank financial institutions, such as foreign exchange bureaus, to launder the proceeds of narcotics trafficking. Criminals can also launder their illicit proceeds through investment in banking, insurance, real estate, automotive import, and general import businesses. Reportedly, donations to religious institutions have been used as a vehicle to launder money. The number of "advance fee" or 419 fraud letters, known as Sakawa in Ghana, that

originate from Ghana continues to increase, as do other related financial crimes, such as use of stolen credit and ATM cards.

Informal activity accounts for about 45 percent of the total Ghanaian economy. Ghana's 2000 census found that 80 percent of employment was in the informal sector. Only a small percentage of the informal economy, however, relies on the banking sector. Because some traders smuggle goods to evade tax and import counterfeit goods, black market activity in smuggled goods is a concern. In most cases the smugglers bring the goods into the country in small quantities, and Ghanaian authorities have no indication that these smugglers have links to criminals who want to launder money gained through narcotics or corruption.

Ghana has designated four free trade zone areas, but the Tema Export Processing Zone is currently the only active free trade zone. Ghana also licenses factories outside the free zone area as free zone companies. Free zone companies must export at least 70 percent of their output. Most of the companies produce garment and processed foods. The Ghana Free Zone Board and the immigration and customs authorities monitor these companies. Immigration and customs officials do not suspect that trade-based money laundering (TBML) schemes are a major problem in the free trade zones. Although the Government of Ghana (GOG) has instituted identification requirements for companies, individuals, and their vehicles in the free zone, monitoring and due diligence procedures are lax.

The GOG has developed new laws to stimulate financial sector growth, including the revision of the banking law to strengthen the operational independence of the Central Bank (Bank of Ghana). The government is promoting efforts to model Ghana's financial system on that of the regional financial hub in Mauritius. In line with this, the GOG passed the Banking (Amendment) Act, 2007 Act 738, on June 18, 2007. The law establishes the basis for the provision of international financial services in Ghana and requires the Bank of Ghana to authorize offshore banks. Prior to this law, the Bank of Ghana licensed only reputable and internationally active banks. On September 7, 2007, Barclays Bank of Ghana Ltd., a subsidiary of Barclays Bank PLC, UK became the first to start operating as an offshore bank. The Bank of Ghana is in the process of drafting regulations for offshore banks.

Nearly six years after drafting began, the Parliament passed the Anti-Money Laundering (AML) Bill on November 2, 2007. The President signed it on January 22, 2008, and it was gazetted on January 25, 2008. The law covers obliged institutions and their reporting and disclosure requirements; the role of supervisory authorities; preventive measures; customer identification and record keeping requirements; and rules for suspicious transaction reporting. Ghana has bank secrecy laws, but allows the sharing of information with relevant law enforcement agencies. Law enforcement officials can compel disclosure of bank records for drug-related offenses. Bank officials have protection from liability when they cooperate with law enforcement investigations. The new AML law requires banks and individuals to report suspicious transactions.

The banking sector lacks a strong regulatory framework to prevent money laundering and report suspicious transactions, although entities recognize the importance of such a framework. The Bank of Ghana allows two types of foreign currency bank accounts: the foreign exchange (FE) account and the foreign currency (FC) account. The FE account is tailored to foreign currency sourced within Ghana while the FC account targets transfers from abroad. Bank of Ghana regulations instituted in December 2006 under the Foreign Exchange Act allow U.S. $10,000 per year to be transferred from an FE account without documentation and approval from the Bank of Ghana. The regulations also allow import transactions of up to $25,000 without initial documentation for FE accounts. There are no limits on the number of such transactions made on each account or on the number of such accounts that an individual can hold. The law does not permit foreign exchange bureaus to make outward transfers. Local banks strictly follow "know your customer" rules. Ghana has no effective system to obtain data on an individual's dealings with all the banks in Ghana.

Ghana has a cross-border currency reporting requirement. However, Ghanaian authorities have difficulty monitoring cross-border movement of currency.

The new AML bill calls for establishment of a Financial Intelligence Unit (FIU), overseen by the Minister of Finance. Ghana plans to fund the FIU through government grants and donations. The FIU will not investigate crime but will gather and analyze intelligence to help in identifying proceeds of unlawful activity and the perpetrators of the crimes. The FIU will have the authority to obtain information from other government regulatory authorities and from financial institutions. The GOG made no arrests, nor did it pursue any prosecutions related to money laundering or terrorist finance in 2007.

The Narcotic Drug Law of 1990 provides for the forfeiture of assets upon conviction of a drug trafficking offense. A February 2007 court order compelled authorities to release seized assets in a 1991 landmark narcotics trafficking case which resulted in a ten-year jail sentence of the convict, and return the assets to the owners. The ex-convict had appealed the seizure, arguing that the assets did not belong to him. The draft Proceeds of Crime Bill, pending since 2006, contains provisions dealing with pre-emptive measures, confiscation and pecuniary penalty orders, search and seizure, and restraining orders and realization of property. The draft Proceeds of Crime bill will merge with the existing Serious Fraud Office Law, 1993 (Act 466). The Serious Fraud Office, established by this law, investigates corruption and crimes that have the potential to cause economic loss to the state.

Ghana has not yet criminalized the financing of terrorism, as required by United Nations Security Council Resolution 1373. A draft Anti-Terrorism Bill, incorporating terrorist financing provisions, came before Parliament in 2005. The Bill is under examination by members of the Constitutional, Legal, and Parliamentary Affairs Committee and the Defense and Interior Committee. The draft bill addresses terrorist acts, support for terrorist offenses, specific entities associated with acts of terrorism, and search, seizure, and forfeiture of property relating to acts of terrorism. The Central Bank has circulated the list of individuals and entities on the UNSCR 1267 Sanctions Committee's consolidated list to local banks, but no Ghanaian entities have identified assets belonging to any of the designees.

Although current Ghanaian law does not allow for the sharing of seized narcotics assets with other governments, the Narcotic Drug Law of 1990 includes provisions for the sharing of information, documents, and records with other governments. It also provides for extradition between Ghana and foreign countries for drug-related offenses. The United States has not requested financial investigative assistance from Ghanaian authorities.

Ghana is a member of the Inter-Governmental Action Group Against Money Laundering and Terrorist Financing in West Africa (GIABA), a regional body modeled after the Financial Action Task Force (FATF). Ghana has bilateral agreements for the exchange of money laundering-related information with the United Kingdom, Germany, Brazil, and Italy. Ghana is a party to the twelve UN conventions on terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism. Ghana is a party to the 1988 UN Drug Convention, and the African Union Convention on Preventing and Combating Corruption. In June 2007, Ghana ratified the UN Convention against Corruption. Ghana has not signed the UN Convention against Transnational Organized Crime. Ghana has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision."

Although the Government of Ghana (GOG) became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002, it has not criminalized terrorist financing. It should do so. The GOG should move swiftly to implement the AML Bill, and should expand the list of predicate crimes to comply with international standards. The GOG should issue promulgating regulations, improve capacity among the agencies impacted, and establish its FIU. The GOG should make every effort to pass asset seizure and forfeiture legislation that comports with international standards as soon as possible. Once the laws are in place, Ghana should take the necessary steps to promote public awareness and understanding of financial crime, money laundering and financing of

terrorist activities. The GOG should reconsider establishing the offshore center altogether. Ghana should immediately release regulations and guidance for its new offshore entities, and draft legislation to ensure that offshore entities are treated identically to the onshore sector under the AML Bill. Additionally, the GOG should require that the true names of all offshore entities are held in a registry, accessible to law enforcement. The GOG should increase cooperation and information sharing with other governments. Ghana should also become a party to the UN Convention against Transnational Organized Crime.

Gibraltar

Gibraltar is an overseas territory of the United Kingdom. A November 2006 referendum resulted in constitutional reforms transferring powers exercised by the U.K. government to Gibraltar. Gibraltar is a significant international financial center with strong ties to London, the Channel Islands, Israel, Cyprus, and other financial centers. Located at the southern tip of Spain, near the north coast of Africa, Gibraltar is adjacent to known drug-trafficking and human smuggling routes. It is also a retail banking centre for northern European expatriates with property in southern Spain. All of these factors reportedly contribute to money laundering and terrorist financing vulnerabilities in Gibraltar.

Gibraltar was one of the first jurisdictions to introduce and implement money laundering legislation that covered all crimes. The Gibraltar Criminal Justice Ordinance to Combat Money Laundering, which related to all crimes, entered into effect in 1996. The Drug Offenses Ordinance (DOO) of 1995 and Criminal Justice Ordinance of 1995, amended in June 2007 as the Criminal Justice Act, criminalize money laundering related to all crimes. The laws mandate reporting of suspicious transactions by any obliged entity or individual therein. The DOO obliges banks, mutual savings companies, insurance companies, financial consultants, postal services, exchange bureaus, attorneys, accountants, financial regulatory agencies, unions, casinos, charities, lotteries, car dealerships, yacht brokers, company formation agents, dealers in gold bullion, and political parties.

Authorities issued comprehensive anti-money laundering (AML) Guidance Notes, which have the force of law, to clarify the obligations of Gibraltar's financial service providers. Gibraltar issued its most recent Guidance Notes in December 2007 with amendments based on the Criminal Justice (Amendment) Act 2007 and Terrorist (Amendment) Act 2007. The 2007 Guidance Notes apply to banks and building societies, the Gibraltar Saving Bank, investment business and controlled activities, life insurance companies, currency exchangers/bureaux de change, and money transmission/remittance offices. In transposing the EU's Third Money Laundering Directive to include nonfinancial sectors, Gibraltar extended the Criminal Justice Act.

Gibraltar established the Financial Services Commission (FSC), the unified regulatory and supervisory authority for financial services, under the FSC Ordinance (FSCO) 1989. Required by statute to match the supervisory standards of the United Kingdom, the FSC is the supervisory body for banks and building societies, investment businesses, insurance companies, and controlled activities, which include investment services, company management, professional trusteeship, insurance management and insurance intermediation. The main legal instruments governing the regulation and supervision of the financial system, in addition to the FSCO, are: the Banking Ordinance (1992) that provides powers to license and supervise banking and other deposit-taking business in Gibraltar; the Insurance Ordinance (1987) that provides powers to regulate and restrict the conduct of the business of insurance; and the Financial Services (Collective Investment Schemes) Ordinance that provide for the licensing and supervision of investment business.

Legislation requires that all businesses establish the beneficial owner of any companies or assets before undertaking a relationship or incorporating any company or asset. Onshore and offshore banks are subject to the same legal and supervisory requirements. Institutions must retain financial records for at least five years from the date of completion of the business. If the obligated institution has

submitted a suspicious transaction report (STR) to the Gibraltar financial intelligence unit (FIU) or when it knows that a client or transaction is under investigation, it is required to maintain any relevant record even if the five year interval has expired. If a law enforcement agency investigating a money laundering case cannot link the funds passing through the financial system with the original criminal money, then the funds cannot be confiscated.

The Financial Services Commission Act 2007 (FSCA) became effective in May 2007. This act repeals and replaces the Financial Services Commission Act of 1989. With this legislation, the FSC modernized and restructured itself. One of the most significant changes arising from the FSCA is in respect to the appointment of members of the Commission, who will be selected by the minister with responsibility for financial services (presently the Chief Minister) from a short list of three suitable persons provided to him by existing members. The FSC has also received expanded statutory functions. The FSC now holds formal licensing, supervisory, and regulatory powers over all firms authorized under the Supervisory Acts. The FSC authority also ensures compliance with legislation, rules and guidance notes in general as well as those specific to combating financial crime. The FSC is now able to issue Rules and Guidance, which enables the FSC to draft practical guidance for compliance with legislative measures, and regulatory expectations to supplement legislative provisions. As a safeguard against inappropriate or overregulation, the rules and guidance undergo a public consultation process and are subject to final veto of the Minister.

The Government of Gibraltar (GOG) permits Internet gaming that is subject to a licensing regime. Gibraltar has guidelines for correspondent banking, politically exposed persons (PEPs), bearer securities, and "know your customer" (KYC) procedures. In 2006, Gibraltar underwent a mutual evaluation by the International Monetary Fund (IMF). The IMF rated Gibraltar "largely compliant" or "better" with 32 of the Financial Action Task Force's (FATF's) 40 Recommendations and nine Special Recommendations.

In 1996, Gibraltar established the Gibraltar Coordinating Center for Criminal Intelligence and Drugs (GCID) to receive, analyze, and disseminate financial information and disclosures filed by obliged institutions. The GCID serves as Gibraltar's FIU (GFIU) and is a sub-unit of the Gibraltar Criminal Intelligence Department. The GCID consists mainly of police and customs officers but is independent of law enforcement. The GFIU has responded to over 40 international requests for information and has initiated ten requests to counterpart FIUs. The GFIU receives approximately 100 STRs per year.

Gibraltar's 2001 Terrorism (United Nations Measures) (Overseas Territories) Order criminalizes the financing of terrorism. The Order requires banks to report any knowledge that a present, past or potential client or customer is a terrorist, or receives funds in relation to terrorism, or makes funds available for terrorism. Gibraltar also addresses terrorist financing through the Terrorism Ordinance (2005).

Application of the 1988 U.S.-UK Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking was extended to Gibraltar in 1992. The DOO of 1995 provides for mutual legal assistance with foreign jurisdictions on matters related to narcotics trafficking and related proceeds. Gibraltar has passed legislation to update mutual legal assistance arrangements with its EU and Council of Europe partners. Gibraltar is a member of the Offshore Group of Banking Supervisors (OGBS) and the International Organization of Securities Commissions (IOSC). The GFIU is a member of the Egmont Group. The GOG has implemented the 1988 UN Drug Convention.

The Government of Gibraltar should continue its efforts to implement a comprehensive anti-money laundering and counter-terrorist financing (AML/CTF) regime. The criminal laws on money laundering should be consolidated, and powers presently available only in drug-related money laundering cases should be extended to money laundering cases involving the proceeds of other crimes. The GOG should introduce legislative provisions to its asset seizure and confiscation regime

allowing authorities to confiscate assets, including cash, even without a link to the original criminal proceeds. Gibraltar needs to conduct risk assessment of those designated nonfinancial businesses and professions that are unsupervised and determine and extend the necessary authority to conduct AML/CTF compliance examinations of these entities.

Greece

Greece is becoming a regional financial center in the rapidly developing Balkans as well as a bridge between Europe and the Middle East Anecdotal evidence of illicit transactions suggests an increase in financial crimes in the past two years. Greek law enforcement proceedings indicate that Greece is vulnerable to narcotics trafficking, trafficking in persons and illegal immigration, prostitution, cigarette, and other forms of smuggling, large scale tax evasion, serious fraud or theft, and illicit gambling activities. The widespread use of cash facilitates a gray economy and tax evasion. Due to the gray economy, it is difficult to determine the amount of smuggled goods in the country. Crimes are often carried out by criminal organizations from Southeastern Europe and the Balkans.

U.S. law enforcement agencies believe that criminally derived proceeds are not typically laundered through the Greek banking system. Instead, they are most commonly invested in real estate, the lottery, and a growing stock market. U.S. law enforcement agencies also believe Greece's geographic location has led to a moderate increase in cross-border movements of illicit currency and monetary instruments due to the increasing interconnection of financial services companies operating in Southeastern Europe and the Balkans. Reportedly, currency transactions involving international narcotics-trafficking proceeds do not appear to include significant amounts of U.S. currency.

The June 2007 Financial Action Task Force (FATF) mutual evaluation report (MER) of Greece found its legal requirements in place to combat money laundering and terrorist financing generally inadequate to meet the FATF standards. The report articulated concerns about the overall effectiveness of the AML/CTF system, including inadequate customer identification preventative systems, lack of adequate legal systems to prevent money laundering and terrorist financing, and a lack of adequate preventive measures and regulatory oversight. Of the FATF 40 Recommendations and Nine Special Recommendations on Terrorist Financing, Greece received 12 ratings of "largely compliant" or better and 13 ratings of "noncompliant." Of the 5 core FATF recommendations (Recommendations 1, 5, 10, and 13, SR II and IV), Greece's Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) regime was only deemed "partially compliant".

The Government of Greece has criminalized money laundering through a series of laws that have expanded the list of predicate offenses for money laundering that now includes terrorist financing, trafficking in persons, electronic fraud, and stock market manipulation. However evidence indicates that the ML provisions have not been effectively implemented. The laws also empower supervisory authorities to block transactions when money laundering is suspected and authorizes the financial intelligence unit (FIU) director to temporarily freeze assets without a court order. With its Act 25779/2006, the Bank of Greece has applied the main provisions of the Third European Union (EU) Money Laundering Directive to all financial institutions. The Greek government anticipates it will take steps to formally transpose the Directive into national law in 2008.

The Bank of Greece (BOG), through its Banking Supervision Department and the Ministry of National Economy and Finance, through its Capital Market Commission, supervise and monitor credit and financial institutions. Both the BOG and the Hellenic Capital Markets Commission (HCMC) have extensive supervisory programs. Each entity has internal departments focused on AML/CTF staffed with auditors and examiners. Supervision includes the issuance of guidelines and circulars, and on-site audits with a component assessing compliance with AML legislation. The Central Bank conducts on-site examinations for banks located in Greece as well as of Greek banks located in the Balkans. The HCMC conducts on-site examinations on a routine basis for its supervised entities and off-cycle

examinations of supervised entities when HCMC internal surveillance activities uncover possible noncompliance with regulations. In addition to their supervisory programs, both the BOG and HCMC conduct continuing education seminars for stakeholders inside and outside of the financial industry, to further heighten awareness of AML/CTF. While the BOG and HCMC have been granted sufficient powers and authorities to monitor financial institutions for AML/CTF requirements, according to the MER, these organizations may not be able to effectively carry out their supervisory functions due to a lack of resources.

Supervised institutions must send to their competent authority a description of the internal control and communications procedures they have implemented to prevent money laundering. In addition, banks must undergo internal audits. Bureaux de Change must send the BOG a monthly report on their daily purchases and sales of foreign currency. Infrequent audits of such companies also occur. However, there is reportedly weak implementation of regulatory requirements documenting the flow of large sums of cash through financial and other institutions.

Law 3148 incorporates EU directives regarding the operation of credit institutions and the operation and supervision of electronic transfers. Under this legislation, the BOG has direct scrutiny and control over transactions by credit institutions and entities involved in providing services for funds transfers. The BOG issues operating licenses after assessing the institutions, their management, and their capacity to ensure the transparency of transactions. The Ministry of Development, through its Directorate of Insurance Companies, supervises the insurance sector, but supervisory authority will soon shift to the Hellenic Private Insurance Supervisory Committee. The Directorate of Insurance Companies has not established a regulatory authority.

Under Decree 2181/93, banks in Greece must demand customer identification information when a customer opens an account or conducts transactions exceeding 15,000 euros (approximately U.S. $22,000). If there is suspicion of illegal activities, banks may take measures to gather more information on the identification of the person involved in the transaction, but, reportedly, do not normally do so. The BOG has taken steps to change this. Newly enacted legislation now requires banks to obtain specific documents from both natural and legal persons. Furthermore, credit institutions are now required to obtain identification documents in money changing transactions exceeding 500 euros (U.S. $735). The law requires that banks and financial institutions maintain adequate records and supporting documents for at least five years after ending a relationship with a customer, or, in the case of occasional transactions, for five years after the date of the transaction. According to the MER, customer due diligence (CDD) and other preventative measures lack both sufficient requirements on collecting beneficial ownership information and adequate measures relating to ongoing CDD requirements on existing clients and account holders.

Current AML laws do not adequately prevent anonymous accounts or accounts in fictitious names. Greek law does not prohibit financial institutions from engaging in business with foreign financial institutions that allow their accounts to be used by shell companies.

Both banks and nonbank financial institutions must report suspicious transactions, though in practice, the latter rarely do so. The law requires every financial institution to appoint a compliance officer to whom all other branches or other officers must report suspicious transactions. Reporting obligations also apply to government employees involved in auditing, including employees of the BOG, the Ministry of Economy and Finance, and the Capital Markets Commission. Those who report individuals must furnish all relevant information to the prosecuting authorities. In 2007, the FIU formalized the standard information required on the suspicious transaction reports (STRs), so that the information provided on the form is consistent. Safe harbor provisions in Greek law protect individuals reporting violations of AML laws and statutes.

Greece has adopted banker negligence laws under which individual bankers face liability if their institutions launder money. Authorities levy “fines” on banks and credit institutions if they breach

their obligations to report instances of money laundering, and bank officers can receive fines and a prison term of up to two years. In 2007, the BOG "fined" approximately 14 institutions for failure to supervise general compliance regulations. The fines totaled approximately 20 million euros (approximately U.S. $30 million). The credit institution deposits the "fines" with the Central Bank in a separate, interest free account. After a designated period of time, the Central Bank returns the money to the credit institution. In 2007, the HCMC "fined" two supervised entities for failure to supervise in relation to AML/CTF regulations. The "fines" ranged from 5,000 to 10,000 euros (U.S. $7,350-$14,700). Some believe this sanction is not sufficiently prohibitive.

Law 2331/1995 established the Competent Committee (CC), which functions as Greece's FIU. Law 3424 makes the CC a statutorily independent authority with access to public and private files and removes tax confidentiality restrictions. The law also broadens the CC's authority with respect to evaluating information it receives from various organizations. The CC has, on paper, broad authority; however the FATF MER raised concerns about the CC, including its current structure, insufficient staff and technical resources to properly perform its tasks and functions and inadequate security measures to effectively protect information. A senior retired judge chairs the CC, which includes eleven senior representatives from the BOG, various government ministries and law enforcement agencies, the Hellenic Bankers Association, and the securities commission. The CC employs few or no financial analysts or experienced specialized AML/CTF personnel, and is significantly understaffed.

The CC has responsibility for receiving and processing all STRs, of which it receives approximately 1,000 per year. Although the CC recently established a database to track STR submissions, it still lacks other elements of a technology-savvy modern organization. STRs are hand delivered to the CC, where, upon receipt, the committee (comprised of only senior officials) reviews the STRs to determine whether further investigation is necessary. If the committee seeks more information from the reporting institution, the CC mails its questions to the institution. When it receives the reply, the committee reviews the file again to determine whether the report warrants further investigation. When the CC considers an STR to warrant further investigation, it forwards the case to the Special Control Service (YPEE), which functions as the CC's investigative arm.

The YPEE is under the direct supervision of the Ministry of Economy and Finance and has formal investigative authority over cases that, broadly defined, involve smuggling and high-worth tax evasion. The CC is responsible for preparing money laundering cases on behalf of the Public Prosecutor's Office and the YPEE has its own in-house prosecutor to facilitate confidentiality and speed of action. The director of the FIU can temporarily freeze funds.

Although the CC has the authority to impose heavy penalties on those who fail to report suspicious transactions, it has not done so. Reportedly, staff limitations have hampered effective communication with Greece's broader financial community, as well as with its international counterparts. The lack of adequate personal and fiscal resources and political support for its mission limits its effectiveness.

Authorities do not frequently prosecute money laundering cases independent of a predicate crime, and according to the MER, limited data indicates a low rate of convictions on ML prosecutions. . There are no prosecutors specifically assigned to prosecute financial crimes and all prosecutors carry a very large caseload. Furthermore, the Greek judicial system has only one court handling all judicial activity related to money laundering and terrorist financing. Greek authorities do not have an effective information technology (IT) system in place to track money laundering prosecution statistics. Despite requests by the CC and Greek Bar Association to do so, the Ministry of Justice has yet to compile statistics related to arrests or prosecutions for money laundering or terrorist financing offenses.

The Government of Greece does not provide guidance to institutions on freezing assets without delay and does not monitor compliance with requests. Furthermore, there are no sanctions for failure to follow freezing requests. The current process for notifying ministries and the financial sector to freeze or confiscate funds is lengthy. Therefore, these entities are unable to comply with requests to freeze

assets without delay. Greek law allows for the seizure of assets upon conviction for a money laundering offense with a jail term of three years or greater. The director of the CC can temporarily freeze assets, but must prepare a report and forward it to an investigating magistrate and prosecutor, who conduct further investigation and who, upon conclusion of the investigation, can issue a freezing order, pending the outcome of the criminal case. The YPEE has established a mechanism for identifying, tracing, freezing, seizing, and forfeiting assets of narcotics-related and other serious crimes, the proceeds of which are turned over to the government. YPEE investigators have authorization to immediately seize property pending court review and seize property purchased with proceeds of narcotics trafficking or used to facilitate narcotics trafficking. However, official forfeiture requires a court order. If the basis for the forfeiture is facilitation proceeds, the Government of Greece need not prove that the property was purchased with narcotics-related proceeds. It must only demonstrate that it was used in furtherance of narcotics trafficking. Even legitimate businesses can be seized if they have laundered narcotics money.

Greek authorities maintain that Greece is not an offshore financial center. However, Greek law 89/1967 provides for the establishment of offshore entities of any legal form which may be registered in Greece but engage exclusively in commercial activities outside of Greece—a typical identifying restriction of offshore centers. “Law 89” companies reportedly operate in the shipping industry and are known for their complex corporate and ownership structures which are frequently designed to hide the the identity of the true beneficial owners of the companies.

Offshore entities must provide a bank letter of guarantee for U.S. $50,000 to the Ministry of Economy and Finance. If it is a shipping company, it must cover its annual operating expenses in Greece. It must keep a receipts and expenses book, though it has no obligation to publish any financial statements. These firms fall under the authority of nonGreek jurisdictions and often operate through a large number of intermediaries. As such, these entities can serve as a catalyst for money laundering. Although Greek law allows banking authorities to check these companies’ transactions, other Greek jurisdictions must work with the banking authorities for audits to be effective. There is no separate regulatory authority for the offshore sector and there is no longer a tax exemption for offshore companies.

Greek law does not provide for nominee directors or trustees in Greek companies. Although the government has abolished bearer shares for banks and a limited number of other companies, most companies may still issue bearer shares. The information available in the Companies Registries maintained by several authorities relates solely to the Board of Directors at the time of the incorporation of the company and does not log changes of directors, or the true beneficial owners of the company. Rather, regional registries keep this information in a paper format.

Authorities have recently targeted the gaming industry to restrain money launderers from using Greece’s nine casinos to launder illicit funds, however there is little regulatory oversight of the gaming industry. Greece has three free trade zones, located at the ports of Piraeus, Thessalonica, and Heraklion, where foreign goods may be brought in without payment of customs duties or other taxes if they are subsequently transshipped or re-exported. There is no specific information regarding whether these zones are being used in trade-based money laundering (TBML) or in the financing of terrorism

The BOG maintains that alternative remittance systems do not exist in Greece and has no plans to introduce initiatives for their regulation. Foundations in Greece are self-governing, nonmembership organizations with an endowment that serves public or private purposes and which receive legal capacity by state approval. Types of foundations include private law foundations, public benefit foundations, public foundations, and nonautonomous foundations. Nonprofit organizations fall within the purview of YPEE. The Greek government does not view charitable organizations as vulnerable to terrorist financing or money laundering and does not actively monitor such entities for these crimes.

Laws criminalizing terrorism, organized crime, money laundering and corruption have been in effect since July 2002. In 2004, Law 3251 was enacted criminalizing the financing of, the joining, or the forming of a terrorist group with a penalty of up to ten years imprisonment. If a private legal entity is implicated in terrorist financing, it faces fines of between 20,000 and 3 million euros (approximately U.S. $44,000 and U.S. $4.5 million), closure for a period of two months to two years, and ineligibility for state subsidies. However, some have described the law as poorly drafted. The law is not comprehensive as it is not illegal in Greece to fund an already established terrorist group and it is only considered a terrorist financing crime if a person funds a specific attack executed by three or more people. As a consequence, the financing of an individual terrorist act conducted by an individual terrorist or the financing of an individual terrorist is not an offense.

The BOG has circulated to all financial institutions under its supervisory jurisdiction the list of individuals and entities on the United Nations Security Council Resolution (UNSCR) 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Laden, the Al-Qaida organization, or the Taliban, as well as the EU's list of designees. The BOG now includes Office of Foreign Asset Control lists for circulation to its supervised entities. The Greek government does not routinely circulate lists disseminated by the U.S. government, but it does circulate EU lists. In most instances, there must be an active investigation by Greek authorities before the Government of Greece can seize assets, thus hindering its ability to freeze assets without delay. The government has not found any accounts belonging to anyone on the circulated lists.

Greece is a member of the FATF. Its FIU is a member of the Egmont Group. The government is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Greece is a signatory to the UN Convention against Transnational Organized Crime and to the UN Convention against Corruption, but has not yet ratified them. Greece exchanges information on money laundering through its mutual legal assistance treaty (MLAT) with the United States, which entered into force November 20, 2001. The Bilateral Police Cooperation Protocol provides a mechanism for exchanging records with U.S. authorities in connection with investigations and proceedings related to narcotics trafficking, terrorism, and terrorist financing. Cooperation between the U.S. Drug Enforcement Administration and YPEE has been extensive. Greece has signed bilateral police cooperation agreements with twenty countries, including the United States. It also has a trilateral police cooperation agreement with Bulgaria and Romania, and a bilateral agreement with Ukraine to combat terrorism, drug trafficking, organized crime, and other criminal activities. Despite the existing mechanisms for information exchange, the FATF report highlighted a lack of cooperation between Greek national and international authorities.

To meet its stated goal of effectively addressing money laundering, the Greek government should implement all recommendations of the June 2007 FATF mutual evaluation report on Greece. Greece should accelerate its efforts to realize new laws and regulations aimed at upgrading its FIU. This includes fully staffing with experienced analysts and improving its IT standards and capabilities so that analysts can effectively use its database. These IT upgrades should allow Greek authorities to implement a system to track statistics on money laundering prosecutions and convictions, as well as asset freezes and forfeitures. The Greek government should improve its asset freezing capabilities and develop a clear and effective system for identifying and freezing terrorist assets within its jurisdiction. The government should also publicize its system for appealing assets frozen in accordance with its UN obligations.

Greece should ensure uniform enforcement of its cross-border currency reporting requirements and take steps to deter the smuggling of currency across its borders. The government should abolish company-issued bearer shares, so that all bearer shares are legally prohibited. It should also ensure that its "Law 89" offshore companies and companies operating within its free trade zones are subject to the same AML requirements and gatekeeper and due diligence provisions, including know your customer rules and the identification of the beneficial owner, as in other sectors. The GOG should dedicate

additional resources to the investigation and prosecution of ML cases, as well as increase specialization and training on AML/CTF for law enforcement and judicial authorities. The GOG should also amend the existing legislative and regulatory framework to ensure that appropriate CDD requirements are implemented. Finally, it should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Grenada

Grenada is not a regional financial center. As a transit location, money laundering in Grenada is primarily related to smuggling and drug trafficking. Illicit proceeds are typically laundered through a wide variety of businesses, as well as through the purchase of real estate, boats, jewelry, and cars.

As of December 2007, Grenada's domestic financial sector is comprised of six commercial banks, 26 registered domestic insurance companies, two credit unions, and five money remitters. Grenada has one trust company and 1,580 international business companies (IBCs), a significant, if unexplained, decrease from the reported 6,000 IBCs in 2006. There are no casinos or Internet gaming sites operating in Grenada. There are no free trade zones in Grenada, although the Government of Grenada (GOG) has indicated that it may create one in the future. The GOG has repealed its economic citizenship legislation.

Bearer shares are not permitted for offshore banks. Registered agents are required by law to verify the identity of the beneficial owners of all shares. In addition, the International Companies Act requires registered agents to maintain records of the names and addresses of directors and beneficial owners of all shares. There is an U.S. $11,500 penalty and possible revocation of the registered agent's license for failure to maintain records. Grenada has not enacted laws preventing disclosure of client and ownership information by domestic and offshore services companies to bank supervisors and law enforcement authorities.

The Grenada Authority for the Regulation of Financial Institutions (GARFIN) became operational in early 2007. The GARFIN was created to consolidate supervision of all nonbank financial institutions, and effectively replace the Grenada International Financial Services Authority (GIFSA). Institutions supervised by GARFIN include insurance companies, credit unions, offshore financial services, the building and loan society, money service businesses, and other such services. The Eastern Caribbean Central Bank (ECCB) retains supervision responsibility for Grenada's commercial banks.

The Money Laundering Prevention Act (MLPA), enacted in 1999, and the Proceeds of Crime Act (POCA) No. 3 of 2003 criminalize money laundering in Grenada. Under the MLPA, the laundering of the proceeds of narcotics trafficking and all serious crimes is an offense. Under the POCA, the predicate offenses for money laundering extend to all criminal conduct, which includes illicit drug trafficking, trafficking of firearms, kidnapping, extortion, corruption, terrorism and its financing, and fraud. According to the POCA, a conviction on a predicate offense is not required to prove that certain goods are the proceeds of crime, and subsequently convict a person for laundering those proceeds. The POCA establishes a penalty three to ten years in prison and fines of $18,500 or more. This legislation applies to banks and nonbank financial institutions, as well as the offshore sector.

Established under the MLPA, the Supervisory Authority supervises the compliance of banks and nonbank financial institutions (including money remitters, stock exchange, insurance, casinos, precious gem dealers, real estate, lawyers, notaries, and accountants) with money laundering and terrorist financing laws and regulations. These institutions are required to know, record, and report the identity of customers engaging in significant transactions. This applies to large currency transactions over the threshold of $3,700. Records must be maintained for seven years. In addition, a reporting entity must monitor all complex, unusual or large business transactions, or unusual patterns of transactions, whether completed or not. Once a transaction is determined to be suspicious or

potentially indicative of money laundering, the reporting entity must forward a suspicious transaction report (STR) to the Supervisory Authority within 14 days. Reporting individuals are protected by law with respect to their cooperation with law enforcement entities.

The Supervisory Authority issued its Anti-Money Laundering Guidelines in 2001. The guidelines direct financial institutions to maintain records, train staff, identify suspicious transactions, and designate reporting officers. The guidelines also provide examples to help institutions recognize and report suspicious transactions. The Supervisory Authority is authorized to conduct anti-money laundering inspections and investigations. The Supervisory Authority can also conduct investigations and inquiries on behalf of foreign counterparts and provide corresponding information. Financial institutions may be fined for not granting access to Supervisory Authority personnel.

In June 2001, the GOG established a police-style financial intelligence unit (FIU). The FIU is charged with receiving and analyzing suspicious transaction reports (STRs) from the Supervisory Authority, and with investigating alleged money laundering offenses. The FIU has access to the records and databases of all government entities and financial institutions and is empowered to request any documents it considers necessary to its investigations. From January to November 2007, the FIU received 25 STRs and investigations commenced for all STRs received. The FIU has the authority to exchange information with its foreign counterparts without a memorandum of understanding (MOU).

Two foreign nationals were arrested by GOG authorities for money laundering in October 2007. These individuals came to Grenada with a large number of fraudulent credit cards and over a short period of time, withdrew in excess of $40,000 from automatic teller machines (ATMs) from several local banks. Half of the amount stolen was sent out to a number of different destinations via a legitimate money remittance company, which agreed to freeze the transaction. Local authorities are working with the company to repatriate those funds. The two perpetrators were arrested and charged with money laundering and fraud by false pretense. The case is currently ongoing.

The FIU and the Director of Public Prosecution's Office are responsible for tracing, seizing and freezing assets. Under current law, all assets can be seized, including legitimate businesses if they are used in the commission of a crime. The banking community cooperates with law enforcement efforts to trace funds and seize or freeze bank accounts. The time period for restraint of property is determined by the High Court. Presently, only criminal forfeiture is allowed by law. Proceeds from asset seizures and forfeitures can either be placed in the consolidated fund or the confiscated asset fund, which is supervised by the Supervisory Authority or the Cabinet for use in the development of law enforcement. The approximate dollar amount seized in the past year was U.S. $62,000, with approximately U.S. $22,000 forfeited. The Civil Forfeiture Bill, Cash Forfeiture Act, and Confiscation of the Proceeds of Crime Bill were introduced in 2006 and remain under discussion.

Grenada is not engaged in bilateral or multilateral negotiations with other governments to enhance asset tracing, freezing, and seizure. However, the GOG works actively with other governments to ensure tracing, freezing, and seizures take place, if and when necessary, regardless of the status of existing agreements.

The GOG regulates the cross-border movement of currency. However, there is no threshold requirement for currency reporting. Law enforcement and Customs officers have the powers to seize and detain cash that is imported or exported from Grenada. Cash seizure reports are shared between government agencies, particularly between Customs and the FIU.

The GOG criminalized terrorist financing through the Terrorism Act No. 5 2003. Grenada has the authority to identify, freeze, seize, and/or forfeit terrorist finance-related assets under the POCA and the Terrorism Act. The GOG circulates to the appropriate institutions the lists of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. There has

been no known identified evidence of terrorist financing in Grenada. It is suspected that alternative remittance systems are used in Grenada, though none have been positively identified.

In 2003, the GOG passed the Exchange of Information Act No. 2, which strengthens Grenada's ability to share information with foreign regulators. Grenada has a Mutual Legal Assistance Treaty (MLAT), Tax Information Exchange Agreement (TIEA) and an Extradition Treaty with the United States. The GOG cooperates fully with MLAT requests and responds rapidly to U.S. Government requests for information involving money laundering cases.

Grenada is a member of the Caribbean Financial Action Task Force (CFATF), and is expected to undergo a mutual evaluation in 2008. The GOG is also a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Grenada's FIU is a member of the Egmont Group. Grenada is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the Inter-American Convention against Terrorism. The GOG has not yet signed the UN Convention against Corruption.

Although the Government of Grenada has strengthened the regulation and oversight of its financial sector, it must remain alert to potential abuses and must steadfastly implement the laws and regulations it has adopted. The GOG should also move forward in adopting civil forfeiture legislation, and establish mechanisms to identify and regulate alternative remittance systems. Law enforcement and customs authorities should initiate money laundering investigations based on regional smuggling. Grenada should also become a party to the UN Convention against Corruption.

Guatemala

Guatemala is a major transit country for illegal narcotics from Colombia and precursor chemicals from Europe. Those factors, combined with historically weak law enforcement and judicial regimes, corruption, and increasing organized crime activity, contribute to a favorable climate for significant money laundering in Guatemala. According to law enforcement agencies, narcotics trafficking and corruption are the primary sources of money laundered in Guatemala; however, the laundering of proceeds from other illicit activities, such as human trafficking, contraband, kidnapping, tax evasion, and vehicle theft, is substantial. Officials of the Government of Guatemala (GOG) believe that the sources of the criminal proceeds laundered in Guatemala are derived from both domestic sources (primarily corruption cases) and foreign criminal activities. GOG officials also believe that cash couriers, offshore accounts, and wire transfers are used to launder funds, which are subsequently invested in real estate, capital goods, large commercial projects, and shell companies, or are otherwise transferred through the financial system.

Guatemala is not considered a regional financial center, but it is an offshore center. Exchange controls have been lifted and dollar accounts are common, but some larger banks conduct significant business through their offshore subsidiaries. The Guatemalan financial services industry is comprised of 22 commercial banks; ten offshore banks, all of which are affiliated, as required by law, with a domestic financial group (including affiliated credit card, insurance, finance, commercial banking, leasing, and related companies); two licensed money exchangers; 27 money remitters, including wire remitters and remittance-targeting courier services; 17 insurance companies; 17 financial societies; 15 bonded warehouses; 325 savings and loan cooperatives; eight credit card issuers; nine leasing entities; 11 financial guarantors; and one check-clearing entity run by the Central Bank. There are also hundreds of unlicensed money exchangers that exist informally.

The Superintendence of Banks (SIB), which is directed by the Monetary Board, has oversight and inspection authority over the Central Bank (Bank of Guatemala), as well as over banks, credit institutions, financial enterprises, securities entities, insurance companies, currency exchange houses

and other institutions as may be designated by the Bank of Guatemala Act. Guatemala's relatively small free trade zones target regional maquila (assembly line industry) and logistic center operations, and are not considered by GOG officials to be a major money laundering concern, although some proceeds from tax-related contraband may be laundered through them.

The offshore financial sector initially offered a way to circumvent currency controls and other costly financial regulations. However, financial sector liberalization has largely removed incentives for legitimate businesses to conduct offshore operations. All offshore institutions are subject to the same requirements as onshore institutions and are regulated by the Superintendence of Banks. In June 2002, Guatemala enacted the Banks and Financial Groups Law (No. 19-2002), which places offshore banks under the oversight of the SIB. The law requires offshore banks to be authorized by the Monetary Board and to maintain an affiliation with a domestic institution. It also prohibits an offshore bank that is authorized in Guatemala from doing business in another jurisdiction; however, banks authorized by other jurisdictions may do business in Guatemala under certain limited conditions.

To authorize an offshore bank, the financial group to which it belongs must first be authorized, under a 2003 resolution of the Monetary Board. By law, no offshore financial services businesses, other than banks, are allowed. In 2004, the SIB and Guatemala's financial intelligence unit (FIU), the Intendencia de Verificación Especial (IVE), concluded a process of reviewing and licensing all offshore entities, a process which resulted in the closure of two operations. No offshore trusts have been authorized. Offshore casinos and Internet gaming sites are not regulated.

There is continuing concern over the volume of money passing informally through Guatemala. Much of the more than U.S. $4.1 billion in 2007 remittance flows passed through informal channels, although sector reforms led to an increased use of banks and other formal means of transmission. Terrorist finance legislation enacted in August 2005 requires remitters to maintain name and address information on senders (principally U. S. based) on transfers equal to or over an amount to be determined by implementing regulations. Increasing financial sector competition should continue to expand services and bring more people into the formal banking sector, isolating those who abuse informal channels.

Decree 67-2001, or the "Law Against Money and Asset Laundering," criminalizes money laundering in Guatemala. This law specifies that individuals convicted of money or asset laundering are subject to a noncommutable prison term ranging from six to 20 years, and fines equal to the value of the assets, instruments or products resulting from the crime. Convicted foreigners are deported from Guatemala. Conspiracy and attempt to commit money laundering are also penalized. The law applies to money laundering from any crime and does not require a minimum threshold to be invoked. It also holds institutions and individuals responsible for failure to prevent money laundering or allowing money laundering to occur, regardless of personal culpability. Bank and financial institution directors or other employees can lose their banking licenses and face criminal charges if they are found guilty of failure to prevent money laundering. This law also applies to the offshore entities that operate in Guatemala but are registered under the laws of another jurisdiction.

Decree 67-2001 also obligates individuals to declare the cross-border movement of currency in excess of approximately U.S. $10,000 at the port of entry. The declaration forms are provided and collected by the tax authority at land borders, airports, and ports. The tax authority sends a copy of the sworn declaration to IVE for its database. The IVE can share this information with other countries under the terms and conditions specified by mutual agreement. In addition, the Law Against the Financing of Terrorism penalizes the omission of declaration with a sentence from one to three years in prison. At Guatemala City's international airport, a special unit was formed in 2003 to enforce the use of customs declarations upon entry to and exit from Guatemala. Money seized at the airports—approximately U.S. $1.8 million in 2007—suggests that proceeds from illicit activity are regularly hand-carried over

Guatemalan borders. However, apart from a cursory check of a self-reporting customs form, there is little monitoring of compliance at the airport. Compliance is not regularly monitored at land borders.

In addition to the requirements of Decree 67-2001, the Guatemalan Monetary Board's Resolution JM-191, which approves the "Regulation to Prevent and Detect the Laundering of Assets" (RPDLA), establishes anti-money laundering requirements for financial institutions. The RPDLA required all financial institutions under the oversight and inspection of the SIB to establish anti-money laundering measures, and introduced requirements for transaction reporting and record keeping. The Guatemalan financial sector has largely complied with these requirements and has a generally cooperative relationship with the SIB.

Financial institutions are prohibited from maintaining anonymous accounts or accounts that appear under fictitious or inexact names. Nonbank financial institutions, however, may issue bearer shares, and there is limited banking secrecy. However, Guatemalan law prohibits banking secrecy or privacy laws from being used to prevent the disclosure of financial information to bank supervisors and law enforcement authorities. Financial institutions are required to keep a registry of their customers as well as some types of transactions, such as the opening of new accounts or the leasing of safety deposit boxes. Financial institutions must also keep records of the execution of cash transactions exceeding $10,000 or more per day, and report these transactions to the IVE. Under Decree 67-2001, financial institutions must maintain records of these registries and transactions for five years. Financial institutions are also mandated by law to report all suspicious transactions to the IVE. The law also exonerates financial institutions and their employees of any criminal, civil or administrative penalty for their cooperation with law enforcement and supervisory authorities with regards to the information they provide.

Decree 67-2001 established the IVE within the Superintendence of Banks to supervise financial institutions and ensure their compliance with the law. The IVE began operations in 2002 and in 2007 had a staff of 32. The IVE has the authority to obtain all information related to financial, commercial, or business transactions that may be connected to money laundering. The IVE conducts inspections of financial institution management, compliance officers, anti-money laundering training programs, "know-your-client" policies, and auditing programs. From January 2001 to December 2007, the IVE imposed over U.S. $115,000 in administrative penalties for institutional failure to comply with anti-money laundering regulations.

Since its inception, the IVE has received approximately 2,302 suspicious transaction reports (STRs) from the 400 obligated entities in Guatemala. All STRs are received electronically, and the IVE has developed a system of prioritizing them for analysis. After determining that an STR is highly suspicious, the IVE gathers further information from public records and databases, other covered entities and foreign FIUs, and assembles a case. Once the IVE has determined a case warrants further investigation, the case must receive the approval of the SIB before being sent to the Anti-Money or Other Assets Laundering Unit (AML Unit) within the Public Ministry. Under current regulations, the IVE cannot directly share the information it provides to the AML Unit with any other special prosecutors (principally the anticorruption or counternarcotics units) in the Public Ministry. The IVE also assists the Public Ministry by providing information upon request for other cases the prosecutors are investigating.

The AML Unit is in charge of directing the investigation and prosecution of money laundering cases. This unit has a staff of 14 officials, and an investigative support group of 16 law enforcement officers and investigators. Both the prosecutors and investigators receive yearly ad hoc training in various investigative and legal issues. In 2006, Guatemala created a money laundering task force. The money laundering task force is a joint unit comprised of individuals from the Guatemalan Tax Authority (SAT), the IVE, Public Ministry, Prosecutor's Office, Government Ministry, National Police and Drug Police. Together they work on investigating financial crimes, building evidence and bringing the cases

to prosecution. In late 2007, the task force was working on four major money laundering investigations and a number of smaller money laundering and drug-related cases. Under the Anti-Organized Crime Law of 2006, the use of undercover operations, controlled deliveries, and wire taps is permitted to investigate many forms of organized crime activity, including money laundering crimes.

Twenty-seven cases have been referred by the IVE to the AML Unit. In several cases, assets have been frozen. Sixteen money laundering prosecutions have been concluded, fifteen of which resulted in convictions. The Public Ministry's AML Unit had initiated 63 cases as of January 2007, five of which have been transferred to other offices (such as the anticorruption unit) for investigation and prosecution, due to the nature of the particular crime. The seizures were made possible by information supplied by cooperating financial institutions.

Current law permits the seizure of any assets linked to money laundering. The IVE, the National Civil Police, and the Public Ministry have the authority to trace assets; the Public Ministry can seize assets temporarily in urgent circumstances, and the Courts of Justice have the authority to permanently seize assets. In 2003, the Guatemalan Congress approved reforms to allow seized money to be shared among several GOG agencies, including police and the IVE. Nevertheless, the Constitutional Court ruled that forfeited currency remains under the jurisdiction of the Supreme Court of Justice. The Anti-Organized Crime Law provides the possibility for a summary procedure to forfeit the seized assets and allows both civil and criminal forfeiture.

The courts do not allow seized currency to be used by enforcement agencies while cases remain open. For money laundering and narcotics cases, any seized money is deposited in a bank safe and all material evidence is sent to the warehouse of the Public Ministry. There is no central tracking system for seized assets, and it is currently impossible for the GOG to provide an accurate listing of the seized assets in custody. In 2006, Guatemalan authorities seized approximately U.S. $222,000 in bulk currency. No statistics are currently on the amount of assets seized in 2007. The lack of access to the resources of seized assets outside of the judiciary has made sustaining seizure levels difficult for the resource-strapped enforcement agencies.

In June 2005, the Guatemalan Congress passed legislation criminalizing terrorist financing, the Law Against the Financing of Terrorism. Implementing regulations were enacted by the Monetary Board in December 2005. The counter-terrorist financing legislation also clarifies the legality of freezing assets in the absence of a conviction where the assets were destined to support terrorists or terrorist acts. The legislation brings Guatemala into compliance with the FATF Special Recommendations on terrorist financing and the United Nations Security Council Resolution 1373.The GOG has cooperated fully with U.S. efforts to track terrorist financing funds.

Guatemala is a party to the UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Guatemala is also a party to the Inter-American Convention against Terrorism and the Central American Convention for the Prevention of Money Laundering and Related Crimes. The GOG is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). In 2003, the IVE became a member of the Egmont Group. The IVE has signed a number of Memoranda of Understanding regarding the exchange of information on money laundering issues, seventeen of which also include the exchange of information regarding the financing of terrorism.

Corruption and organized crime remain endemic in Guatemala and are the biggest long-term challenges to the rule of law in Guatemala. The Government of Guatemala has made efforts to comply with international standards and improve its anti-money laundering and counter-terrorist financing regime; however, Guatemala should eliminate the use of bearer shares as well as identify and regulate

offshore financial services and gaming establishments. The GOG should also continue efforts to improve enforcement of existing regulations and implement needed reforms. Cooperation between the IVE and the Public Ministry has improved in recent years, and several investigations have led to prosecutions. However, Guatemala should increase its capacity to successfully investigate and prosecute money laundering cases. Additionally, the GOG should identify or create a centralized agency to manage and dispose of seized and forfeited assets, create an assets forfeiture fund which would distribute forfeited assets to law enforcement agencies to assist in the fight against money laundering, terrorist financing, and other financial crime.

Guernsey

The Bailiwick of Guernsey (the Bailiwick) encompasses a number of the Channel Islands (Guernsey, Alderney, Sark, and Herm). A Crown Dependency of the United Kingdom, it relies on the United Kingdom for its defense and international relations. However, the Bailiwick is not part of the UK. Alderney and Sark have their own separate parliaments and civil law systems. Guernsey's parliament legislates in matters of criminal justice for all of the islands in the Bailiwick. Guernsey is a sophisticated financial center and, as such, it continues to be vulnerable to money laundering at the layering and integration stages.

The approximately 18,800 companies registered in the Bailiwick do not fall within the standard definition of an international business company (IBC). Guernsey and Alderney incorporate companies, but Sark, which has no company legislation, does not. Companies in Guernsey must disclose beneficial ownership to the Guernsey Financial Services Commission (FSC) before legal formation or acquisition.

Guernsey has 47 banks, all of which have offices, records, and a substantial presence in the Bailiwick. The banks are licensed to conduct business with residents and nonresidents alike. There are 632 international insurance companies and 851 collective investment funds. There are also 18 bureaux de change, ten of which are part of a licensed bank. Bureaux de change and other money service providers must register their information with the FSC.

Guernsey has a comprehensive legal framework to counter money laundering and the financing of terrorism. Guernsey had further honed its anti-money laundering and counter-terrorist financing (AML/CTF) legislation with the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007. The legislation criminalizes money laundering for all crimes except drug trafficking, which the Drug Trafficking (Bailiwick of Guernsey) Law, 2000, as amended, covers in identical terms. The Disclosure (Bailiwick of Guernsey) Law 2007 makes failure to disclose the knowledge or suspicion of money laundering a criminal offense. The duty to disclose suspicious activity extends to all businesses, not only financial services businesses. The original 1999 money laundering law creates a system of suspicious transaction reporting (including suspicion of tax evasion) to Guernsey's financial intelligence unit (FIU), the Financial Intelligence Service (FIS). In 2007, the FSC issued companion guidance entitled "Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing" which replaced the Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism.

Guernsey's legal framework contains additional legislative provisions aimed at assisting in the detection of money laundering and terrorist financing. These include search and seizure powers, customer information orders and account monitoring orders. The Transfer of Funds (Guernsey) Ordinance 2007 requires any parties that offer funds transfer services to provide verified identification information for any person transferring funds electronically.

Guernsey authorities have approved further measures to strengthen the existing AML/CTF regime that should be in force by the middle of 2008. These include a comprehensive civil forfeiture law, new

regulations for certain entities involved in high value transactions, and legislation governing charities and other nonprofit organizations.

Guernsey enacted the Prevention of Corruption (Bailiwick of Guernsey) Law of 2003 and the Regulation of Fiduciaries, Administration Businesses, and Company Directors, etc. (Bailiwick of Guernsey) Law of 2000 ("the Fiduciary Law") to license, regulate and supervise company and trust service providers. Pursuant to Section 35 of the Fiduciary Law, the FSC must license all fiduciaries, corporate service providers and persons acting as company directors on behalf of any business. The FSC creates Codes of Practice for corporate service providers, trust service providers and company directors. To receive licenses, these agencies must follow strict standards, including client identification and "know your customer" (KYC) requirements. These entities are subject to regular inspection, and an entity's failure to comply could result in prosecution and revocation of its license. The Bailiwick is fully compliant with the Offshore Group of Banking Supervisors (OGBS) Statement of Best Practice for Company and Trust Service Providers.

The FSC regulates the Bailiwick's financial banks, insurance companies, mutual funds and other collective investment schemes, investment firms, fiduciaries, company administrators and company directors. The Bailiwick does not permit bank accounts to be opened unless there has been a KYC inquiry and the customer provides verification details. Regulations contain penalties to be applied when financial services businesses do not follow their obligations. Upon a company's application for incorporation, the FSC evaluates the request. The Royal Court maintains the registry of incorporated companies. The Court will not permit incorporation unless the FSC and the Attorney General or Solicitor General have given approval. The Commission conducts regular on-site inspections and analyzes the accounts of all regulated institutions.

On July 1, 2005, the European Union Savings Tax Directive (ESD) came into force. The ESD is an agreement between the Member States of the European Union (EU) to automatically exchange information with other Member States about EU tax resident individuals who earn income in one EU Member State but reside in another. Although not part of the EU, the three UK Crown Dependencies (Guernsey, Jersey, and the Isle of Man), have voluntarily agreed to apply the same measures to those in the ESD and have elected to implement the withholding tax option (also known as the "retention tax option") within the Crown Dependencies.

Under the retention tax option, each financial services provider will automatically deduct tax from interest and other savings income paid to EU resident individuals. The tax will then be submitted to local and Member States tax authorities annually. The tax authorities receive a bulk payment but do not receive personal details of individual customers. If individuals elect the exchange of information option, then no tax is deducted from their interest payments but details of the customer's identity, residence, paying agent, level and time period of savings income received by the financial services provider will be reported to local tax authorities where the account is held and then forwarded to the country where the customer resides.

The Guernsey authorities have established a forum, the Crown Dependencies Anti-Money Laundering Group, where the Attorneys General, Directors General, and representatives of Police, Customs, the regulatory community and FIUs from the Crown Dependencies meet to coordinate AML/CTF policies and strategy.

The FIS operates as the Bailiwick's FIU, and is comprised of Police and Customs Officers. The Service Authority, a committee of senior Police and Customs Officers who coordinate the Bailiwick's financial crime strategy, directs the FIS. With a mandate to focus on money laundering and terrorist financing issues, the FIS serves as the central point within the Bailiwick for the receipt, collation, analysis, and dissemination of all financial crime intelligence. Much of this information comes from suspicious transaction report (STR) filings. In 2007, the FIS received 539 STRs.

The Bailiwick narcotics trafficking, money laundering, and terrorism laws designate the same foreign countries as the UK to enforce foreign restraint and confiscation orders.

In 2008, Guernsey will be the subject of an assessment regarding its compliance with internationally accepted standards and measures of good practice relative to its regulatory and supervisory arrangements for the financial sector. The International Monetary Fund (IMF) will conduct this assessment. The previous IMF assessment, conducted in 2002, determined that Guernsey had developed a legal and institutional AML/CTF framework and had a high level of compliance with what was then the Financial Action Task Force (FATF) Forty Recommendations.

There has been counterterrorism legislation covering the Bailiwick since 1974. The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, replicates equivalent UK legislation. The Terrorism Law criminalizes the failure to report suspicion or knowledge of terrorist financing.

Guernsey cooperates with international law enforcement on money laundering cases. The FSC also cooperates with regulatory/supervisory and law enforcement bodies. The Criminal Justice (International Cooperation) (Bailiwick of Guernsey) Law, 2000, furthers cooperation between Guernsey and other jurisdictions by allowing certain investigative information concerning financial transactions to be exchanged. In cases of serious or complex fraud, Guernsey's Attorney General can provide assistance under the Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law 1991.

On September 19, 2002, the United States and Guernsey signed a Tax Information Exchange Agreement, which came fully into force in 2006. The agreement provides for the exchange of information on a variety of tax investigations, paving the way for audits that could uncover tax evasion or money laundering activities. Guernsey is negotiating similar agreements with other countries. The 1988 U.S.-UK Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking, as amended in 1994, was extended to the Bailiwick in 1996.

Guernsey enacted the necessary legislation to implement the Council of Europe Convention on Mutual Assistance in Criminal Matters, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and the 1988 UN Drug Convention, upon their extension to the Bailiwick in 2002. The Bailiwick has requested that the UK Government seek the extension to the Bailiwick of the UN International Convention for the Suppression of the Financing of Terrorism.

Guernsey is a member of the Offshore Group of Insurance Supervisors and the Offshore Group of Banking Supervisors. The FIS has been a member of the Egmont Group since 1997 and represents the jurisdiction within The Camden Assets Recovery Inter-Agency Network (CARIN), an informal network of European Union (EU) member state contacts convened to work on asset recovery.

Guernsey continues to amend current legislation to stay current with international standards. Guernsey should ensure passage of its new 2008 legislation, and enact it, as soon as possible. It should integrate civil forfeiture into its legal framework. Guernsey should also work to ensure that the obliged entities uphold their legal obligations, and that the regulatory authorities have the tools they need to provide supervisory functions, especially with regard to nonfinancial businesses and professions. Guernsey should likewise ensure that all obliged entities receive the UN 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations.

Guinea-Bissau

Guinea-Bissau is not a regional financial center. Guinea-Bissau's instability and tiny economy make it an unlikely site for major money laundering. Increased drug trafficking and the prospect of oil

production, however, increase its vulnerability to money laundering and financial crime. Drug traffickers transiting between Latin America and Europe have increased their use of the country. Often, Guinea-Bissau is the placement point for proceeds from drug payoffs, theft of foreign aid, and corrupt diversion of oil and other state resources headed for investment abroad. A recent boom in construction of luxury homes, hotels and businesses, and the proliferation of expensive vehicles stands in sharp contrast with the conditions in the poor local economy. It is likely that at least some of the new wealth derives from money laundered from drug trafficking. Banking officials also think the country is vulnerable to trade-based money laundering (TBML).

The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the eight countries in the West African Economic and Monetary Union (WAEMU or UEMOA), including Guinea-Bissau, and uses the CFA franc currency. The Commission Bancaire, the BCEAO division responsible for bank inspections, is based in Abidjan. However, it does not execute a full AML examination during its standard banking compliance examinations.

The legal basis for Guinea-Bissau's AML/CTF framework is the Loi Uniforme Relative a Lutte Contre le Blanchiment de Capiteaux No. 2004-09 of February 6, 2004, or the Anti-Money Laundering Uniform Law (Uniform Law). As the common law passed by the members of UEMOA/WAEMU, all member states are required to enact and implement the legislation. On November 2, 2004, Guinea-Bissau became the third WAEMU/UEMOA country to enact the Uniform Law. The new legislation largely meets international standards with respect to money laundering. Guinea-Bissau has an "all crimes" approach to money laundering. The law requires banks and other financial institutions to know their customers and record and report the identity of any person who engages in significant transactions, including the recording of large currency transactions. Covered institutions include financial institutions and nonbank financial institutions such as exchange houses, brokerages, cash couriers, casinos, insurance companies, charities, nongovernmental organizations (NGOs), and intermediaries such as lawyers, accountants, notaries and broker/dealers. All obliged entities must report all suspicious transactions to the financial intelligence unit (FIU). There is no threshold amount triggering a report. Safe harbor provisions give reporting individuals and their supervisors civil and criminal immunity and immunity from professional sanctions for providing information to the FIU in good faith. There is no exemption for "self laundering". It is not necessary to have a conviction for the predicate offense before prosecuting or obtaining a conviction for money laundering. Criminal liability applies to all legal persons as well as natural persons. The new legislation meets many international standards with respect to money laundering, and goes beyond, by covering the microfinance sector, but does not comply with all Financial Action Task Force (FATF) recommendations concerning politically-exposed persons (PEPs), and lacks certain compliance provisions for nonfinancial institutions. All three banks operating in the country report that they have anti-money laundering (AML) compliance programs in place. However, Article 26 of National Assembly Resolution No. 4 of 2004 stipulates that if a bank suspects money laundering, it must obtain a declaration of all properties and assets from the subject and notify the Attorney General, who must then appoint a judge to investigate. The bank solicitation of an asset list from its client could amount to "tipping off" the subject. The WAEMU/UEMOA Uniform Law does not deal with terrorist financing.

Western Union and MoneyGram function under the auspices of the banks. Unlicensed money remitters and currency exchangers, although prevalent, are illegal. Authorities report problems with porous borders and cash smuggling; reportedly, corruption in the Customs agency exacerbates this situation.

The Uniform Law provides for the establishment of an FIU, and a 2006 Directive to establish it is in place. However, no operational FIU exists in the country. Guinea-Bissau is working with external donors to establish a functioning FIU, which will be housed within the Ministry of Economy and Finance. A senior Ministry of Finance official will administer the FIU. The FIU's mandate will be to receive and analyze suspicious transaction reports (STRs) and, when it deems appropriate, to refer

files to the Prosecutor General. The FIU will rely on counterparts in law enforcement and other governmental institutions to provide information upon request for the FIU's investigations. Lack of capacity, corruption, instability, and distrust (particularly of the judicial sector), could significantly hamper progress in the FIU's development. Reportedly, banks are reluctant to file STRs because of the fear of "tipping off" by an allegedly indiscrete judiciary. The FIU, when operational, can legally share information with any other FIU in the WAEMU/UEMOA countries.

The Judicial Police and Prosecutors investigate money laundering as well as terrorist financing. The Attorney General's office houses a small unit to investigate corruption and economic crimes. In November 2007, Guinea-Bissau's government Audit Office created a commission to investigate illegal acquisition of wealth by present and former government officials. However, a lack of training and capacity, as well as endemic corruption and reported lack of cooperation from banks, impede investigations. Official statistics regarding the prosecution of financial crimes are unavailable. There are no known prosecutions of money laundering.

Although the current AML legislation obliges NGOs and nonprofits, including charities, to file STRs, the current regulatory regime is unknown.

Article 203, Title VI of Guinea-Bissau's penal code criminalizes terrorist financing. However, there are no reporting requirements or attendant regulations. In addition, because the penal code only criminalizes the financing of terrorist groups or organizations, it does not address financing of a single or individual terrorist. The penal code also does not criminalize the financing of terrorist organizations when the money is not used to commit terrorist acts. The BCEAO has released Directive No. 04/2007/CM/UEMOA, obliging member states to pass domestic counter-terrorist financing legislation. Member states must enact a law against terrorist financing, which will likely be a Uniform Law to be adopted by all WAEMU/UEMOA members in the same manner as the AML law. Each national assembly must then enact the law. In July 2007, UEMOA/WAEMU released attendant guidance on terrorist financing for member states. In addition, the FATF-style regional body for the Economic Community of Western African States (ECOWAS), the African Anti-Money Laundering Inter-governmental Group (GIABA) has drafted a uniform law, which it has recommended that all of its member states adopt and enact.

The Ministry of Finance and the BCEAO circulate the UN 1267 Sanctions Committee consolidated list to commercial financial institutions. To date, no entity has identified assets relating to terrorist entities. The WAEMU/UEMOA Council of Ministers has issued a directive requiring banks to freeze assets of entities designated by the Sanctions Committee.

Multilateral ECOWAS treaties deal with extradition and legal assistance. Under the Uniform Law, once established, the FIU may share information freely with other FIUs in the union. Guinea-Bissau is a party to the 1988 UN Drug Convention, and has signed but not ratified the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, or the African Union (AU) Anticorruption Convention. Guinea-Bissau is a member of ECOWAS and GIABA. It has not signed or ratified the UN Convention against Corruption. Transparency International's 2007 Corruption Perception Index ranks Guinea Bissau 147 out of 180 countries.

The Government of Guinea-Bissau (GOGB) should continue to work with its partners in GIABA, WAEMU/UEMOA and ECOWAS to establish and implement a comprehensive AML/CTF regime that comports with all international standards. GOGB should ensure that the sectors covered by its AML law have implementing regulations and supervisory authorities to ensure compliance with the law's requirements. The GOGB should clarify, amend or eliminate Article 26 of the 2004 National Assembly Resolution that appears to mandate actions resulting in the tipping off of suspects. It should also adopt and enact the uniform terrorist financing law when it is presented to the WAEMU/UEMOA states. Guinea-Bissau should amend the definitions in its penal code to comport with the international

standards regarding financing of individual terrorists and terrorist groups engaging in acts other than terrorism. It should establish, staff and train, its FIU, and ensure that resources are available to sustain its capacity. It should work to improve the training and capacity of its police and judiciary to combat financial crimes, and address any issues resulting from a lack of understanding of money laundering and terrorist financing. Guinea-Bissau should undertake efforts to eradicate systemic corruption and become a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Conventions against Corruption and Transnational Organized Crime, and the African Union (AU) Anti-corruption Convention.

Guyana

Guyana is neither an important regional nor an offshore financial center, nor does it have any free trade zones. Money laundering is perceived as a serious problem, and has been linked to trafficking in drugs, firearms, and persons, as well as to corruption and fraud. The Government of Guyana (GOG) made no arrests or prosecutions for money laundering in 2007. Guyana currently has inadequate legal and enforcement mechanisms to combat money laundering, although legislation tabled in Parliament would enhance the GOG's anti-money laundering regime.

The Money Laundering Prevention Act (MLPA) of 2000 criminalizes money laundering related to narcotics trafficking, illicit trafficking of firearms, extortion, corruption, bribery, fraud, counterfeiting, and forgery. The MLPA does not specifically cover the financing of terrorism or all serious crimes in its list of offenses. Banks, finance companies, factoring companies, leasing companies, trust companies, and securities and loan brokers are required to report suspicious transactions to the GOG's financial intelligence unit (FIU), and records of suspicious transaction reports (STRs) must be kept for six years. However, the GOG does not release statistics on the number of STRs received by the FIU, despite the requirement to make these statistics available to relevant authorities as mandated by the Financial Action Task Force (FATF). The MLPA also requires that the cross-border transportation of currency exceeding U.S. $10,000 be reported to the Customs Administration, but does not allow for the provision of this information to the FIU or other law enforcement bodies. The MLPA establishes the Guyana Revenue Authority, the Customs Anti-Narcotics Unit, the Attorney General, the Director for Public Prosecutions, and the FIU as the authorities responsible for investigating financial crimes.

The GOG's anti-money laundering regime is rendered ineffective by other major structural weaknesses of the MLPA. While the MLPA provides for the seizure of assets derived as proceeds of crime, guidelines for implementing seizures and forfeitures have never been established. Conviction for a predicate offense is considered necessary before a money laundering conviction can be obtained, and the list of such predicate offenses is cursory. While the FIU may request additional information from obligated entities, it does not have access to law enforcement information or the authority to exchange information with its foreign counterparts. These limitations collectively stifle the analytical and investigative capabilities of the FIU and law enforcement agencies. As a result of these legislative weaknesses, there have been no money laundering prosecutions or convictions to date.

To augment the tools available to the GOG's anti-money laundering authorities, the FIU drafted legislation entitled the Anti-Money Laundering and Countering the Financing of Terrorism Bill 2007. The bill provides for the identification, freezing, and seizure of proceeds of crime and terrorism; establishes comprehensive powers for the prosecution of money laundering, terrorist financing, and other financial crimes; requires reporting entities to take preventive measures to help combat money laundering and terrorist financing; provides for the civil forfeiture of assets; expands the scope of the money laundering offense; and mandates the accessibility of all relevant data among law enforcement agencies. The legislation provides for oversight of export industries, the insurance industry, real estate, and alternative remittance systems, and sets forth the penalties for noncompliance. The bill also establishes the FIU as an independent body that answers only to the President, and defines in detail its

role and powers. The draft legislation was tabled in Parliament in late 2007, but its passage in the near future is uncertain.

In January 2007, the National Assembly passed the Gambling Prevention (Amendment) Bill, which legalizes casino gambling. The bill establishes a Gaming Authority authorized to issue casino licenses to new luxury hotel or resort complexes with a minimum of 150 rooms. Vocal opposition to the bill from religious groups, opposition parties, and the public included concerns that casino gambling would provide a front for money launderers. No casinos have opened in Guyana to date.

The Ministry of Foreign Affairs and the Bank of Guyana continue to assist U.S. efforts to combat terrorist financing by working towards compliance with relevant United Nations Security Council Resolutions (UNSCRs). In 2001, the Bank of Guyana, the sole financial regulator as designated by the Financial Institutions Act of March 1995, issued orders to all licensed financial institutions expressly instructing the freezing of all financial assets of terrorists, terrorist organizations, and individuals and entities associated with terrorists and their organizations. Guyana has no domestic laws authorizing the freezing of terrorist assets, but the government created a special committee on the implementation of UNSCRs, co-chaired by the Head of the Presidential Secretariat and the Director General of the Ministry of Foreign Affairs. To date the procedures have not been tested, as no terrorist assets have been identified in Guyana. The FIU director also disseminates the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list to relevant financial institutions.

Guyana is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). Guyana is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. On September 12, 2007, the GOG became a party to the International Convention for the Suppression of the Financing of Terrorism, and on June 5, 2007, Guyana ratified the Inter-American Convention against Terrorism. The GOG has not signed the UN Convention against Corruption. Guyana's FIU is one of the few in the region that is not a member of the Egmont Group, and no change in that status is anticipated until Guyana's anti-money laundering laws have been modernized and the financing of terrorism is criminalized. Guyana does not have a Mutual Legal Assistance Treaty (MLAT) with the United States.

The Government of Guyana should pass the draft legislation on money laundering and terrorist financing that is currently before the Parliament. The passage of this legislation would extend preventive measures to a far wider range of reporting entities, including casinos and designated nonfinancial businesses and professions. The draft legislation would also provide greater resources and critical autonomy for the FIU, enable the FIU to access law enforcement data, and ensure that the FIU has the operational capacity to meet the membership requirements of the Egmont Group. In short, the passage of this legislation is essential in enhancing the GOG's compliance with international standards and ensuring that its anti-money laundering and counter-terrorist financing regime is operational and effective. In the interim, Guyana should provide appropriate resources and awareness training to its regulatory, law enforcement, and prosecutorial personnel, and establish procedures for asset seizure and forfeiture. The GOG should also become a party to the UN Convention against Corruption.

Haiti

Haiti is not a major financial center. Haiti's dire economic condition and unstable political situation inhibit the country from advancing its formal financial sector. Nevertheless, Haiti is a major drug-transit country with money laundering activity linked to the drug trade. Money laundering and other financial crimes are facilitated through the banks and casinos, and through foreign currency transactions and real estate transactions. While the informal economy in Haiti is significant and partly

funded by illicit narcotics proceeds, smuggling is historically prevalent and predates narcotics trafficking.

Flights to Panama City, Panama, remain the main identifiable mode of transportation for money couriers. Suspected drug flights from Venezuela continue, where a permissive environment allows smuggling aircraft to operate with impunity. Travelers, predominantly Haitian citizens, usually hide large sums ranging from U.S. $30,000 to $100,000 on their persons. There is low confidence in the efforts of Haitian customs and narcotics personnel to interdict these outbound funds. Suspicions that clandestine fees are collected to facilitate the couriers continuing without arrest appear to be well-founded. In addition, those persons that are actually interdicted are frequently released by the courts and the funds are ordered to be returned.

During interviews, couriers usually declare that they intend to use the large amounts of U.S. currency to purchase clothing and other items to be sold upon their return to Haiti, a common practice in the informal economic sector. Cash that is routinely transported to Haiti from Haitians and their relatives in the United States in the form of remittances represented over 21.2 percent of Haiti's gross domestic product in 2006, according to the World Bank. The Inter-American Development Bank estimated the flow of remittances through official channels to Haiti at $1.65 billion in fiscal year 2006.

The Government of Haiti (GOH) has made progress in recent years to improve its legal framework, create and strengthen core public institutions, and enhance financial management processes and procedures. The constitutional government of President René Préval and Prime Minister Jacques Edouard Alexis continued the monetary, fiscal and foreign exchange policies initiated under the past Interim Government of Haiti with the assistance of the International Monetary Fund and the World Bank. Continued insecurity and a lack of personnel expertise, however, have reduced the impact of the Government's initiatives and hampered its ability to modernize its regulatory and legal framework.

Despite political instability, Haiti has taken steps to address its money laundering and financial crimes problems. President Preval has openly affirmed his commitment to fight corruption, drug trafficking, and money laundering. He is actively seeking technical assistance and cooperation with countries in the region to reinforce Haiti's institutional capacity to fight financial crime. In March 2007, the GOH participated in a Summit on Drug and Money Laundering in the Dominican Republic to identify synergies between countries in the region (Haiti, Dominican Republic, Jamaica and Colombia) to fight organized crime. Preparations are underway for a subsequent meeting to be held by the end of December 2007 in Cartagena, Colombia.

Since 2001, Haiti has used the Law on Money Laundering from Illicit Drug Trafficking and other Crimes and Punishable Offenses (AML Law) as its primary anti-money laundering legislation. Although the government has publicly committed to combat corruption, the court system is slow to move forward with pending cases. None of the investigations initiated under the interim government have led to any prosecutions, and the Financial Crimes Task Force (FCTF), which is charged with conducting financial investigations, is currently inoperative.

The AML Law criminalizes money laundering and establishes a wide range of financial institutions as obligated entities, including banks, money remitters, exchange houses, casinos, and real estate agents. Insurance companies, which are only nominally represented in Haiti, are not covered. The AML Law requires financial institutions to establish money laundering prevention programs and to verify the identity of customers who open accounts or conduct transactions that exceed 200,000 gourdes (approximately U.S. $5,550). It also requires exchange brokers and money remitters to compile information on the source of funds exceeding 200,000 gourdes or its equivalent in foreign currency. Microfinance institutions and credit unions, however, remain largely unregulated. A draft banking law, if passed by Parliament, will address this regulatory gap.

The AML Law contains provisions for the forfeiture and seizure of assets; however, the government cannot seize and declare the assets forfeited until there is a conviction. Although the AML Law provides grounds for seizure, it does not contain procedures to handle the management and proceeds of seized assets. This deficiency in the law reduces the government's authority and resources to prosecute cases. Out of U.S. $565,723 seized in 2007 at the airport in Port-au-Prince, courts ordered that U.S. $367,417 be returned to the owners.

Implementation of the AML Law is compromised by weak enforcement mechanisms, poor understanding of the law on the part of legal and judicial personnel and an overall weak judicial system. From 2001 to 2007, 475 persons were arrested in connection with drug trafficking and money laundering. Fifteen individuals were sent to the United States to face prosecution. The remaining 460 individuals have yet to be prosecuted in Haitian courts. An amendment to the AML Law to redress weaknesses in the current law is being drafted for consideration by Parliament.

In 2002, Haiti formed a National Committee to Fight Money Laundering (CNLBA) under the supervision of the Ministry of Justice and Public Safety. The CNLBA is in charge of promoting, coordinating, and recommending policies to prevent, detect, and suppress the laundering of assets obtained from the illicit trafficking of drugs and other serious offenses. Haiti's financial intelligence unit (FIU), established in 2003, is the Unité Centrale de Renseignements Financiers (UCREF), which falls under the supervision of the CNLBA. The UCREF's mandate is to receive and analyze reports submitted by financial institutions in accordance with the law. The UCREF has 42 employees, including 23 analysts. Institutions, including banks, credit unions exchange brokers, insurance companies, lawyers, accountants, and casinos, are required to report to the UCREF transactions involving funds that may be derived from a crime, as well as transactions that exceed 200,000 gourdes (U.S. $5,550). Failure to report such transactions is punishable by more than three years' imprisonment and a fine of 20 million gourdes (approximately U.S. $550,000). Banks are required to maintain records for at least five years and to present this information to judicial authorities and UCREF officials upon request. Bank secrecy or professional secrecy cannot be invoked as grounds for refusing information requests from these authorities.

In 2006, the UCREF assisted the U.S. in at least three major investigations. UCREF also assisted the interim government in filing the first-ever civil lawsuit in a U.S. court for reparation of Haitian government funds diverted through U.S. banks and businesses. However, the lawsuit was dropped shortly after the new government took office. Despite recent achievements, the UCREF is still not fully functional, and the UCREF's analysts lack the experience and skills needed to independently analyze suspect financial activities, write adequate reports and expeditiously move cases to prosecutors. Due to the absence of an investigative institution tasked with conducting financial investigations in the justice system, the UCREF responded to fill the void. This has led to a perception of conflict of interest and has, in some high-profile cases, sparked controversy.

In November, in response to a request for assistance from President Preval, the U.S. Treasury and the GOH entered into an agreement to restructure UCREF into an administrative FIU, and to reconstitute the investigative functions of the FCTF into a new and separate Office of Financial and Economic Affairs (BAFE). The U.S. Treasury Department agreed to provide training and technical assistance to BAFE investigators as well as the UCREF analysts, prosecutors, and judges. The World Bank has also entered into an agreement with the GOH to assist with training. These steps were supported by President Préval, who has sent out a presidential mandate to his ministers to support these new efforts in combating money laundering and corruption. In addition, draft counter-terrorist financing legislation has been submitted to the USG for review and comment.

Corruption is an ongoing challenge to economic growth. Haiti is ranked one of the most corrupt countries in the world according to Transparency International's Corruption Perception Index for 2007. The GOH has made incremental progress in enforcing public accountability and transparency,

but substantive institutional reforms are still needed. In 2004, the government established the Specialized Unit to Combat Corruption (ULCC) in the Ministry of Economy and Finance. The ULCC is in the process of drafting a national strategy to combat corruption and has prepared a draft law for asset declaration by public sector employees and a code of ethics for the civil service. ULCC will submit the law to Parliament for consideration in the coming months.

Haiti has yet to pass legislation criminalizing the financing of terrorists and terrorism, and is not a party to the International Convention for the Suppression of the Financing of Terrorism. Haiti reportedly circulates the list of terrorists and terrorist organizations identified in UN Security Council Resolution 1267. The AML Law may provide sufficient grounds for freezing and seizing the assets of terrorists; however, given that there is currently no indication of the financing of terrorism in Haiti, this has not been tested.

Haiti is a party to the 1988 UN Drug Convention, and has signed, but not ratified, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. Haiti is a member of the OAS/CICAD Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). In September 2007, the World Bank conducted an assessment of the GOH that will also serve as a CFATF mutual evaluation; the report will be released in the spring of 2008. The UCREF is not a member of the Egmont Group of financial intelligence units. The UCREF has memoranda of understanding with the FIUs of the Dominican Republic, Panama, Guatemala and Honduras.

The GOH appears cognizant of deficiencies in its anti-money laundering and counter-terrorist financing regime through its efforts to improve its legal framework to combat, drug trafficking, money laundering, and corruption, and its action to reform the judicial process. President Preval has made these improvements a key element of his national agenda. Areas in need of improvement include an ineffective court system, weak enforcement mechanisms and poor knowledge of current laws governing this area. The GOH should move quickly to prosecute cases of corruption, drug trafficking and money laundering. This could send a positive message that financial crimes will be punished to the fullest extent of the law and also help garner broader public support for the rule of law. The GOH should also reinforce the capacity of the Haitian justice system to prosecute financial crimes. Initiatives to enhance the UCREF's capacity to meet the Egmont Group membership standards and provide timely and accurate reports on suspicious financial activities are also needed. The GOH should finalize its draft legislation on terrorist financing to criminalize the financing of terrorism and become a party to the International Convention for the Suppression of the Financing of Terrorism.

Honduras

Money laundering in Honduras stems primarily from significant narcotics trafficking, particularly cocaine, throughout the region. Trafficking in persons also constitutes a growing source of laundered funds. Laundered proceeds typically pass directly through the formal banking system, but currency exchange houses and front companies may be used with increasing frequency. High remittance inflows, which reached more than $2.6 billion in 2007, as well as a rapidly growing construction sector and smuggling of contraband goods, may also generate funds that are laundered through the banking system. Money laundering in Honduras derives both from domestic and foreign criminal activity, and the majority of proceeds are suspected to be controlled by local drug trafficking organizations and organized crime syndicates. Honduras does not appear to be experiencing an increase in financial crimes such as bank fraud. Lack of resources for investigations and analysis, as well as corruption, remain serious problems, particularly within the judiciary and law enforcement sectors.

Honduras is not an important regional or offshore financial center. It does not have a significant black market for smuggled goods, although recent high-profile smuggling cases have involved gasoline and

illegal lobster. Honduras has established a number of free trade zones with special tax and customs benefits. The majority of companies with free trade zone status operate in the textile and apparel industry, mostly assembling piece goods that originated in the United States for re-export to the United States. Under Honduran legislation, companies may register for "free trade zone" status, and enjoy the associated tax benefits, regardless of their location in the country. In 2007, banks reported two abnormal transactions into the accounts of free-trade zone factory owners. Although prosecutors suspect money laundering, they were not able to build enough evidence to prosecute either case. There is no other evidence Honduran free trade zone companies are being used in trade-based money-laundering schemes or by financiers of terrorism.

Money laundering has been a criminal offense in Honduras since 1998. Law No. 27-98 criminalizes the laundering of narcotics-related proceeds and contains various record-keeping and reporting requirements for financial institutions. Decree No. 45-2002 strengthens the legal framework and available investigative and prosecutorial tools to fight money laundering. Decree 45-2002 expands the definition of money laundering to include transfer of assets that proceed directly or indirectly from trafficking of drugs, arms, human organs or persons; auto theft; kidnapping; bank and other forms of financial fraud; and terrorism, as well as any sale or movement of assets that lacks economic justification. The penalty for money laundering is 15 to 20 years. The law also requires all persons entering or leaving Honduras to declare (and, if asked, present) cash and convertible securities that they are carrying if the amount exceeds U.S. $10,000 or its equivalent.

Decree 45-2002 also creates the financial intelligence unit (FIU), the Unidad de Información Financiera (UIF), within the National Banking and Insurance Commission (CNBS). Banks and financial institutions are required to report any suspicious transactions and all transactions over $10,000, or its equivalent to the UIF. The UIF and reporting institutions must keep a registry of reported transactions for five years. Banks are required to know the identity of all their clients and depositors, regardless of the amount of deposits, and to keep adequate records of the information. Banker negligence provisions subject individual bankers to two- to five-year prison terms if, by carelessness, negligence, inexperience, or nonobservance of the law, they permit money to be laundered through their institutions. Anti-money laundering requirements apply to all financial institutions that are regulated by the CNBS, including state and private banks, savings and loan associations, bonded warehouses, stock markets, currency exchange houses, securities dealers, insurance companies, credit associations, and casinos.

Decree No. 129-2004 eliminates any ambiguity concerning the responsibility of banks to report information to the supervisory authorities, and the duty of these institutions to keep customer information confidential, by clarifying that the provision of information requested by regulatory, judicial, or other legal authorities shall not be regarded as an improper divulgence of confidential information. Under the Criminal Procedure Code, officials responsible for filing reports on behalf of obligated entities are protected by law with respect to their cooperation with law enforcement authorities. However, some have alleged that their personal security is put at risk if the information they report leads to the prosecution of money launderers.

Congress is currently considering legislation that, if adopted, would bring the Government of Honduras (GOH) up to international legal standards for illicit financing, including money laundering and terrorist financing. In October 2007, the CNBS proposed to Congress major amendments to the money laundering law and proposed a new chapter to the penal code that would criminalize terrorist financing. The proposed amendments to the money laundering law would give the UIF oversight for collecting all suspicious transactions reports, and expand the scope of entities required to report suspicious transactions to the UIF beyond the financial scope of the CNBS. Such entities would include real estate agents, used car dealership, antique and jewelry dealers, remittance companies, armed car contractors, and nongovernmental organizations. The reforms would also give the UIF sole

oversight and responsibility not only for collecting suspicious transaction reports but for analyzing and presenting to prosecutors cases deemed appropriate for prosecution.

The Public Ministry (Attorney General's Office), UIF, and police all suffer from low funding, limited capacity, and a lack of personnel and training. For example, the police officers charged with investigations of money laundering crimes in Honduras must ride public buses to conduct investigations. The lack of capacity and coordination limits the scope of analysis and prosecutions, and prosecutors expend the bulk of their limited resources focusing on high-profile crimes related to money laundering, such as narcotics, trafficking in persons, and cash smuggling. Prior to 2004, there had been no successful prosecutions of crimes specifically labeled as money laundering in Honduras. Between 2004 and 2006, prosecutors obtained 11 convictions. Prosecutors initiated legal proceedings in eight cases in 2007, all of which are still ongoing, and obtained two additional convictions from prosecutions initiated in 2005. Only two of 54 ongoing investigations in 2007 originated from financial reports.

Attempts to improve coordination among the Public Ministry (Attorney General's Office), the UIF, and police have met with some degree of success; however there is still a need for additional improvement. An attempt in late 2004 to create a coordinating body, the Interagency Commission for the Prevention of Money Laundering and Financing of Terrorism (CIPLAFT), failed in early 2006, for political reasons. Although Decree 45-2002 requires that a public prosecutor be assigned to the UIF, the Special Prosecutor for Money Laundering himself acts as coordinator and contact is sporadic. Nevertheless, response times for information sharing between the UIF and the seized assets unit have improved due to a 2006 agreement between the Public Ministry, CNBS, and UIF to prioritize money laundering cases. These actions helped to streamline the number of cases for potential prosecution, and allowed many cases to be officially closed. Fewer active cases have allowed the overloaded prosecutors and under-funded police units to focus on the strongest and most important cases. Adoption of the new anti-money laundering amendments should improve coordination and clarify division of responsibilities for investigations and reporting.

Remittance inflows, mostly from the United States, are estimated at more than U.S. $2.6 billion in 2007, which constitutes more than 25 percent of GDP. There has been no evidence to date linking these remittances to the financing of terrorism. However, it is estimated that up to half of cash flows labeled as remittances to Honduras may involve laundered money. Without the new money laundering amendment, the UIF lacks oversight capacity to properly investigate remittance companies, which are required to report suspicious transactions but currently not required to register under Honduran law. Remittances are increasingly sent through wire transfer or bank services, but the remittance companies themselves facilitate transactions that are carried out by separate financial institutions.

The GOH's asset seizure law has been in effect since 1993. The law allows for both civil and criminal forfeiture, and there are no significant legal loopholes that allow criminals to shield their assets. Decree No. 45-2002 strengthens the asset seizure provisions of the law, and establishes an Office of Seized Assets (OABI) under the Public Ministry. Decree 45-2002 also authorizes the OABI to guard and administer all goods, products, or instruments of a crime and requires money seized or money realized from the auctioning of seized goods to be transferred to the public entities that participated in the investigation and prosecution of the crime.

The OABI has moved to distribute funds to various law enforcement units and nongovernmental organizations (NGOs). The funds, which constituted the first systematic distribution under the new guidelines, went to the Supreme Court, federal prosecutors, OABI, and two civil society groups. Equitable sharing of seized monies has been a continuing problem, controlled by political influence. Police entities involved in the original investigations rarely see an equitable share of the assets seized. Groups like OABI and the Public Ministry generally receive an inflated portion of the forfeiture

proceeds, leaving next to nothing for the police. In some cases, entities that have nothing to do with the investigation receive an unjustified portion of the funds

The OABI is currently a poorly administered organization, evident by the vast amounts of assets that are unaccounted for, especially after the initial seizure, as well as the number of assets rotting away in parking lots, boat yards, and airports. The processing of final forfeiture of assets is mostly motivated by the entities that "arm wrestle" over who will actually receive disbursement of monies from auctioned assets or bulk cash seizure. This is typically influenced by political will. Momentum is now gaining for OABI to more quickly liquidate all assets once confiscated, in an effort to avoid parking lots full of deteriorating assets or high protection and maintenance fees. With new management and guidelines in place, OABI is set to expand its role significantly when a witness protection law passes that will allow the unit to hold all seized assets, not just assets seized under the money laundering law.

Decree No. 45-2002 leaves ambiguous the question of whether legitimate businesses found to be laundering money derived from criminal activities can be seized. Although the chief prosecutor for organized crime believes that businesses laundering criminal assets cease to be "legitimate," subjecting them to seizure and prosecution, this authority is not explicitly granted in the law. There has been no test case to date that would set an interpretation. There are currently no new laws being considered regarding seizure or forfeiture of assets of criminal activity.

Under the Criminal Procedure Code, when goods or money are seized in any criminal investigation, a criminal charge must be submitted against the suspect within 60 days of the seizure; if one is not submitted, the suspect has the right to demand the release of the seized assets.

As of December 2006, the total value of assets seized since Decree 45-2002 came into effect was approximately U.S. $5.7 million, including U.S. $4.6 million in tangible assets such as cars, houses, and boats. The total for 2007 decreased compared to 2006, because the prosecutor was forced to return almost U.S. $1 million this year, more than the sum collected. However, several high profile cases succeeded: U.S. $750,000 collected from the sale of an abandoned plane in 2007, probably related to narcotics, was used to purchase several cars for police investigators, and U.S. $500,000 collected from a high-profile lobster-smuggling case was awarded to the Ministry of Agriculture. Most of these seized assets have derived from crimes related to drug trafficking; none is suspected of being connected to terrorist activity.

Decree 45-2002 designates an asset transfer related to terrorism as a crime, but terrorist financing is not identified as a crime itself. However, in October 2007 the CNBS proposed adding a new chapter and five appendices to the Penal Code that would make financing of terrorism a crime. The crime would carry a 20 to 30 year prison sentence, along with a fine of up to $265,000. Changes to the penal code may not be discussed by Congress until the Supreme Court issues an opinion on the penalties. The proposal was being considered by the Supreme Court as of November 2007. It is unlikely that the terrorist financing and money laundering amendments will be considered by Congress before April 2008.

Under separate authority, the Ministry of Foreign Affairs is responsible for instructing the CNBS to issue freeze orders for organizations and individuals named by the United Nations Security Council Resolution (UNSCR) 1267 and those organizations and individuals on the list of Specially Designated Global Terrorists by the United States pursuant to Executive Order 13224. The Commission directs Honduran financial institutions to search for, hold, and report on terrorist-linked accounts and transactions, which, if found, would be frozen. Both the Ministry of Foreign Affairs and CNBS have responded promptly to these requests. CNBS has reported that, to date, no accounts linked to the entities or individuals on the lists have been found in the Honduran financial system.

Honduras cooperates with U.S. investigations and requests for information pursuant to the 1988 United Nations Drug Convention. No specific written agreement exists between the United States and

Honduras to establish a mechanism for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing, and other crime investigations. However, Honduras has cooperated, when requested, with appropriate law enforcement agencies of the U.S. Government and other governments investigating financial crimes. The UIF has signed memoranda of understanding to exchange information on money laundering investigations with Panama, El Salvador, Guatemala, Mexico, Peru, Colombia and the Dominican Republic.

Honduras is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. At the regional level, Honduras is a member of the Central American Council of Bank Superintendents, which meets periodically to exchange information. Honduras is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering, and the Caribbean Financial Action Task Force (CFATF). In 2005, the UIF became a member of the Egmont Group.

The Government of Honduras made progress in 2007 by continuing to implement existing anti-money laundering regulations, and proposing improvements to existing anti-money laundering legislation and amendments to the criminal code to criminalize terrorist financing. The GOH should ensure the passage and implementation of the proposed legislation in 2008 to bring its anti-money laundering and counter-terrorist financing regime into greater compliance with international standards. In the interim, the GOH should continue to support the developing law enforcement and regulatory entities responsible for combating money laundering and other financial crimes. It should hire and train more financial crimes investigators and analysts; improve cooperation between police, prosecutors, and the UIF; and ensure that resources are available to strengthen its anti-money laundering regime. The GOH should also resolve any ambiguity regarding the seizure of businesses used for criminal purposes.

Hong Kong

Hong Kong is a major international financial center. Its low taxes and simplified tax system, sophisticated banking system, shell company formation agents, and the absence of currency and exchange controls facilitate financial activity but also make Hong Kong vulnerable to money laundering. The Hong Kong Special Administrative Region Government (HKSARG) considers the primary sources of laundered funds to be corruption (both foreign and domestic), tax evasion, fraud, illegal gambling and bookmaking, prostitution, loan sharking, commercial crimes, and intellectual property rights infringement. Laundering channels include Hong Kong's banking system, legitimate and underground remittance and money transfer networks, trade-based money laundering, and large-ticket consumer purchases—such as property, gold and jewelry. The proceeds from narcotics trafficking are believed to be only a small percentage of illicit proceeds laundered.

Money laundering is a criminal offense in Hong Kong under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO). The money laundering offense extends to the proceeds of drug-related and other indictable crimes. Money laundering is punishable by up to 14 years' imprisonment and a fine of HK $5,000,000 (approximately U.S. $641,000).

Money laundering ordinances apply to covered institutions—including banks and nonbank financial institutions—as well as to intermediaries such as lawyers and accountants. All persons must report suspicious transactions of any amount to the Joint Financial Intelligence Unit (JFIU). The JFIU does not investigate suspicious transactions itself but receives, stores, and disseminates suspicious transactions reports (STRs) to the appropriate investigative unit. Typically, STRs are passed to the Narcotics Bureau, the Organized Crime and Triad Bureau of the Hong Kong Police Force, or to the Customs Drug Investigation Bureau of the Hong Kong Customs and Excise Department.

Financial regulatory authorities have issued anti-money laundering guidelines reflecting the revised FATF Forty Recommendations on Money Laundering to institutions under their purview and monitor compliance through on-site inspections and other means. The Hong Kong Monetary Authority (HKMA) is responsible for supervising and examining compliance of financial institutions that are authorized under Hong Kong's Banking Ordinance. The Hong Kong Securities and Futures Commission (SFC) is responsible for supervising and examining compliance of persons that are licensed by the SFC to conduct business in regulated activities, as defined in Schedule 5 of the Securities and Futures Ordinance. The Office of the Commissioner of Insurance (OCI) is responsible for supervising and examining compliance of insurance institutions. Hong Kong law enforcement agencies provide training and feedback on suspicious transaction reporting.

Financial institutions are required to know and record the identities of their customers and maintain records for five to seven years. The filing of a suspicious transaction report cannot be considered a breach of any restrictions on the disclosure of information imposed by contract or law. Remittance agents and moneychangers must register their businesses with the police and keep customer identification and transaction records for cash transactions above a legal threshold for at least six years. A directive from Hong Kong's Monetary Authority (HKMA) reduced this threshold amount from HK $20,000 (approximately U.S. $2,565) to HK $8,000 (approximately U.S. $1,000), effective January 1, 2007.

Hong Kong does not require reporting of the movement of any amount of currency across its borders, or of large currency transactions above any threshold level. Hong Kong is examining the effectiveness of its existing regime in interdicting illicit cross border cash couriering activities. Reportedly, Hong Kong is deliberating ways of complying with FATF Special Recommendation Nine but does not intend to put in place a "declaration system" and is instead considering a disclosure-based system. Law enforcement agents in Hong Kong are already empowered to seize criminal proceeds anywhere in the jurisdiction, including at the border.

Hong Kong does not make a distinction between onshore and offshore entities, including banks. Its financial regulatory regimes are applicable to residents and nonresidents alike. No differential treatment is provided for nonresidents, including with respect to taxation and exchange controls. The HKMA regulates banks. The Office of Commissioner of Insurance (OCI) and the Securities and Futures Commission (SFC) regulate insurance and securities firms, respectively. All three impose licensing requirements and screen business applicants. There are no legal casinos or Internet gambling sites in Hong Kong.

In Hong Kong, it is not uncommon to use solicitors and accountants, acting as company formation agents, to set up shell or nominee entities to conceal ownership of accounts and assets. Many of the more than 500,000 international business companies (IBCs) created in Hong Kong are established with nominee directors; and many are owned by other IBCs registered in the British Virgin Islands. The concealment of the ownership of accounts and assets is ideal for laundering funds. Additionally, some banks permit shell companies to open bank accounts, based only on vouching by the company formation agent. In such cases, the HKMA's anti-money laundering guidelines require banks to verify the identity of the owners of the company, including beneficial owners. The bank should also assess whether the intermediary is "fit and proper." However, solicitors and accountants have filed a low number of suspicious transaction reports in recent years; and Hong Kong officials seek to improve their reporting through regulatory requirements and oversight.

Hong Kong's open financial system has long made it the primary conduit for funds transferred out of China. Hong Kong's role has been evolving as China's financial system gradually opens. On February 25, 2004, Hong Kong banks began to offer Chinese currency-based (renminbi or RMB) deposit, exchange, and remittance services. Later that year, Hong Kong banks began to issue RMB-based credit cards, which could be used both in Mainland China and in Hong Kong shops that had enrolled

in the Chinese payments system, China Union Pay. In November 2005, Hong Kong banks were permitted modest increases in the scope of RMB business they can offer clients. The new provisions raised daily limits and expanded services. This change brought many financial transactions related to China out of the money-transfer industry and into the more highly regulated banking industry, which is better equipped to guard against money laundering. Banks in Hong Kong are still not permitted to make loans in RMB.

Despite Hong Kong's efforts to encourage capital shifts to the banking industry, Chinese capital controls impel entities in both Hong Kong and Mainland China to use underground financial systems to avoid restrictions on currency exchange. A well-publicized June 2007 raid by Chinese police on an underground bank in Shenzhen resulted in the detention of six suspects, including a Hong Kong-based businesswoman, accused of facilitating the transfer of RMB 4.3 billion (over U.S. $570 million) out of China since the beginning of 2006—including transfers by Chinese state-owned enterprises. Authorities believe the majority of these funds were used to purchase properties and stocks in Hong Kong. Media reports indicate that such underground exchange houses are rampant in Guangdong province and have transferred more than RMB 200 billion (U.S. $26.7 billion) out of China since 2006.

Under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO), a court may issue a restraining order against a defendant's property at or near the time criminal proceedings are instituted. Property includes money, goods, real property, and instruments of crime. A court may issue confiscation orders at the value of a defendant's proceeds from illicit activities. Cash imported into or exported from Hong Kong that is connected to narcotics trafficking may be seized, and a court may order its forfeiture. Legitimate businesses can be seized if the business is the "realizable property" of a defendant. Realizable property is defined under the DTRoP and OSCO as any property held by the defendant, any property held by a person to whom the defendant has directly or indirectly made a gift, or any property that is subject to the effective control of the defendant. The Secretary of Justice is responsible for the legal procedures involved in restraining and confiscating assets. There is no time frame ascribed to freezing drug proceeds or the proceeds of other crimes. Regarding terrorist property, a formal application for forfeiture must be made within two years of freezing. Confiscated or forfeited assets and proceeds are paid into general government revenue. In July 2002, the legislature passed several amendments to the DTRoP and OSCO to strengthen restraint and confiscation provisions. These changes, effective January 1, 2003, lowered the evidentiary threshold for initiating confiscation and restraint orders against persons or properties suspected of drug trafficking, eliminated the requirement of actual notice to an absconded offender, eliminated the requirement that the court fix a period of time in which a defendant is required to pay a confiscation judgment, authorized courts to issue restraining orders against assets upon arrest rather than charging, required the holder of property to produce documents and otherwise assist the government in assessing the value of the property, and created an assumption under the DTRoP (to make it consistent with OSCO) that property held within six years of the violation by a person convicted of drug money laundering constitutes proceeds from that money laundering.

According to JFIU figures, as of September 30, 2007, the value of assets under restraint was $199 million, and the value of assets under a court confiscation order but not yet paid to the government was $9.85 million. JFIU also reported that, as of September 30, 2007, $56.5 million had been confiscated and paid to the government since the enactment of DTRoP and OSCO. Hong Kong has shared confiscated assets with the United States.

Hong Kong Customs and Hong Kong Police are responsible for conducting financial investigations. The Hong Kong Police has a number of dedicated units responsible for investigating financial crime, but the primary units responsible for investigating money laundering and terrorist financing are the Commercial Crimes and Narcotics Bureaus in Police Headquarters. There were 157 prosecutions for money laundering during the first 6 months of 2007. Hong Kong Customs had a significant money

laundering case in 2006 in which the mastermind of a local pirated optical disc syndicate was convicted of money laundering involving HK $27.4 million (U.S. $3.5 million) accrued over a four-year period from piracy activities. This conviction was upheld on appeal in May 2007. The judge increased the sentence by 50 percent, in accordance with OSCO provisions. Hong Kong Customs arrested two individuals charged with copyright infringement and money laundering in 2007.

The JFIU receives and analyzes STRs to develop information that could aid in prosecuting money laundering cases and, in suitable cases, distributes reports to law enforcement investigating units. The JFIU can refer cases to all Hong Kong law enforcement agencies and, in certain circumstances, to regulatory bodies in Hong Kong as well as to overseas law enforcement bodies. The JFIU also conducts research on money laundering trends and methods and provides case examples (typologies) to financial and nonfinancial institutions to assist them in identifying suspicious transactions. The JFIU has no regulatory responsibilities. Since 1994, when OSCO first mandated the filing of suspicious transaction reports (STRs), the number of STRs received by JFIU has generally increased. In the first nine months of 2007, 12,308 STRs were filed, of which 1798 were referred to law enforcement agencies. This compares with 10,782 STRs filed for the same period in 2006, 13,505 STRs filed during all of 2005, 14,029 filed during 2004, and 11,671 during 2003. The JFIU launched an electronic system for reporting STRs by registered users in late 2006

On July 3, 2004, the Legislative Council passed the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance. This law is intended to implement UNSCR 1373 and the FATF Special Eight Recommendations on Terrorist Financing in place in July 2004. It extends the HKSARG's freezing power beyond funds to the property of terrorists and terrorist organizations. It also criminalizes the provision or collection of funds by a person intending or knowing that the funds will be used in whole or in part to commit terrorist acts. Hong Kong's financial regulatory authorities have directed the institutions they supervise to conduct record searches for assets of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224.

The People's Republic of China (PRC) represents Hong Kong on defense and foreign policy matters, including UN affairs. Through the PRC, the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism are all applicable to Hong Kong

To help deal with anti-money laundering (AML) issues from a practical perspective and reflect business needs, the Hong Kong Monetary Authority (HKMA) has recently coordinated the establishment of an Industry Working Group on AML. The Group, which includes representatives of some 20 authorized institutions, has met twice. Three subgroups have been established to share experiences and consider the way forward on issues such as PEPs (politically exposed persons), terrorist financing, transaction monitoring systems and private banking issues. The subgroup on Customer Due Diligence (CDD) issued guidelines on issues related to PEPs in November 2007. The HKMA has also implemented a number of initiatives on AML issues, including issuing circulars and guidance to authorized institutions on combating the financing of weapons of mass destruction conducting in-depth examinations of institutions' AML controls and setting out best practices for AML in high-risk areas—such as correspondent banking, private banking, and remittance.

The HKMA circulated guidelines that require banks to maintain a database of terrorist names and management information systems to detect unusual patterns of activity in customer accounts. The Securities and Futures Commission (SFC) and the Office of the Commissioner of Insurance (OCI) circulated guidance notes in 2005 that provided additional guidance on CDD and other issues, reflecting the new requirements in the Revised FATF Forty Recommendations on Money Laundering and Special Recommendations on Terrorist Financing. In 2006, the OCI and the SFC revised their guidance notes to take into account the latest recommendations by the FATF.

Other bodies governing segments of the financial sector are also engaged in advancing anti-money laundering efforts. The Hong Kong Estates Agents Authority, for instance, has drawn up specific guidelines for real estate agents on filing suspicious transaction reports; and the Law Society of Hong Kong and the Hong Kong Institute of Certified Public Accountants are in the process of drafting such guidance for their members.

Hong Kong is an active member of the Financial Action Task Force's FATF and Offshore Group of Banking Supervisors and was a founding member of the Asia Pacific Group on Money Laundering (APG).

In November 2007, the APG and FATF conducted a site visit as part of their joint mutual evaluation of Hong Kong. The mutual evaluation report will be discussed at FATF's June 2008 Plenary

Hong Kong's banking supervisory framework is in line with the requirements of the Basel Committee on Banking Supervision's "Core Principles for Effective Banking Supervision." Hong Kong's JFIU is a member of the Egmont Group and is able to share information with its international counterparts. Hong Kong is known to cooperate with foreign jurisdictions in combating money laundering.

Hong Kong's mutual legal assistance agreements generally provide for asset tracing, seizure, and sharing. Hong Kong signed and ratified a mutual legal assistance agreement (MLAA) with the United States that came into force in January 2000. Hong Kong has MLAAs with 22 other jurisdictions. Hong Kong has also signed surrender-of-fugitive-offenders (extradition) agreements with 17 countries, including the United States, and has signed agreements for the transfer of sentenced persons with ten countries, also including the United States. Hong Kong authorities exchange information on an informal basis with overseas counterparts and with Interpol.

The Government of Hong Kong should further strengthen its anti-money laundering regime by establishing threshold reporting requirements for currency transactions and putting into place "structuring" provisions to counter evasion efforts. Per FATF Special Recommendation IX, Hong Kong should also establish mandatory cross-border currency reporting requirements. Hong Kong should continue to encourage more suspicious transaction reporting by lawyers and accountants, as well as by business establishments, such as auto dealerships, real estate companies, and jewelry stores. Hong Kong should also take steps to stop the use of "shell" companies, IBCs, and other mechanisms that conceal the beneficial ownership of accounts by more closely regulating corporate formation agents. Particularly, since Hong Kong is a major trading center, Hong Kong law enforcement and customs authorities should seek to address trade-based money laundering.

Hungary

With an advantageous and pivotal location in central Europe, a cash-based economy and a well-developed financial services industry, criminal organizations from countries such as Russia and Ukraine have reportedly entrenched themselves in Hungary. Money laundering is related to a variety of criminal activities, including illicit narcotics trafficking, prostitution, trafficking in persons, and organized crime. Other prevalent economic and financial crimes include real estate fraud and the copying/theft of bankcards. Financial crime reportedly has not increased in recent years though there have been some isolated, albeit well-publicized, cases.

Hungary has worked continuously to improve its money laundering enforcement regime following its 2003 removal from the Financial Action Task Force (FATF) list of Non-Cooperative Countries and Territories. Since then, it has worked to implement the FATF Forty Recommendations and the Nine Special Recommendations on Terrorist Financing. In early 2005, the International Monetary Fund (IMF), in conjunction with the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), conducted the third-round mutual evaluation of Hungary's anti-money laundering and counter-terrorist financing (AML/CTF) regime. Of the FATF

49 Recommendations, Hungary received 38 ratings of "largely compliant" or better. Since the evaluation, Hungarian authorities have been committed to full implementation of the IMF/MONEYVAL recommendations to address deficiencies in its AML/CTF framework and implementation.

Hungary banned offshore financial centers, including casinos, by Act CXII of 1996 on Credit Institutions. Hungary discontinued its preferential tax treatment for offshore centers at the end of 2005; and in 2006 these companies automatically became Hungarian companies. The only special status they retain is the ability to keep financial records in foreign currencies. Hungary no longer permits the operation of free trade zones.

Act CXII of 1996 on Credit Institutions bans the use of any indigenous alternative remittance systems that bypass, in whole or in part, financial institutions. Act CXX of 2001 eliminated bearer shares and required that all such shares be transferred to identifiable shares by the end of 2003. All shares now are subject to transparency requirements, and both owners and beneficiaries must be registered.

The Government of Hungary (GOH) has prohibited the use of anonymous savings booklets since 2001. Act CXX of 2001 eliminated bearer shares and required that all such shares be transferred to identifiable shares by the end of 2003. All shares are now subject to transparency requirements, and all owners and beneficiaries must be registered. By mid-2003, Hungary had successfully transferred 90 percent of anonymous savings accounts into identifiable accounts. Individuals with remaining anonymous passbook accounts now need written permission from the police to access their accounts. The total balance remaining in anonymous accounts is approximately 20 million euros (approximately U.S. $29.5 million) for 2.5 million owners. This total is mainly comprised of accounts for which savings booklets were lost, accounts whose holders have not proceeded with the conversion nor tried to make a withdrawal, and accounts whose original owners have died and their heirs do not know how to access the funds.

The European Union's Third Money Laundering Directive (Directive 2005/60/EC of the European Parliament and of the Council of October 26, 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing) entered into force in December 2005 with member states required to enact the laws, regulations and administrative provisions necessary to comply with this Directive by December 15, 2007. The EU's Third Directive, which is consistent with the FATF 40 Recommendations and Nine Special Recommendations, necessitated that Hungary re-codify its original money laundering legislation, Act XV of 2003 on the Prevention and Impeding of Money Laundering. Hungary amended the legislation, and the implementing regulations entered into force in August 2006. These measures ensure the uniform implementation of the EU Directive with regard to the definition of "politically exposed persons" (PEPs), the technical criteria for simplified customer due diligence procedures, and exemptions for financial activity conducted on an occasional or very limited basis.

On November 19, 2007, the Parliament adopted Act CXXXVI on the Prevention and Combating of Money Laundering and Terrorist Financing (AML/CTF Act) and published the AML/CTF Act on November 28, 2007. The AML/CTF Act entered into force on December 15, 2007.
The AML/CTF Act establishes the legislative framework for the prevention and combat of terrorist financing and complies with international AML standards and requirements. The AML/CTF Act expands its scope to cover the following professions: financial services, investment services, insurance industry, commodity exchange services, postal money order and transfers, real estate agents, auditors, accountants, tax advisors, casinos, jewelry, lawyers, and notaries. The AML/CTF Act introduces more specific and detailed provisions relating to customer and beneficial owner identification and verification. The Act introduces a risk-sensitive approach regarding customer due diligence (CDD) and establishes detailed rules for CDD, including simplified as well as enhanced CDD for low or high-risk customers or business relationships, appropriate procedures to determine whether a person is a

PEP, and other requirements. Regulation (EC) No 1781/2006 of the European Parliament and of the Council of November 15, 2006 regarding originator information accompanying transfers of funds entered into force on the January 1, 2007. Hungary has implemented the regulation's requirements in the AML/CTF Act.

Obliged entities must send a suspicious transaction report (STR) to the financial intelligence unit (FIU) and suspend the transaction if there is suspicion of money laundering or terrorist financing. The AML/CTF Act sets out the requirements for disclosure of information, and mandates the keeping of statistics so that the effectiveness of the AML/CTF measures can be evaluated. The Act contains provisions on the internal procedures, training and internal communication, detailing special protocols for lawyers and notaries. Safe harbor provisions protect individuals when executing their AML/CTF reporting obligations.

Only banks or their authorized agents can operate currency exchange booths, of which there are approximately 300 in Hungary. These exchange houses are subject to "double supervision," because they are subject to both the banks' internal control mechanisms, as well as to supervision by the HFSA. In addition, the AML/CTF Act contains threshold-reporting requirements for currency exchange enterprises. Exchange booths must verify customer identity for currency exchange transactions totaling or exceeding 500,000 forints (approximately U.S. $3,000), whether in single transaction or derived from consecutive separate transactions. Exchange booths must file STRs for suspicious transactions in any amount.

Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of October 26, 2005 on controls of cash entering or leaving the Community addresses FATF Special Recommendation Nine regarding cash couriers. The regulation requires travelers to make a declaration to the competent authorities of all movement of cash reaching or exceeding 10,000 euros (approximately U.S. $15,000). Act No. XLVIII of 2007 on the promotion of the Regulation states that based on the EC regulation, the Hungarian customs authorities should record the information obtained under Article 3 (Obligation to declare) as well as the data collected in connection with any inspection of the declaration. If the data suggests money laundering or terrorist financing, the Hungarian Customs and Finance Guard (HCFG) must immediately send an STR to the financial intelligence unit (FIU).

A new provision on the money laundering offence [Section 303 of the Hungarian Criminal Code (HCC) after the amendment by Act XXVII of 2007] brings Hungary into compliance with the Vienna and Palermo Conventions by enlarging the scope of the money laundering offense to cover the transfer of proceeds to a third party even if it is carried out through a nonbanking or nonfinancial transaction. Act XXVII of 2007 also addresses problems that have occurred with the AML reporting regime. Strict criminal penalties for nonreporting have resulted in over-filing by Hungarian financial institutions. This, in turn, has resulted in a high volume of STRs that are reportedly of low quality. Act XXVII of 2007 reduces the maximum punishment for intentional noncompliance with reporting obligations from three years imprisonment to two years imprisonment. Hungary has also abolished the negligent form of nonreporting as a criminal offence. Section 9 of Act XXVII of 2007 includes provisions punishing individual financing of terrorist acts. In January 2008, Act XIX of 1998 on the Hungarian Criminal Procedure was amended. This amendment transferred the authority to investigate money laundering crimes and noncompliance with the AML/CTF Act from the Hungarian National Police (HNP) to the HCFG.

Hungary's financial regulatory body, the Hungarian Financial Supervisory Authority (HFSA), supervises financial service providers with the exception of cash processors, which are supervised by the National Bank of Hungary. The Hungarian Tax and Financial Control Administration supervises casinos. The FIU supervises most designated nonfinancial businesses and professions (DNFBPs), such as real estate agents, accountants and tax advisors. Supervisory functions are performed by self-regulatory bodies in certain cases: the Hungarian Bar Association with respect to lawyers, the

Hungarian Association of Notaries Public with respect to notaries public, and by the Chamber of Hungarian Auditors and Auditing Activities with respect to auditors. The Hungarian Trade Licensing Office is the supervisory authority with respect to the natural and legal persons trading in goods and allowing cash payments above the amount of 3.6 million forints (approximately U.S. $20,000).

In 2006, the HFSA established a new division to deal with money laundering and financial crimes. The division coordinates supervisory tasks related to money laundering and terrorist financing and also assists other departments of the HFSA with on-site inspections. In 2007, the HFSA enlarged the staff of its Financial Forensic division. One of the HFSA's major undertakings in 2007 was its participation in the implementation of the Third EU Directive on AML/CTF. The HFSA established a standing AML/CTF working group with the participation of the representatives of financial institutions and their associations.

Hungary's FIU, the National Bureau of Investigation's Anti-Money Laundering Department (ORFK), was originally a unit under the HNP. The FIU serves as the national center for receiving and analyzing STRs and other information regarding potential money laundering or terrorist financing. and disseminating them to the competent authorities As a law-enforcement style FIU, the ORFK has the authority to itself investigate money laundering cases. From January 1, 2007 until December 15, 2007 the FIU received 9,475 STRs, opened 40 cases, and confiscated 971,681,352 forints (approximately U.S. $5.5 million). In 2006, the FIU received 9,999 STRs, and opened 193 cases based upon STRs received.

As of December 15, 2007, the ORFK has undergone substantial organizational changes. It has moved from its current position within the HNP to the Hungarian Customs Authority. Although the ORFK still exists and receives STR data, its future operational capacity under the Hungarian Customs Authority remains unclear. The FIU's move to the Customs Authority has caused a significant reduction in information exchange with international counterparts. The Egmont Group of FIUs has decided to temporarily suspend information exchange with the ORFK, pending further clarification of the structural changes within the FIU.

The Hungarian Criminal Code (HCC), Act IV of 1978 contains a provision on asset forfeiture. Under this provision, assets used to commit crimes, pose a danger to public safety, or derive from criminal activity, are subject to forfeiture. All property related to criminal activity during the interval when its owner was involved with a criminal organization can be confiscated, unless the owner proves it was acquired legally. For most crimes, the police or FIU first freeze the assets and inform the bank within 24 hours whether they will pursue an investigation. A court ruling determines forfeiture and seizure for all crimes, including terrorist financing. The banking community has cooperated fully with enforcement efforts to trace funds and seize and freeze bank accounts. If the owner of the assets requests it, and the FIU approves the request, the frozen assets may be released on the basis of financial need, such as health-related expenses or basic sustenance,

Act IV of 1978, Article 261, criminalizes terrorist acts. Hungary has criminalized terrorism and all forms of terrorist financing with Act II of 2003, which modifies Criminal Code Article 261. Section 261 of the HCC, amended by Act XXVII of 2007, states that any person sponsoring activities of a terrorist or a terrorist group by providing material assets or any other support faces two to ten years imprisonment. The HFSA provides access for supervised institutions as well as for the general public on its homepage to access updates to the UN 1373 Sanctions Committee Consolidated List and its equivalent EU list, as well as the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. Terrorist finance-related assets can be frozen. The Act XIX of 1998 on Criminal Procedures, Articles 151, 159, and 160, provide for the immediate seizure, sequestration, and precautionary measures against terrorist assets.

Hungary and the United States have a Mutual Legal Assistance Treaty and a nonbinding information sharing arrangement designed to enable U.S. and Hungarian law enforcement to work more closely to

fight organized crime and illicit transnational activities. In May 2000, Hungary and the U.S. Federal Bureau of Investigation established a joint task force to combat Russian organized crime groups. Hungary has signed bilateral agreements with 41 other countries to cooperate in combating terrorism, drug trafficking, and organized crime.

Hungary is a member of the MONEYVAL Committee, a FATF-style regional body (FSRB). Hungary's FIU is a member of the Egmont Group; however, information exchanges within this body have been suspended pending the finalization of the FIU's reorganization and new functions. Hungary is a party to the UN International Convention for the Suppression of the Financing of Terrorism; the UN Convention against Transnational Organized Crime; the 1988 UN Drug Convention; and the UN Convention against Corruption.

Hungary has strengthened its legal and institutional background, and has made a significant progress regarding international communication and cooperation as well as training for the service providers who face money laundering and terrorist financing risks. Despite this progress, the GOH needs to continue its efforts with regard to implementation. An increased level of cooperation and coordination among the different law enforcement entities involved in fighting financial crime should be pursued. Prosecutors, judges, and police require enhanced knowledge to promote the successful prosecution of money laundering cases. The police and FIU should also have the option to extend their 24-hour time limit for the freezing of assets. The HFSA and other supervisory bodies should improve supervision and provide increased outreach and guidance to financial institutions with regard to reporting obligations. Hungary should re-criminalize negligent nonreporting of suspicious activities and transactions. The GOH should take steps to ensure that nonbank financial institutions file STRs. Increased AML/CTF training for the employees of financial institutions and other obliged entities is also necessary to improve the quality of STRs filed, in particular those which may be related to the financing of terrorism. The GOH should distribute the updates of the UN designated terrorist lists to the obliged entities, and not rely on posting updates online.

India

India's emerging status as a regional financial center, its large system of informal cross-border money flows, and its widely perceived tax avoidance problems all contribute to the country's vulnerability to money laundering activities. Some common sources of illegal proceeds in India are narcotics trafficking, illegal trade in endangered wildlife, trade in illegal gems (particularly diamonds), smuggling, trafficking in persons, corruption, and income tax evasion. Historically, because of its location between the heroin-producing countries of the Golden Triangle and Golden Crescent, India continues to be a drug-transit country.

India's strict foreign-exchange laws and transaction reporting requirements, combined with the banking industry's due diligence policy, make it increasingly difficult for criminals to use formal channels like banks and money transfer companies to launder money. However, large portions of illegal proceeds are often laundered through "hawala" or "hundi" networks or other informal money transfer systems. Hawala is an alternative remittance system that is popular among not only immigrant workers, but all strata of Indian society. Hawala transaction costs are less than the formal sector; hawala is perceived to be efficient and reliable; the system is based on trust and it is part of the Indian culture. According to Indian observers, funds transferred through the hawala market are equal to between 30 to 40 percent of the formal market. The Reserve Bank of India (RBI), India's central bank, estimates that remittances to India sent through legal, formal channels in 2006-2007 amounted to U.S. $28.2 billion. Due to the large number of expatriate Indians in North America and the Middle East, India continues to retain its position as the leading recipient of remittances in the world, followed by China and Mexico.

Many Indians, especially among the poor and illiterate, do not trust banks and prefer to avoid the lengthy paperwork required to complete a money transfer through a financial institution. The hawala system can provide the same remittance service as a bank with little or no documentation and at lower rates and provide anonymity and security for their customers. Hawala is also used to avoid currency restrictions, assists in capital flight, facilitates tax evasion, and avoids government scrutiny in financial transactions. The Government of India (GOI) neither regulates hawala dealers nor requires them to register with the government. The RBI argues that hawala dealers cannot be regulated since they operate illegally and therefore cannot be registered. Indian analysts also note that hawala operators are often protected by some politicians.

However, the Indian government is attempting to regulate a broader swath of the financial sector. In December 2005, the RBI issued guidelines requiring financial institutions, including money changers, to follow "know your customer" (KYC) guidelines and maintain transaction records for the sale and purchase of foreign currency. Foreigners and Nonresident Indians are permitted to receive cash payments up to U.S. $3,000 or its equivalent in other currencies from moneychangers. Recently, the RBI has been taking additional steps to crack down on unlicensed money transmitters and increase monitoring of nonbanking money transfer operations like currency exchange kiosks and wire transfer services. In September 2007, the RBI asked Western Union's Indian-based subsidiary, Western Union Services India, to desist from appointing any more sub-agents until further instruction. Western Union officials have explained to U.S. government officials that this is due to a new policy the Ministry of Home Affairs (MHA) is formulating to require wire transfer businesses to perform due diligence on sub-agents and seek RBI and MHA approval before appointing new sub-agents.

Historically, in Indian hawala transactions, gold has been one of the most important commodities. There is a widespread cultural demand for gold in India and South Asia. Since the mid-1990s, India has liberalized its gold trade restrictions. In recent years, the growing Indian diamond trade has been considered an important factor in providing counter-valuation; a method of "balancing the books" in external hawala transactions. Invoice manipulation is also used extensively to avoid both customs duties, taxes, and to launder illicit proceeds through trade-based money laundering.

India has illegal black market channels for selling goods. Smuggled goods such as food items, computer parts, cellular phones, gold, and a wide range of imported consumer goods are routinely sold through the black market. By dealing in cash transactions and avoiding customs duties and taxes, black market merchants offer better prices than those offered by regulated merchants. However, due to trade liberalization, the rise in foreign companies working and investing in India, and increased government monitoring, the business volume in smuggled goods has fallen significantly. In the last 10-15 years, most products previously sold in the black market are now traded through lawful channels.

With tax evasion a widespread problem in India, the GOI is gradually making changes to the tax system. The government now requires individuals to use a personal identification number to pay taxes, purchase foreign exchange, and apply for passports. The GOI also introduced a central value added tax (VAT) in April 2005 which replaced numerous complicated state sales taxes and excise taxes with one national uniform VAT rate. As a result, the incentives and opportunities for entrepreneurs and businesses to conceal their sales or income levels have been reduced. Except for Uttar Pradesh, all Indian states have implemented the national VAT mandate. Uttar Pradesh announced in late October 2007 that it would also implement the VAT.

In the aftermath of September 11, India joined the global community in addressing concerns about money laundering and terrorist finance by implementing the Prevention of Money Laundering Act (PMLA) in January 2003. The PMLA criminalized money laundering, established fines and sentences for money laundering offenses, imposed reporting and record keeping requirements on financial institutions, provided for the seizure and confiscation of criminal proceeds, and established a financial

intelligence unit (FIU). In July 2005, the PMLA's implementing rules and regulations were promulgated. The legislation outlines predicate offenses for money laundering. Predicate offenses are listed in a schedule to the Act, but these do not include many of the predicate offenses listed as essential by the FATF Recommendations, including organized crime, fraud, smuggling and insider trading. Penalties for offenses under the PMLA are severe and may include imprisonment for three to seven years and fines as high as U.S. $12,500. If the money laundering offense is related to a drug offense under the Narcotic Drugs and Psychotropic Substances Act (NDPSA), imprisonment can be extended to a maximum of ten years. The PMLA mandates that banks, financial institutions, and intermediaries of the securities market (such as stock market brokers) maintain records of all cash transactions (deposits/withdrawals, etc.) exceeding U.S. $25,000 and keep a record of all transactions dating back 10 years.

The Criminal Law Amendment Ordinance allows for the attachment and forfeiture of money or property obtained through bribery, criminal breach of trust, corruption, or theft, and of assets that are disproportionately large in comparison to an individual's known sources of income. The 1973 Code of Criminal Procedure, Chapter XXXIV (Sections 451-459), establishes India's basic framework for confiscating illegal proceeds. The NDPSA of 1985, as amended in 2000, calls for the tracing and forfeiture of assets that have been acquired through narcotics trafficking and prohibits attempts to transfer and conceal those assets. The Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act of 1976 (SAFEMA) also allows for the seizure and forfeiture of assets linked to Customs Act violations. The Competent Authority (CA), within the Ministry of Finance (MOF), administers both the NDPSA and the SAFEMA.

The 2001 amendments to the NDPSA allow the CA to seize any asset owned or used by an accused narcotics trafficker immediately upon arrest. Previously, assets could only be seized after a conviction. Even so, Indian law enforcement officers lack knowledge of the procedures for identifying individuals who might be subject to asset seizure/forfeiture and in tracing assets to be seized. They also appear to lack sufficient knowledge in drafting and expeditiously implementing asset freezing orders. In 2005, pursuant to the NDPSA and with U.S. government funding through its Letter of Agreement (LOA) with India, the CA began training law enforcement officials on asset forfeiture laws and procedures. CA has since held ten asset seizure and forfeiture workshops in New Delhi, Himachal Pradesh, Uttar Pradesh, Rajasthan, Andhra Pradesh, Karnataka and Assam. CA reports that the workshops have led to increased seizures and forfeitures. In 2007, the joint U.S./GOI Project Implementation Committee provided additional funds so that the Competent Authority could expand its training.

One of the GOI's principal provisions in combating money laundering is the Foreign Exchange Management Act (FEMA) of 2000. The FEMA's objectives include establishing controls over foreign exchange, preventing capital flight, and maintaining external solvency. FEMA also imposes fines on unlicensed foreign exchange dealers. Related to the FEMA is the Conservation of Foreign Exchange and Prevention of Smuggling Act (COFEPOSA), which provides for preventive detention in smuggling and other matters relating to foreign exchange violations. The MOF's Directorate of Enforcement (DOE) enforces the FEMA and COFEPOSA. The RBI also plays an active role in the regulation and supervision of foreign exchange transactions.

In April 2002, the Indian Parliament also passed the Prevention of Terrorism Act (POTA), which criminalizes terrorist financing, among other provisions. In March 2003, the GOI announced that it had charged 32 terrorist groups under the POTA. In July 2003, the GOI arrested 702 persons under the POTA. In November 2004, due to concerns that the overall law permitted overreaching police powers not related to the terrorist financing provisions, the Parliament repealed the POTA and amended the Unlawful Activities (Prevention) Act 1967 (UAPA) to include the POTA's salient elements such as criminalization of terrorist financing.

As part of the PMLA mandate, India's FIU was established in January 2006 to combat money laundering and terrorist financing. The FIU is responsible for receiving, processing, analyzing, and disseminating cash and suspicious transaction reports from financial institutions, banking companies, and intermediaries of the securities market. Over the last two years, the FIU has become fully operational and disseminates report analysis to law enforcement, investigative, and intelligence officers to investigate and prevent money laundering and curb financial crimes. The FIU has a staff of forty-three officers, headed by an Indian Administrative Service Director of equal rank to a Joint Secretary in the GOI ministries.

As of September 2007, FIU received more than 1800 suspicious transaction reports (STRs), of which about 800 were shared with relevant enforcement agencies. According to FIU officials, income tax evasion has been readily detected in the STRs and has also led to the arrest of suspected terror operatives. Reporting entities have immunity from civil proceedings for disclosures to FIU. The FIU also receives threat information and leads from foreign intelligence agencies concerning terrorists, terrorist groups, and international financial crimes information. Cash smuggling reports, which are prepared by Customs and the Enforcement Directorate, are not disclosed to the FIU but are shared with them indirectly on a need to know basis.

The FIU is an independent body reporting directly to the Economic Intelligence Council (EIC), which is headed by the Finance Minister. For administrative purposes, the FIU's operations are supervised by the MOF's Department of Revenue. While the FIU receives processes, analyzes, and disseminates information relating to suspect financial transactions to enforcement agencies and foreign FIUs, the unit does not have criminal enforcement, investigative, or regulatory powers. In 2007, the FIU initiated a project to adopt industry best practices and appropriate technology for creating an Information Technology Integrator. The integrator will process financial intelligence and alert on suspicious transactions.

In June 2007, India's FIU was admitted as a member of the Egmont Group. Admission of India's FIU as a member of the Egmont Group is seen by Indian officials as a major step forward in India joining the international community in its fight against money laundering and terrorist financing. FIU officials have expressed an interest in signing bilateral MOUs with foreign FIUs to facilitate sharing of money laundering information.

Under the MOF, the Enforcement Directorate is responsible for investigations and prosecutions of money laundering cases. In 2006-2007, the Enforcement Directorate initiated investigations into 38 cases of money laundering, eight of which were related to terrorist financing. The directorate has made seven seizure cases of properties worth $436,000. Headquartered in New Delhi, the directorate has seven zonal offices in Mumbai, Kolkata, Delhi, Jalandhar, Chennai, Ahmedabad, and Bangalore. In addition to the MOF, the Central Bureau of Investigation (CBI), the Directorate of Revenue Intelligence (DRI), Customs and Excise, RBI, and the CA are involved in GOI's anti-money laundering efforts.

The CBI is a member of INTERPOL. All state police forces and other law enforcement agencies have a link through INTERPOL/New Delhi to their counterparts in other countries for purposes of criminal investigations. India's Customs Service is a member of the World Customs Organization and shares enforcement information with countries in the Asia/Pacific region.

To assist in enhancing coordination among various enforcement agencies and directorates at the MOF, the GOI has established an Economic Intelligence Council (EIC). This provides a forum to strengthen intelligence and operational coordination, to formulate common strategies to combat economic offenses, and to discuss cases requiring interagency cooperation. In addition to the central EIC, there are eighteen regional economic committees in India. The Central Economic Intelligence Bureau (CEIB) functions as the secretariat for the EIC in the MOF. The CEIB interacts with the National

Security Council, the Intelligence Bureau, and the Ministry of Home Affairs on matters concerning national security and terrorism.

In October 2006, the MOF started the process to reconcile its list of predicate crimes under the PMLA with that of international FATF recommendations. Having made some progress towards that commitment, India gained FATF observer status in February 2007 and has a two-year probationary period to adopt FATF core recommendations towards gaining full membership. As defined by FATF, this includes criminalization of money laundering, customer due diligence, record-keeping, suspicious transaction reporting, criminalization of terrorist financing, and suspicious transaction reporting relating to terrorist financing, as well as expressing a political commitment to international standards for anti-money laundering. India is a member of the Asia/Pacific Group (APG) on Money Laundering, a FATF-style regional body.

The MOF is leading an inter-ministerial effort to amend the PMLA to meet FATF requirements. At present, the PMLA does not include comprehensive provisions on terrorist financing, and the required legislative amendments to the PMLA are still awaiting Cabinet approval before moving to Parliament for enactment. MOF officials have stated that changes to the PMLA will include incorporating provisions of the UAPA that criminalize terrorist financing, adopt most FATF recommended categories for predicate offenses, and implement reporting requirements for money changers, money transfer service providers, and casinos.

The Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority and the National Housing Board have also adopted anti-money laundering policies. SEBI has also issued a circular to all registered intermediaries on their obligations as financial institutions to prevent money laundering. This includes guidelines on maintaining records, preserving sensitive information with respect to certain transactions, and reporting suspicious cash flows and financial transactions to the FIU.

Prompted by the RBI's 2002 notice to commercial banks to adopt due diligence rules, many of these institutions have taken steps to combat money laundering. For example, most private banks and several public banks have hired anti-money laundering compliance officers to design systems and training to ensure compliance with these regulations. The Indian Bankers Association has also established a working group to develop self-regulatory anti-money laundering procedures and assist banks in adopting the mandated rules.

The RBI and SEBI have worked together to tighten regulations, strengthen supervision, and ensure compliance with KYC norms, which were implemented in December 2005. This includes, for example, provisions that banks must identify politically involved account holders who reside outside of India and identify the source of these funds before accepting deposits of more than U.S. $10,000. The RBI continues to update its due diligence guidelines based on FATF recommendations. For banks that are found noncompliant, the RBI has the power to order banks to freeze assets.

Banks are required to file STRs with FIU. Banks have installed software to enable their internal controllers to better monitor accounts for any unusual relationship between the size of the deposit and the turnover in the account and for matching names of terrorists and terrorist-associated countries. All banks have been advised by RBI that they should guard against establishing relationships with foreign financial institutions that permit their accounts to be used by shell companies. The UNSCR 1267 Sanctions Committee's consolidated list is routinely circulated to all financial institutions.

India does not have an offshore financial center but does license offshore banking units (OBUs). These OBUs are required to be predominantly owned by individuals of Indian nationality or origin resident outside India. The OBUs include overseas companies, partnership firms, societies, and other corporate bodies. OBUs must be audited to confirm that ownership by a nonresident Indian is not less than 60 percent. These entities are susceptible to money laundering activities, in part because of a lack of

stringent monitoring of transactions in which they are involved. Finally, OBUs must be audited financially; however, the auditing firm is not required to obtain government approval.

GOI regulations governing charities remain antiquated and the process by which charities are governed at the provincial and regional levels is weak. The GOI does require charities to register with the state-based Registrar of Societies, and, if seeking tax exempt status, they must apply separately with the Exemptions Department of the Central Board of Direct Taxes. There are no guidelines or provisions governing the oversight of charities for anti-money laundering or counter-terrorist financing (AML/CTF) purposes, and there is insufficient integration and coordination between charities' regulators and law enforcement authorities regarding the threat of terrorist finance. The Foreign Contribution Regulation Act (FCRA) of 1976, supervised by the MHA, regulates the use of foreign funds received by charitable/nonprofit organizations.

The GOI is a party to the 1988 UN Drug Convention. It is a signatory to, but has not yet ratified, the UN Convention against Transnational Organized Crime or the UN Convention against Corruption. India is a party to the UN International Convention for the Suppression of the Financing of Terrorism. India has signed and ratified a number of mutual legal assistance treaties with many countries, including the United States.

The Government of India should move forward expeditiously with amendments to the PMLA that explicitly criminalize terrorist financing, and expand the list of predicate offenses so as to meet FATF's core recommendations. Further steps in tax reform will also assist in negating the popularity of hawala and in reducing money laundering, fraud, and financial crimes. The GOI should ratify the UN Conventions against Transnational Organized Crime and Corruption. The GOI needs to promulgate and implement new regulations for nongovernment organizations including charities. Given the number of terrorist attacks in India and the fact that in India hawala is directly linked to terrorist financing, the GOI should prioritize cooperation with international initiatives that provide increased transparency in alternative remittance systems. India should devote more law enforcement and customs resources to curb abuses in the diamond trade. It should also consider the establishment of a Trade Transparency Unit (TTU) that promotes trade transparency; in India, trade is the "back door" to underground financial systems. The GOI also needs to strengthen regulations and enforcement targeting illegal transactions in informal money transfer channels.

Indonesia

Although neither a regional financial center nor an offshore financial haven, Indonesia is vulnerable to money laundering and terrorist financing due to a poorly regulated financial system, cash-based economy, the lack of effective law enforcement, and widespread corruption. Most money laundering in the country is connected to nondrug criminal activity such as gambling, prostitution, bank fraud, theft, credit card fraud, maritime piracy, sale of counterfeit of goods, illegal logging, and corruption. Indonesia also has a long history of smuggling, a practice facilitated by thousands of miles of un-patrolled coastline and law enforcement and customs infrastructure riddled with corruption. The proceeds of illicit activities are easily parked offshore and only repatriated as required for commercial and personal needs.

In June 2001, the Financial Action Task Force (FATF) added Indonesia to its list of Non-Cooperative Countries and Territories (NCCT). This designation was due to a number of serious deficiencies in Indonesia's Anti-Money Laundering (AML) framework including the lack of a basic set of AML provisions and the failure to criminalize money laundering. As a result of Indonesia's enactment of relevant AML legislation and its ongoing efforts to implement reforms to its AML regime, the FATF removed Indonesia from its NCCT list on February 11, 2005.

In April 2002, Indonesia passed Law No. 15/2002 Concerning the Crime of Money Laundering, making money laundering a criminal offense. The law identifies 15 predicate offenses related to money laundering, including narcotics trafficking and most major crimes. Law No. 15/2002 established the Financial Transactions Reports and Analysis Centre (PPATK), Indonesia's financial intelligence unit (FIU) to develop policy and regulations to combat money laundering and terrorist financing.

Law No. 15/2002 stipulated important provisions to enhance Indonesia's anti-money laundering regime, such as: obligating financial service providers to submit suspicious transactions reports and cash transaction reports; exempting reporting, investigation and prosecution of criminal offenses of money laundering from the provisions of bank secrecy that are stipulated in Indonesia's banking law; placing the burden of proof on the defendant; establishing the PPATK as an independent agency with the duty and the authority to prevent and eradicate money laundering; and establishing a clear legal basis for freezing and confiscating the proceeds of crime.

In September 2003, Parliament passed Law No. 25/2003, amending Law No. 15/2002, to further address FATF's concerns. Law No. 25/2003 provides a new definition for the crime of money laundering, making it an offense for anyone to deal intentionally with assets known, or reasonably suspected, to constitute proceeds of crime with the purpose of disguising or concealing the origin of the assets. The amendment removes the threshold requirement for proceeds of crime. The amendment further expands the scope of regulations by expanding the definition of reportable suspicious transactions to include attempted or unfinished transactions. The amendment also shortens the time to file an STR to three days or less after the discovery of an indication of a suspicious transaction. However, there is no clear legal obligation to report STRs related to terrorist financing. The amendment makes it an offense to disclose information about the reported transactions to third parties, which carries a penalty of imprisonment for a maximum of five years and a maximum fine of one billion rupiah (approximately U.S. $105,000).

Additionally, Articles 44 and 44A of Law 25/2003 provide for mutual legal assistance with respect to money laundering cases, with the ability to provide assistance using the compulsory powers of the court. Article 44B imposes a mandatory obligation on the PPATK to implement provisions of international conventions or international recommendations on the prevention and eradication of money laundering. In March 2006, the GOI expanded Indonesia's ability to provide mutual legal assistance by enacting the first Mutual Legal Assistance (MLA) Law (No. 1/2006), which establishes formal, binding procedures to facilitate MLA with other states.

A proposed second amendment to the AML law was submitted to the parliament in October 2006. If passed, it would require nonfinancial service businesses and professionals who potentially could be involved in money laundering, such as car dealers, real estate companies, jewelry traders, notaries and public accountants, to report suspicious transactions. The amendments also would include civil asset forfeiture and give more investigative powers to the PPATK, as well as the authority to block financial transactions suspected of being related to money laundering. Despite these provisions, the draft amendments appear to have remaining gaps when measured against current AML/CTF international standards.

Indonesia's FIU, PPATK, established in April 2002, became operational in October 2003 and continues to make progress in developing its human and institutional capacity. The PPATK is an independent agency that receives, analyzes, and evaluates currency and suspicious financial transaction reports, provides advice and assistance to relevant authorities, and issues publications. As of November 2007 the PPATK had received approximately 12,000 suspicious transactions reports (STRs) from 112 banks, seven rural banks, and 82 nonbank financial institutions. Approximately 5,000 of these STRs were received during 2007. The agency also reported that it had received a total of over four million cash transaction reports (CTRs) from 132 banks, 48 moneychangers, 35 rural

banks, five insurance companies, and two securities companies. PPATK have submitted a total of 521 cases to various law enforcement agencies based on their analysis of 882 STRs.

The PPATK actively pursues broader cooperation with relevant GOI agencies. The PPATK has signed a total of 16 domestic memoranda of understanding (MOUs) to assist in financial intelligence information exchange with the following entities: Attorney General's Office (AGO), Bank Indonesia (BI), the Capital Market Supervisory Agency (BAPEPAM), the Ministry of Finance Directorate General of Financial Institutions, the Directorate General of Taxation, Director General for Customs and Excise, the Ministry of Forestry Center for International Forestry Research, the Indonesian National Police, the Supreme Audit Board (BPK), the Corruption Eradication Committee, the Judicial Commission, the Directorate General of Immigration, the State Auditor, the Directorate General of the Administrative Legal Affairs Department of Law and Human Rights, the Anti-Narcotics National Board, and the Province of Aceh.

Bank Indonesia (BI), the Indonesian Central Bank, issued Regulation No. 3/10/PBI/2001, "The Application of Know Your Customer Principles," on June 18, 2001. This regulation requires banks to obtain information on prospective customers, including third party beneficial owners, and to verify the identity of all owners, with personal interviews if necessary. The regulation also requires banks to establish special monitoring units and appoint compliance officers responsible for implementation of the new rules and to maintain adequate information systems to comply with the law. BI has issued an Internal Circular Letter No. 6/50/INTERN, dated September 10, 2004 concerning Guidelines for the Supervision and Examination of the Implementation of KYC and AML by Commercial Banks. In addition, BI also issued a Circular Letter to Commercial Banks No. 6/37/DPNP dated September 10, 2004 concerning the Assessment and Imposition of Sanctions on the Implementation of KYC and other Obligations Related to Law on Money Laundering Crimes. BI is also preparing Guidelines for Money Changers on Record Keeping and Reporting Procedures, and Money Changer Examinations to be given by BI examiners. Currently, banks must report all foreign exchange transactions and foreign obligations to BI.

With respect to the physical movement of currency, Article 16 of Law No. 15/2002 contains a reporting requirement for any person taking cash into or out of Indonesia in the amount of 100 million Rupiah or more, or the equivalent in another currency, which must be reported to the Director General of Customs and Excise. These reports must be given to the PPATK in no later than five business days and contain details of the identity of the person. Indonesia Central Bank regulation 3/18/PBI/2001 and the Directorate General of Customs and Excise Decree No.01/BC/2005 contain the requirements and procedures of inspection, prohibition, and deposit of Indonesia Rupiah into or out of Indonesia.

The Decree provides implementing guidance for Ministry of Finance Regulation No.624/PMK. 2004 of December 31, 2004, and requires individuals who import or export more 100 million Rupiah in cash (approximately U.S. $10,500) to declare such transactions to Customs. This information is to be declared on the Indonesian Customs Declaration (BC3.2). The cash declaration requirements do no cover bearer negotiable instruments as required by FATF's Special Recommendation IX. In addition, cash can only be restrained if the passenger fails to disclose or a false declaration is made. In most cases, the cash is returned to the traveler after a small administrative penalty is applied. There is no clear authority to stop, restrain or seize money that is suspected of promoting terrorism or crime or constitutes the proceeds of crime. As of December 2007, the PPATK has received more than 2,137 reports from Customs on cross border cash carrying issues. The reports were derived from two airports, Jakarta Cengkarang and Denpasar, the seaports of Batam and Tanjung Balai Karimun, Bandung, Batam and Denpasar. As of July 2007, the Indonesian National Police have conducted 20 investigations based on cross-border currency reports. Despite these investigations, detection capacity is very weak and criminal penalties are limited and are not being applied.

Indonesia's bank secrecy law covers information on bank depositors and their accounts. Such information is generally kept confidential and can only be accessed by the authorities in limited circumstances. However, Article 27(4) of the Law No. 15/2002 expressly exempts the PPATK from "the provisions of other laws related to bank secrecy and the secrecy of other financial transactions" in relation to its functions in receiving and requesting reports and conducting audits of providers of financial services. In addition, Article 14 of the Law No. 15/2002 exempts providers of financial services from bank secrecy provisions when carrying out their reporting obligations. Providers of financial services, their officials, and employees are given protection from civil or criminal action for making required disclosures under Article 15 of the anti-money laundering legislation.

There is a mechanism to obtain access to confidential information from financial institutions through BI regulation number 2/19/PBI/2000. PPATK has the authority to conduct supervision and monitoring compliance of providers of financial services. PPATK may also advise and assist relevant authorities regarding information obtained by the PPATK in accordance with the provisions of this Law No. 15/2002.

The GOI has limited formal instruments to trace and forfeit illicit assets. Under the Indonesian legal system, confiscation against all types of assets must be effected through criminal justice proceedings and be based on a court order. The GOI has no clear legal mechanism to trace and freeze assets of individuals or entities on the UNSCR 1267 Sanctions Committee's consolidated list, and there is no clear administrative or judicial process to implement this resolution and UNSCR 1373. While the BI circulates the consolidated list to all banks operating in Indonesia, this interagency process is too complex and inefficient to send out asset-freezing instructions in a timely manner. In addition, no clear instructions are provided to financial institutions as to what will happen when assets are discovered. Banks also note that without very specific information, the preponderance of similar names and inexact addresses, along with lack of a unique identifier in Indonesia, make identifying the accounts very difficult. Attempts to use a criminal process are confusing and ad hoc at best, and rely on lengthy investigation processes before consideration can be given to freezing or forfeiting assets.

Article 32 of Law No. 15/2002, as amended by Law No. 25/2003, provides that investigators, public prosecutors and judges are authorized to freeze any assets that are reasonably suspected to be the proceeds of crime. Article 34 stipulates that if sufficient evidence is obtained during the examination of the defendant in court, the judge may order the sequestration of assets known or reasonably suspected to be the proceeds of crime. In addition, Article 37 provides for a confiscation mechanism if the defendant dies prior to the rendition of judgment.

In August, 2006, the GOI enacted Indonesia's first Witness and Victim Protection Law (No. 13/2006). Indonesia's AML Law and Government Implementing Regulation No. 57/2003 also provide protection to whistleblowers and witnesses.

The October 18, 2002 emergency counter-terrorism regulation, the Government Regulation in Lieu of Law of the Republic of Indonesia (Perpu), No. 1 of 2002 on Eradication of Terrorism, criminalizes terrorism and provides the legal basis for the GOI to act against terrorists, including the tracking and freezing of assets. The Perpu provides a minimum of three years and a maximum of 15 years imprisonment for anyone who is convicted of intentionally providing or collecting funds that are knowingly used in part or in whole for acts of terrorism. However, the terrorist financing regulation appears to suffer from a number of deficiencies. For example, the terrorist financing offense must be linked to a specific act of terrorism and the prosecution must prove that the offender specifically intended that the funds be used for acts of terrorism. This regulation is necessary because Indonesia's anti-money laundering law criminalizes the laundering of "proceeds" of crimes, but it is often unclear to what extent terrorism generates proceeds. Terrorist financing is therefore not fully included as a predicate for the money laundering offence. In October 2004, an Indonesian court convicted and

sentenced one Indonesian to four years in prison on terrorism charges connected to his role in the financing of the August 2003 bombing of the Jakarta Marriott Hotel.

The GOI has begun to take into account alternative remittance systems and charitable and nonprofit entities in its strategy to combat terrorist financing and money laundering. The PPATK has issued guidelines for nonbank financial service providers and money remittance agents on the prevention and eradication of money laundering and the identification and reporting of suspicious and other cash transactions. The GOI has initiated a dialogue with charities and nonprofit entities to enhance regulation and oversight of those sectors.

Indonesia is an active member of the Asia/Pacific Group on Money Laundering (APG), and currently serves as the co-chair. The APG conducted its second mutual evaluation of Indonesia in November 2007 and the report will be discussed and adopted at the APG Annual Meeting in July 2008. In June 2004, PPATK became a member of the Egmont Group. The PPATK has pursued broader cooperation through the MOU process and has concluded 23 MOUs with other Egmont FIUs. The PPATK has also entered into an Exchange of Letters enabling international exchange with Hong Kong. Indonesia has signed Mutual Legal Assistance Treaties with Australia, China and South Korea. Indonesia joined other ASEAN nations in signing the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters on November 29, 2004, though the GOI has not yet ratified the treaty. The Indonesian Regional Law Enforcement Cooperation Centre was formally opened in 2005 and was created to develop the operational law enforcement capacity needed to fight transnational crimes.

The GOI has enacted Law No. 7/2007 to implement the 1988 UN Drug Convention, to which it is a party. The GOI also has enacted Law No. 22/1997 Concerning Drugs and Psychotropic Substances, which makes the possession, purchase or cultivation of narcotic drugs or psychotropic substances for personal consumption a criminal offense. The GOI is a party to the UN International Convention for the Suppression of the Financing of Terrorism and a party to the UN Convention against Corruption. The GOI has signed but has yet to ratify the UN Convention against Transnational Organized Crime. Indonesia is ranked 143 of 180 countries ranked in Transparency International's 2007 Corruption Perception Index.

While The Government of Indonesia has made progress in constructing an AML regime, efforts to combat terrorist financing have been weak. Sustained public awareness campaigns, new bank and financial institution disclosure requirements, and the PPATK's support for Indonesia's first credible anti-corruption drive has led to increased public awareness about money laundering and, to a lesser degree, terrorist financing. However, weak human and technical capacity, poor interagency cooperation, and rampant corruption in business and government remain significant impediments to the continuing development of an effective anti-money laundering regime. The highest levels of GOI leadership should continue to demonstrate strong support for strengthening Indonesia's anti-money laundering regime. In particular, the GOI must continue to improve capacity and interagency cooperation in analyzing suspicious and cash transactions, investigating and prosecuting cases, and achieving deterrent levels of convictions. As part of this effort, Indonesia should review and streamline its process for reviewing UN designations and identifying, freezing and seizing terrorist assets, and become a party to the UN Convention against Transnational Organized Crime.

Iran

Iran is not a regional financial center. Iran's economy is marked by a bloated and inefficient state sector and over-reliance on the petroleum industry. Iran's huge oil and gas reserves produce 60 percent of government revenue-and state-centered policies that cause major distortions in the economy. Iran earns about U.S. $50 billion a year in oil exports. Private sector activity is typically small-scale; workshops, farming, and services. Reportedly, a prominent Iranian banking official estimates that money laundering encompasses an estimated 20 percent of Iran's economy. There are other reports

that approximately U.S. $12 billion a year is laundered via smuggling commodities in Iran and over U.S. $6 billion is laundered by international criminal networks. The World Bank reports that about 19 percent of Iran's GDP pertains to unofficial economic activities. Money laundering in Iran encompasses narcotics trafficking, smuggling, trade fraud, counterfeit merchandise and intellectual property rights violations, cigarette smuggling, trafficking in persons, hawala, capital flight, and tax evasion.

After the Iranian Revolution of 1979, the Government of Iran (GOI) nationalized the country's banks, leaving the following: Bank Refah, Bank Melli Iran, Bank Saderat, Bank Tejarat, Bank Mellat and Bank Sepah, and three specialized institutions, Bank Keshavrzi, Bank Maskan and Bank Sanat va Madden. No foreign banks were allowed to operate in the country. Since 1983, consistent with Islamic law, banks have been prohibited from paying interest on deposits or charging interest on loans. However, alternative financial instruments were developed including profit-sharing and financing based on trade. In 1994, Iran authorized the creation of private credit institutions. Licenses for these banks were first granted in 2001. Currently, these banks include Karafarin, Parsian, Saman Eghtesad, Pasargad, Sarmayeh, and Eghtesade Novin. Standard Chartered Bank became the first foreign bank to be awarded a license to establish a branch in Iran, although this was limited to Kish, a free-zone island. Currently, some 40 international banks have representative offices in Iran, which may undertake lending but not accept deposits.

There are currently no meaningful anti-money laundering (AML) controls on the Iranian banking system. The Central Bank of Iran (CBI) has issued AML circulars that address suspicious activity reporting and other procedures that demonstrate an awareness of international standards, but there is a lack of implementation. In 2003, the Majlis (Parliament) reportedly passed an anti-money laundering act. The act includes customer identification requirements, mandatory record keeping for five years after the opening of accounts, and the reporting of suspicious activities. However, the act has not been implemented due to reported pressure by vested interests within the government. Iran has reported to the United Nations that it has established a financial intelligence unit (FIU). However, Iran has not provided any documentation or details on the FIU.

The U.S. Department of State has designated Iran as a State Sponsor of Terrorism. On September 8, 2006 the U.S. Treasury Department issued a regulation prohibiting U.S. financial institutions from handling any assets, directly or indirectly, relating to Iran's Bank Saderat, based on evidence of its involvement in transferring funds to terrorist groups. Bank Saderat is one of Iran's largest with approximately 3,400 branches. On January 9, 2007, the U.S. Treasury Department imposed sanctions against Bank Sepah, a state-owned Iranian financial institution for providing support and services to designated Iranian proliferation firms, particularly Iran's missile procurement network. There are reports that Bank Sepah requested other financial institutions to remove its name from processing suspect transactions in the international financial system. Bank Sepah is the fifth largest Iranian state-owned bank and has international branches in Europe.

On October 11, 2007, FATF released a statement of concern stating that "Iran's lack of a comprehensive AML/CTF regime represents a significant vulnerability within the international financial system. FATF calls upon Iran to address on an urgent basis its AML/CTF deficiencies, including those identified in the 2006 International Monetary Fund Article IV Consultation Report for Iran. FATF members are advising their financial institutions to consider the risk arising from the deficiencies in Iran's AML/CTF regime and practice enhanced "due diligence." Iran is currently the only country for which FATF has publicly identified such significant AML/CTF vulnerabilities. On October 16, 2007, the Department of Treasury issued an advisory to financial institutions that they "should be aware that there may be an increased effort by Iranian entities to circumvent international sanctions and related financial community scrutiny through the use of deceptive practices involving shell companies and other intermediaries or requests that identifying information be removed from transactions. Such efforts may originate in Iran or Iranian free trade zones subject to separate

regulatory and supervisory controls, including Kish Island. Such efforts may also originate wholly outside of Iran at the request of Iranian controlled entities."

On October 25, 2007, the Department of Treasury designated for proliferation activities under Executive Order 13382 Iran's state-owned Banks Melli and Mellat. Bank Melli is Iran's largest bank. Bank Melli provides banking services to entities involved in Iran's nuclear and ballistic missile programs, including entities listed by the UN for their involvement in those programs. Bank Melli provides banking services to the Iranian Revolutionary Guards Corps (IRGC) and the Qods Force. When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement in the international banking system. Bank Mellat provides banking services in support of Iran's nuclear entities, including those designated by the United States and by the UN Security Council under UNSCRs 1737 and 1747. On October 25, Bank Saderat was also designated for its support for terrorism, specifically channeling funds to terrorist organizations including Hizballah and EU-designated terrorist groups Hamas, PFLP-GC, and Palestinian Islamic Jihad.

Iran has a very large underground economy, which is spurred by restrictive taxation, widespread smuggling, currency exchange controls, capital flight, and a large Iranian expatriate community. The IMF reports that Iran has the highest "brain drain" rate of 90 countries measured. Over 400,000 Iranians live in Dubai. Anyone engaging in transfers or transactions of foreign currency into or out of Iran must abide by CBI regulations, including registration and licensing. Those who do not are subject to temporary or permanent closure. The regulations and circulars address money transfer businesses, including hawaladars. However, underground hawala and moneylenders in the bazaar are active in Iran. Since there is an absence of an adequate banking system and working capital, the popular informal system meets the need for currency exchange and money lending. Many hawaladars and traditional bazaari are linked directly to the regional hawala hub in Dubai. Counter valuation in hawala transactions is often accomplished via trade. The trade and smuggling of goods into Iranian commerce leads to a significant amount of trade-based money laundering and value transfer. Approximately 7,500 Iranian-owned companies operate out of Dubai.

Iran's real estate market is often used to launder money. Frequently, real estate settlements and payment are made overseas. In addition, there are reports that a massive amount of Iranian capital has been invested in the United Arab Emirates, particularly in Dubai real estate. Iranian investments in Dubai may be in excess of U.S. $350 billion.

Via a transit trade agreement, goods purchased primarily in Dubai are sent to ports in southern Iran and then via land routes to markets in Afghanistan. The transit trade facilitates the laundering of Afghan narcotics proceeds via barter transactions, trade-based money laundering, and trade goods that provide counter valuation in the regional hawala markets. According to the United Nations Office on Drugs and Crime, approximately 60 percent of Afghanistan's opium is trafficked across Iran's border. Reportedly, Iran has an estimated three million drug users and the highest per capita heroin addiction rate in the world. Opiates not intended for the Iranian domestic market transit Iran to Turkey, where the morphine base is converted to heroin. Heroin and hashish are delivered to buyers located in Turkey. The drugs are then shipped to the international market, primarily Europe. In Iran and elsewhere in the region, proceeds from narcotics sales are sometimes exchanged for trade goods via value transfer. The United Nations Global Program against Money Laundering (GPML) also reports that illicit proceeds from narcotics trafficking are used to purchase goods in the domestic Iranian market and then the goods are often exported and sold in Dubai.

Iran's "bonyads," or charitable religious foundations, were originally established at the time of the Iranian revolution to help the poor. They have rapidly expanded beyond their original mandate. Although still funded, in part, by Islamic charitable contributions, today's bonyads monopolize Iranian import-export concerns and major industries including petroleum, automobiles, hotels, and banks.

Bonyad conglomerates account for a substantial percentage of Iran's gross national product. Individual bonyads such as Imman Reza Foundation and the Martyrs' Foundation have billions of dollars in assets. Mullahs direct the bonyad foundations. Given the low rate of capital accumulation in the Iranian economy, the foundations constitute one of the few governmental institutions for internal economic investment. Reportedly, the bonyads stifle entrepreneurs not affiliated with them due to the bonyads' favored status, which includes exemption from taxes, the granting of favorable exchange rates, and lack of accounting oversight by the Iranian government. Bonyads have been involved in funding terrorist organizations and serving as fronts for the procurement of nuclear capacity and prohibited weapons and technology.

On October 25, 2007, the United States designated Iran's IRGC, the armed guardians of Iran's theocracy, as a proliferator of weapons of mass destruction. The elite Quds Force was included in the designation as a supporter of terrorism. The Revolutionary Guard's suspect financing is entwined with Iran's economy. The Revolutionary Guard is involved with more than 100 companies and manages billions of dollars in business. Similar to bonyads, the military/business conglomerate uses high-level political connections, no-bid contracts, and squeezes out competitors. Corruption is widespread throughout Iranian society; at the highest levels of government, favored individuals and families benefit from "baksheesh" deals. Iran is ranked 131 out of 179 countries listed in Transparency International's 2007 Corruption Perception Index. Despite some limited attempts at reforming bonyads and other entities, there has been little transparency or substantive progress.

Iran is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Iran has signed but not ratified the UN Convention against Corruption. It has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Iran should engage with the FATF and construct and implement a viable anti-money laundering and terrorist finance regime that adheres to international standards. Iran should be more active in countering regional smuggling. Iran should implement meaningful reforms in bonyads that promote transparency and accountability. Iran should create an anti-corruption law with strict penalties and enforcement, applying it equally to figures with close ties to the government and the clerical communities. It should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Iran should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Iran should refrain from supporting terrorism or the funding of terrorism.

Iraq

Iraq's economy is primarily cash-based, and there is little data available on the extent of money laundering. However, cross-border smuggling is widespread, including the smuggling of bulk cash. Iraq is a major market for smuggled cigarettes and counterfeit goods, and money is laundered through intellectual property right violations. There is a large market for stolen cars from Europe and the United States. Ransoms generated from kidnapping generate tens of millions of dollars every year. Kidnappings are linked to human exploitation and terrorist finance. Iraq is a source country for human trafficking. Trade-based money laundering, customs fraud, and value transfer are found in the underground economy and are commonly used in informal value transfer systems such as hawala. Hawala networks are prevalent and are widely used in Iraq and the region. Cash, trade-based money laundering, and hawala are all components of terrorist and insurgent finance found in Iraq. In early 2006, the Iraqi oil ministry estimated that ten percent of the $4 billion to $5 billion in fuel imported for public consumption at subsidized rates in 2005 was smuggled internally and out of the country for resale at market rates. Large amounts of Iraqi oil are smuggled to Iran and other Gulf countries through routes established by Saddam Hussein when Iraq was under sanctions in the 1990s. The

organized smuggling rings siphon oil from pipelines, and load it onto tanker trucks that carry the oil to small boats in the Persian Gulf. Corrupt officials facilitate the smuggling by issuing certificates and permits that allow the smugglers to pass through security checkpoints. Moreover, it is reported that approximately ten percent of all oil smuggling profits are going to insurgents. Subsidy scams and black market sales also exist for gasoline, kerosene, and cooking fuel. Corruption is a severe problem that permeates society and commerce and is also found at the highest levels of government, and large public and private institutions. Transparency International's 2007 International Corruption Perception Index ranked Iraq 178 of 180 countries surveyed. The formal financial sector is growing and at least ten new banks, both domestic and international, have been licensed to operate in Iraq. The two largest state-owned banks control at least 90 percent of the banking sector.

The Coalition Provisional Authority (CPA), the international body that governed Iraq beginning in April 2003, issued regulations and orders that carried the weight of law in Iraq. The CPA ceased to exist in June 2004, at which time the Iraqi Interim Government assumed authority for governing Iraq. Drafted and agreed to by Iraqi leaders, the Transitional Administrative Law (TAL) described the powers of the Iraqi government during the transition period. Under TAL Article 26, regulations and orders issued by the CPA pursuant to its authority under international law remain in force until rescinded or amended by legislation duly enacted and having the force of law. The constitution, which was ratified in October 2005, also provides for the continuation of existing laws, including CPA regulations and orders that govern money laundering.

The CPA Order No. 93, "Anti-Money Laundering Act of 2004" (AMLA) governs financial institutions in connection with: money laundering, financing of crime, financing terrorism, and the vigilance required of financial institutions in regard to financial transactions. The law also criminalizes money laundering, financing crime (including the financing of terrorism), and structuring transactions to avoid legal requirements. The AMLA covers: banks; investment funds; securities dealers; insurance entities; money transmitters and foreign currency exchange dealers, as well as persons who deal in financial instruments, precious metals or gems; and persons who undertake hawala transactions. Covered entities are required to verify the identity of any customer opening an account for any amount. Covered entities are also required to verify the identity of nonaccount holders performing a transaction or series of potentially related transactions whose value is equal to or greater than five million Iraqi dinars (approximately U.S. $4,125). Beneficial owners must be identified upon account opening or for transactions exceeding ten million Iraqi dinar (approximately U.S. $8,250). Records must be maintained for at least five years. Covered entities must report suspicious transactions and wait for guidance before proceeding with the transaction; the relevant funds are frozen until guidance is received. Suspicious transaction reports (STRs) are to be completed for any transaction over four million Iraqi dinars (approximately U.S. $3,300) that is believed to involve funds that are derived from illegal activities or money laundering, intended for the financing of crime (including terrorism), or over which a criminal organization has disposal power, or a transaction conducted to evade any law and which has no apparent business or other lawful purpose. The "tipping off" of customers by bank employees where a transaction has generated a suspicious transaction report is prohibited. Bank employees are protected from liability for cooperating with the government. Willful violations of the reporting requirement may result in imprisonment or fines.

CPA Order No. 94, "Banking Law of 2004," gives the Central Bank of Iraq (CBI) the authority to license banks and to conduct due diligence on proposed bank management. Order No. 94 establishes requirements for bank capital, confidentiality of records, audit and reporting requirements for banks, and prudential standards. The CBI is responsible for the supervision of financial institutions. The CBI was mandated by the AMLA to issue regulations and require financial institutions to provide employee training, appoint compliance officers, develop internal procedures and controls to deter money laundering, and establish an independent audit function. The CBI has branches in Irbil, Sulimeniyah, Dahuk (which are located in the Northern Kurdistan Region of Iraq) and Basra. The CBI

also houses Iraq's financial intelligence unit, the Money Laundering Reporting Office (MLRO). The CBI branches are responsible for licensing and examining private and public banks, and money exchangers and transmitters. The CBI branches are required to conduct periodic examinations of the banks. For public banks this occurs every six months and every three months for private banks. Order No. 94 gives administrative enforcement authority to the CBI, up to and including the removal of institution management and revocation of bank licenses. While the banks are ostensibly providing traditional banking services such as lending to the community in practice, they collect funds and send excess reserves to the CBI in Baghdad where they receive an 18 to 20 per cent return. There is no time limit for reserves to be held in the CBI for accrual of interest. Outside of this relationship, there is poor communication with the CBI, particularly with respect to money laundering, terrorist financing and other potential risks.

One of the most significant challenges facing the CBI is the lack of communication both among its branches and between the branches and the CBI in Baghdad. There is a general lack of modern banking technology, in particular a lack of an electronic payment system and wire transfer capability. As the financial sector is relatively new, there is little institutional knowledge with respect to anti-money laundering/counterterrorist finance (AML/CTF) issues. Another challenge confronting the CBI, is the lack of trust, confidence, and modernization in the formal financial sector due to the history of misuse and abuses of the sector during the Saddam Hussein regime

Bulk cash smuggling is a major problem in Iraq. The CBI is considering issuance of regulations to require large currency transaction reports for the cross-border transport of currency of more than 15 million Iraqi dinars (approximately U.S. $12.380). Neither Iraqis nor foreigners are permitted to transport more than U.S. $10,000 in currency when exiting Iraq.

An additional vulnerability to Iraq's AML/CTF regime is that money exchanges and money transmitters are largely unregulated. Although they are required to be licensed, the level of supervision is nominal. Money exchanges are not subject to the same examination process as banks nor are they required to report suspicious transactions. The current training given to managers and operators of money exchanges and money transmitters on AML/CTF and banking examination practices is inadequate. The MLRO, which in other circumstances could assist in the training and monitoring for AML/CTF, is not developed enough yet to execute its core mission and also suffers from a lack of communication with CBI branches outside of Baghdad. Most transactions, foreign exchange operations, and money remittances take place through such money transmitter businesses and not through the banking sector. Most international remittances are done via related offices in Amman or Dubai. While simple funds transfers can take weeks to accomplish through the banking sector, the same transactions can be done very rapidly and far more effectively through money exchange and transfer services.

Although financial institutions are required to report suspicious transactions including potential money laundering and terrorist financing under the Anti-money Laundering Ordinance, in practice they do not do so, due to the isolation of the MLRO and a lack of training and technology. The MLRO was formed in June/July 2006 and has a small but dedicated staff. The CBI and representatives from the United States are working together to build the MLRO's capacity and implement the day-to-day functions of a financial intelligence unit (FIU). The MLRO operates independently to collect, analyze and disseminate information on financial transactions subject to financial monitoring and reporting, including suspicious activity reports. The MLRO is also empowered to exchange information with other Iraqi or foreign government agencies. The CBI and its MLRO finalized implementing regulations to the AMLA, which became effective September 15, 2006.

The predicate offenses for the crimes of money laundering and the financing of crime are quite broad and extend beyond "all serious offenses" to include "some form of unlawful activity." The penalties for violating the AMLA depend on the specific nature of the underlying criminal activity. For

example, "money laundering" is punishable by a fine of up to 40 million dinar (approximately U.S. $33,000) or twice the value of the property involved in the transaction (whichever is greater) or imprisonment of up to four years or both. Other offenses for which there are specific penalties include the financing of crime with a fine of up to 20 million dinar (approximately U.S. $16,510) or two years imprisonment or both and structuring transactions of up to 10 million dinar (approximately U.S. $8,250) or one year imprisonment or both. No arrests or prosecutions under the AMLA have been reported to date.

The AMLA includes provisions for the forfeiture of any property. Such property includes, but is not limited to, funds involved in a covered offense, or any property traceable to the property, or any property gained as a result of such an offense, without prejudicing the rights of bona fide third parties. The courts can order confiscation of property, but it appears they can only do so if the property is directly related to the crime, including drug proceeds. According to the Iraqi Penal Code, a person must pay the government back for any property stolen from the government. In other cases of theft, restitution is made to the victim(s). Any property forfeited to the state becomes state property and goes into the general treasury. Should the government confiscate perishables, it can sell them while the case is on-going and if the defendant is acquitted, the government returns the money it realized from the sale of the goods to the defendant. While the case is on going, the government appoints a judicial guardian to supervise and maintain the property pending the outcome of the case. The AMLA also blocks any funds or assets, other than real property (which is covered by a separate regulation), belonging to members of the former Iraqi regime and authorizes the Minister of Finance to confiscate such assets following a judicial or administrative order. The lack of automation or infrastructure in the banking sector, however, hinders the government's ability to identify and freeze assets linked to illicit activity.

Iraq has free trade zones in Basra/Khor al-Zubair, Ninewa/Falafel, Sulaymaniyah, and Al-Quaymen. Under the Free Zone (FZ) Authority Law, goods imported and exported from the FZ are generally exempt from all taxes and duties, unless the goods are imported into Iraq. Additionally, capital, profits, and investment income from projects in the FZ are exempt from taxes and fees throughout the life of the project, including in the foundation and construction phases.

The CBI is also mandated by the AMLA to distribute the UN 1267 Sanction Committee's consolidated list of suspected terrorists or terrorist organizations. No asset freezes pertaining to any names on the consolidated list have been reported to date.

Iraq became a member of the Middle East and North Africa Financial Action Task Force (MENAFATF) in September 2005. Iraq is a party to the 1988 UN Drug Convention, but not the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, or the UN Convention against Corruption.

The Government of Iraq continues to lay the foundation for anti-money laundering and counterterrorist finance regimes. In these efforts, there is strong cooperation with the U.S. Government. However, there is much work ahead. While Iraq's economy is primarily cash-based, this is likely to change as the expected development of the energy sector will increase the need for the development of a formal financial sector that is integrated into the international payment system. Concurrently, the financial sector must adopt AML/CTF standards and practices. Iraq should take a more active part in MENAFATF and in implementing its recommendations. As independent foreign banks become more interested in opening branches in Iraq, the CBI should be cautious in granting licenses to banks from jurisdictions of concern. Iraq should continue its efforts to build capacity and actively implement the provisions of the AMLA and related authorities. As a priority, as Iraq's MLRO becomes fully functional, it should develop increased capacity to investigate financial crimes and enforce the provisions of the AMLA. Iraqi law enforcement, border authorities, and customs service should strengthen border enforcement and identify and pursue smuggling and trade-based money

laundering networks. Increased border enforcement is also a prerequisite in combating terrorist finance. The Government of Iraq should also take concerted steps to combat the corruption that hinders development and impedes an effective anti-money laundering and counter-terrorist finance regime. Iraq should become a party to the UN Convention against Corruption, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Ireland

Ireland is an increasingly significant European financial hub. Narcotics-trafficking, fraud, and tax offenses are the primary sources of funds laundered in Ireland. Money laundering occurs in credit institutions, although launderers have also made use of money remittance companies, solicitors, accountants, and second-hand car dealerships. The most common laundering methods are: the purchase of high-value goods for cash; the use of credit institutions to receive and transfer funds in and out of Ireland; the use of complex company structures to filter funds; and the purchase of properties in Ireland and abroad.

The Shannon Free Zone was established in 1960 as a free trade zone, offering investment incentives for multinational companies. The Shannon Free Zone is supervised by "Shannon Development," a government-founded body. Reportedly, there are no indications that the Shannon Free Zone is being used in trade-based money laundering (TBML) schemes or by financiers of terrorism. The international banking and financial services sector is concentrated in Dublin's International Financial Services Centre (IFSC). In 2007, there were approximately 440 international financial institutions and companies operating in the IFSC. Services offered include banking, fiscal management, re-insurance, fund administration, and foreign exchange dealing. Although there are no tax benefits for companies in the IFSC, Ireland offers the lowest corporate tax rate (12.5 percent) in the EU. Casinos, including Internet casinos, are illegal in Ireland. Private gaming clubs, however, operate casino-like facilities that fall outside the scope of the law.

Ireland criminalized money laundering relating to narcotics trafficking and all indictable offenses under the 1994 Criminal Justice Act. The law requires financial institutions (banks, building societies, the Post Office, stock brokers, credit unions, bureaux de change, life insurance companies, and insurance brokers) to report suspicious transactions. There is no monetary threshold for reporting suspicious transactions. The obliged entities submit suspicious transaction reports (STRs) to the Garda (Irish Police) Bureau of Fraud Investigation, Ireland's financial intelligence unit (FIU), and to the Revenue (Tax) Department in addition to the FIU, as required by law. Reporting entities must submit the STR before the suspicious transaction is finalized. There are no other legal requirements governing the time period within which an STR must be filed. Financial institutions must implement customer identification procedures and retain records of financial transactions. Ireland has amended its Anti-Money Laundering (AML) law to extend customer identification and suspicious transaction reporting requirements to lawyers, accountants, auditors, real estate agents, auctioneers, and dealers in high-value goods. Ireland's Customer Due Diligence procedure requires designated entities to take measures to identify customers when opening new accounts or conducting transactions exceeding 13,000 euros (approximately U.S. $19,000). These requirements do not extend to existing customers prior to May 1995 except in cases where authorities suspect that money laundering or another financial crime is involved.

The Corporate Law requires that every company applying for registration in Ireland must demonstrate that it intends to carry on an activity in the country. Companies must maintain an Irish resident director at all times, or post a bond as a surety for failure to comply with the appropriate company law. In addition, the law limits the number of directorships that any one person can hold to 25, with certain exemptions. This limitation aims to curb the use of nominee directors as a means of disguising

beneficial ownership or control. The Company Law Enforcement Act 2001 (Company Act) established the Office of the Director of Corporate Enforcement (ODCE). The ODCE investigates and enforces provisions of the Company Act. Under the law, a company must provide the names of its directors. The ODCE has the authority to uncover a company's beneficial ownership and control. The Company Act also creates a mandatory reporting obligation for auditors suspicious of breaches of company law to the ODCE. In 2006, the ODCE secured the conviction of 31 company directors and other individuals on 41 charges for breaching various requirements of the Company Act. An additional 17 company officers were disqualified from eligibility for a lead position in companies for periods ranging from one to 10 years.

EU Regulation 1889/2005, introduced in Ireland on June 15, 2007, requires travelers transporting more than 10,000 euros (approximately U.S. $14,600) into or out of the EU to declare these funds. The declarations are automatically reported to the FIU. Customs authorities also require reports detailing movements of precious metals and stones into or out of the EU when Ireland is the initial entry or final exit point. The FIU will have access to these reports.

The Third EU Money Laundering Directive entered into force in December 2005 and was transposed into Irish law prior to the December 2007 deadline. The Government of Ireland (GOI) is likely to implement new legislation to address customer due diligence, the identification of beneficial owners, politically exposed persons, and the designation of trusts. A Mutual Evaluation conducted in 2005 by the Financial Action Task Force (FATF), published in 2006, noted that Ireland's money laundering definition met the FATF requirements. The mutual evaluation report (MER) acknowledged that Ireland achieved a high standing in AML legal structures and international cooperation, although the number of money laundering prosecutions and convictions was low.

The Irish Financial Services Regulatory Authority (IFSRA), the financial regulator, is a component of the Central Bank and Financial Services Authority of Ireland (CBFSAI) and is responsible for supervising the financial institutions for compliance with money laundering procedures. IFSRA is obliged to report any suspected breaches of the Criminal Justice Act 1994 by the institutions it supervises to the FIU and the Revenue Commissioners. Reports cover suspicion of money laundering and terrorist financing, failure to establish identity of customers, failure to retain evidence of identification, and failure to adopt measures to prevent and detect the commission of a money laundering offense. IFSRA also regulates the IFSC companies that conduct banking, insurance, and fund transactions.

Ireland's FIU receives and analyzes financial disclosures, and disseminates them for investigation. The MER found that although Ireland's FIU met the requirements of the FATF methodology it had limited technical and human resources to manage and evaluate STRs effectively. In 2006, the FIU received 10,403 STRs. Three people were convicted for money laundering. Information regarding the number of STRs received in 2007 is not yet available. A conviction on charges of money laundering carries a maximum penalty of 14 years' imprisonment and an unlimited fine. The lengthiest penalty applied for a money laundering conviction to date has been six years.

Ireland estimates that up to 80 percent of STRs may involve tax violations. Value Added Tax (VAT) Intra-Community Missing Trader Fraud is extensive within the EU, and attacks the VAT system, in which criminals obtain VAT registration to acquire goods VAT free from other Member States. They then sell on the goods at VAT inclusive prices and disappear without remitting the VAT paid by their customers to the tax authorities. There is evidence in several fraud investigations that conduit traders involved in the supply chain have established themselves in Ireland.

The Criminal Assets Bureau (CAB), authorized to confiscate the proceeds of crime in cases where there is no criminal conviction, reports to the Minister for Justice and includes experts from the Garda, Tax, Customs, and Social Security Agencies. Under the 1996 Proceeds of Crime Act, authorities may freeze specified property valued in excess of 13,000 euros (approximately U.S. $19,000) for seven

years, unless the court is satisfied that all or part of the property is not criminal proceeds. With the consent of the High Court and the parties concerned, the authorities have the power to dispose of assets without having to wait the seven years. As of November 2007, the authorities have executed 14 such consent orders. This Act also allows the authorities to take foreign criminality into account in assessing whether assets are the proceeds of criminal conduct. Under certain circumstances, the High Court can freeze, and, where appropriate, seize the proceeds of crimes.

In 2006, CAB obtained interim and disposal orders on assets valued at approximately 6.8 million euros (approximately U.S. $10 million). The CAB has the authority to cooperate with agencies in other jurisdictions, which strengthens Irish cooperation with asset recovery agencies in the United Kingdom.

With the Criminal Justice (Terrorism Offenses) Act, Ireland's legislation comports with United Nations Conventions and European Union Framework decisions on combating terrorism. The IFSRA works with the Department of Finance to draft guidance for regulated institutions on combating and preventing terrorist financing. The authorities revised and issued the guidance to institutions upon the passage of the Criminal Justice Act in 2005.

To date, there have been no prosecutions for terrorism offenses under the Criminal Justice Act. The FATF MER noted that the Act neglects to criminalize funding of either a terrorist acting alone or two terrorists acting in concert. The MER also noted inadequate implementation of UN Security Council Resolution (UNSCR) 1373, in that Ireland relies exclusively on an EU listing system without subsidiary mechanisms to deal with terrorists on the list who are European citizens (EU Regulations do not apply for freezing purposes to such persons) or with persons designated as terrorists by other jurisdictions who are not on the EU list.

The Criminal Justice (Terrorism Offenses) Act imposes evidentiary requirements obstructing Ireland from fulfilling its UNSCR 1373 obligation to freeze all funds and assets of individuals who commit terrorist acts whether or not there is evidence that those particular funds are intended for use in terrorist acts. The Garda can apply to the courts to freeze assets when certain evidentiary requirements are met. From 2001 through 2007, Ireland had reported to the European Commission the names of five individuals who maintained a total of seven accounts that were frozen in accordance with the provisions of the European Union's (EU) Anti-Terrorist Legislation. No designated individuals or entities have surfaced in Ireland's system since 2004. The aggregate value of the funds frozen was approximately U.S. $6,400.

In July 2005, the United States and Ireland signed instruments on extradition and mutual legal assistance as part of a sequence of bilateral agreements that the United States is concluding with all 25 EU Member States. The instruments supplement and update the 1983 U.S.-Ireland extradition treaty and the 2001 bilateral treaty on mutual legal assistance (MLAT). The 2005 instrument also provides for searches of suspect foreign located bank accounts, joint investigative teams, and testimony by video-link. The 1983 extradition treaty between Ireland and the U.S. is in force, but as of November 2007, the GOI has not completed the ratification process for the 2001 MLAT. In November 2006, for the first time in eighteen extradition requests, Ireland extradited a U.S. citizen.

Ireland is a member of the FATF, and its FIU is a member of the Egmont Group. Ireland is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. It has signed, but not ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

The GOI should enact legislation to prohibit the establishment of "shell" companies. Law enforcement should have a stronger role in identifying the true beneficial owners of shell companies as well as of trusts in the course of investigations. Ireland should increase the technical and human resources provided to the FIU to manage and evaluate STRs effectively. The GOI should enact legislation that

covers both funding of a terrorist acting alone and funding of two terrorists acting in concert, as well as legislation fully implementing UNSCR 1373. To this end, Ireland should remove the evidentiary requirements acting as obstacles to full compliance, as well as circulate the UN and the U.S. lists to its regulators and obligated entities. Ireland should continue implementation of its new anti-terrorism legislation and its AML law amendments, and ensure stringent enforcement of all such initiatives. Ireland should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Isle of Man

The Isle of Man (IOM) is a Crown Dependency of the United Kingdom with its own parliament, government, and laws. Its large and sophisticated financial center is potentially vulnerable to money laundering at the layering and integration stages. Most of the illicit funds in the IOM are from fraud schemes and narcotics trafficking in other jurisdictions, including the United Kingdom. The U.S. dollar is the most common currency used for criminal activity in the IOM. Identity theft and Internet abuse are growing segments of financial crime activity.

No current data regarding the entities that comprise the IOM financial industry has been reported. As of September 30, 2004, the IOM's financial industry consisted of approximately 19 life insurance companies, 25 insurance managers, more than 177 captive insurance companies, 53 licensed banks and two licensed building societies, 82 investment business license holders, 30.1 billion pounds (approximately U.S. $59 billion) in bank deposits, and 164 collective investment schemes with 6.5 billion pounds (approximately U.S. $12.7 billion) of funds under management. There were also 171 licensed corporate service providers.

The IOM criminalized money laundering related to narcotics trafficking in 1987. The Criminal Justice (Money Laundering Offenses) Act 1998, extends the definition of money laundering to cover all serious crimes and led to the creation of the Anti-Money Laundering (AML) Code, which came into force in December 1998. The AML Code has subsequently been replaced by the Criminal Justice (Money Laundering) Code 2007 (the Code), enacted in September 2007. Requirements under the 2007 Code apply to banking, investment, and collective investment schemes, fiduciary services business, insurance, building societies, credit unions, local authorities authorized to raise or borrow money, bureaux de change, estate agents, bookmakers and casinos (excluding online gambling), accountants, notaries and legal practitioners, insurance intermediaries, retirement benefits schemes, administrators and trustees, auditors, the Post Office, and any activity involving money transmission services or check encashment facilities.

The Code requires that obligated entities implement AML policies, procedures, and practices, including employing them for countering terrorist financing. The Code mandates that obligated entities institute procedures to establish customer identification requirements; report suspicious transactions; maintain adequate records; adopt adequate internal controls and communication procedures; provide appropriate training for employees; and establish internal reporting protocols. There is no minimum threshold for obliged entities to file a suspicious transaction report (STR), and safe harbor provisions in the law protect reporting individuals when they file an STR. It is an offense to fail to disclose suspicion of money laundering for all predicate crimes. Failure to comply with the requirements of the Code may bring a fine, imprisonment of up to two years, or both.

The Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA) regulate the IOM financial sector. The IPA regulates insurance companies, insurance management companies, general insurance intermediaries, and retirement benefit schemes and their administrators. The FSC is responsible for the licensing, authorization, and supervision of banks, building societies, investment businesses, collective investment schemes, corporate service providers, and companies. The FSC also maintains the Company Registry Database for the IOM, which contains company records dating back

to the first company incorporated in 1865. Statutory documents filed by IOM companies can now be searched and purchased online through the FSC's website.

As IOM's companion to the AML Code, the FSC has AML Guidance Notes (AMLGN), which the FSC rewrote in 2007. The new guidance reflects evolving international standards, new legislation on the Island, and the new licensee status of Corporate Service Providers and Trust Service Providers. In 2008, the FSC will release the new revised guidance as an "Anti-Money Laundering and the Financing of Terrorism Handbook."

The FSC has worked with its counterparts from the Crown Dependencies of Guernsey and Jersey. One of these initiatives was a consultation paper called Overriding Principles for a Revised Know Your Customer (KYC) Framework, to develop a more coordinated AML approach. Work between the Crown Dependencies is continuing, to develop a coordinated strategy on money laundering, and to ensure maximum compliance with the revised Financial Action Task Force (FATF) Forty Recommendations on Money Laundering.

Money service businesses (MSBs) not already regulated by the FSC or IPA must register with Customs and Excise. With this, the IOM implemented the first two EU Directives on Money Laundering, and provides for their supervision by Customs and Excise to ensure compliance with the AML Code. In December 2007, the FSC issued a Consultative Paper on the Proposed Regulation of MSBs, including electronic money (e-money) providers. This document will assist the Island in meeting the standards set by the Financial Action Task Force ("FATF") 40 Recommendations and Nine Special Recommendations on Terrorist Financing. The paper also airs proposals to bring money MSBs and e-money providers under some form of regulation, which would initially be limited.

The IPA, as regulator of the IOM's insurance and pensions business, issues Anti-Money Laundering Standards for Insurance Businesses (the "Standards"). The Standards are binding upon the industry and include "Overriding Principles" requiring all insurance businesses to check their businesses to determine that they have sufficient information available to prove customer identity. The current set of Standards became effective March 31, 2003. The IPA conducts on-site visits to examine procedures and policies of companies under its supervision.

The Online Gambling Regulation Act 2001 and an accompanying AML (Online Gambling) Code 2002 are supplemented by AML guidance notes issued by the Gambling Control Commission, a regulatory body which provides guidance on the prevention of money laundering in the online gaming sector. The Online Gambling legislation, unique to the gaming industry when it passed, brought regulation to an unregulated gaming environment. The revised version of the Online Gambling and Peer to Peer Gambling AML Code came into force in 2006.

The Companies, Etc. (Amendment) Act 2003 provides for additional supervision for all licensable businesses, e.g., banking, investment, insurance, and corporate service providers. The act abolished future bearer shares after April 1, 2004, and mandates that all existing bearer shares be registered before the bearer can exercise any rights relating to the shares.

The Financial Crime Unit (FCU), under the Department of Home Affairs, the intelligence financial unit (FIU) of the Isle of Man, was formed in April 2000 and evolved from the police Fraud Squad. It is the central point for the collection, analysis, investigation, and dissemination of suspicious transaction reports (STRs) from obligated entities. The FCU's work is broadly split between financial intelligence, legal co-operation with other jurisdictions in terms of financial investigation, and local financial crime investigation involving serious or complex cases. It is comprised of Police and Customs Officers, Police Support Staff, and other government departments such as Internal Audit and HM Attorney General's Chambers. The FIU has access to Customs, police, and tax information. The FIU disseminates STRs to the Customs, Tax Administrators, FSC, and the IPA. The FCU is responsible for investigating financial crimes and terrorist financing cases. The FIU received approximately 1,574

suspicious transaction reports in 2007, and 1,653 STRs in 2006. Approximately 45 percent of the STRs are disseminated to the United Kingdom, five percent to other European countries, and seven percent to nonEuropean countries (mainly the U.S.). IOM authorities charged eight people with money laundering offenses in 2007, and investigations are proceeding. Six of the eight have been charged in relation to narcotics, and two to fraud, including wire fraud. In 2006, IOM authorities obtained one conviction for money laundering.

IOM legislation provides powers to constables, including customs officers, to investigate whether a person has benefited from any criminal conduct. These powers allow information to be obtained about that person's financial affairs. These powers can be used to assist in criminal investigations abroad as well as in the IOM. The Customs and Excise (Amendment) Act 2001 gives various law enforcement and statutory bodies within the IOM the ability to exchange information, where such information would assist them in discharging their functions. The Act also permits Customs and Excise to release information it holds to any agency within or outside the IOM for the purposes of any criminal investigation and proceeding. Such exchanges can be either spontaneous or by request.

The Criminal Justice Acts of 1990 and 1991, as amended, extend the power to freeze and confiscate assets to a wider range of crimes, increase the penalties for a breach of money laundering codes, and repeal the requirement for the Attorney General's consent prior to disclosure of certain information. The law also lowers the standard for seizing cash from "reasonable grounds" to believe that it was related to drug or terrorism crimes to a "suspicion" of any criminal conduct. Assistance by way of restraint and confiscation of a defendant's assets is available under the 1990 Act to all countries and territories designated by Order under the Act. Assistance is also available under the 1991 Act to all countries and territories in the form of the provision of evidence for the purposes of criminal investigations and proceedings. The availability of such assistance is not convention-based nor does it require reciprocity.

All charities operating within the IOM are registered and supervised by the Charities Commission.

The Prevention of Terrorism Act 1990 made it an offense to contribute to terrorist organizations or to assist a terrorist organization in the retention or control of terrorist funds. The IOM Terrorism (United Nations Measure) Order 2001 implements UNSCR 1373 by providing for the freezing of terrorist funds, as well as by criminalizing the facilitating or financing of terrorism. The Government of the IOM enacted the Anti-Terrorism and Crime Act, 2003, which enhances reporting by making the failure to report suspicious transactions relating to money intended to finance terrorism an offense. All other UN and EU financial sanctions have been adopted or applied in the IOM, and are administered by Customs and Excise. Institutions are obliged to freeze affected funds and report the facts to Customs and Excise. In December 2001, the FSC issued revised AML guidance notes that include information relevant to terrorism. IOM authorities are reviewing additional amendments that will incorporate the most recent FATF recommendations and EU directives.

The IOM has developed a legal and constitutional framework for combating money laundering and the financing of terrorism. In 2003, the International Monetary Fund (IMF) examined the regulation and supervision of the IOM's financial sector and found that "the financial regulatory and supervisory system of the Isle of Man complies well with the assessed international standards."

Application of the 1988 UN Drug Convention was extended to the IOM in 1993. In 2003, the U.S. and the UK agreed to extend to the Isle of Man the U.S.-UK Treaty on Mutual Legal Assistance in Criminal Matters.

The IOM cooperates with international anti-money laundering authorities on regulatory and criminal matters. Under the 1990 Criminal Justice Act, the provision of documents and information is available to all countries and territories for the purposes of investigations into serious or complex fraud. Similar assistance is also available to all countries and territories in relation to drug-trafficking and terrorist

investigations. All decisions for assistance are made by the Attorney General of the IOM on a case-by-case basis, depending on the circumstances of the inquiry.

In October 2007, the IOM signed tax information exchange agreements (TIEAs) with each member of the Nordic Council (Denmark, the Faroe Islands, Finland, Greenland, Iceland, Norway, and Sweden) and received commendation from the Organization for Economic Co-operation and Development for its commitment to international standards. The IOM has a fully operational TIEA with the United States and has established protocols with the Internal Revenue Service (IRS) to ensure that information exchange requests are handled smoothly.

Although not a member of the FATF, the Island fully endorses FATF 40 Recommendations and Nine Special Recommendations. The IOM's experts are assisting the FATF working group that considers matters relating to customer identification and companies' issues. The IOM is a member of the Offshore Group of Banking Supervisors (OGBS) and Offshore Group of Insurance Supervisors (OGIS). The FCU belongs to the Egmont Group.

Isle of Man officials should continue to support and educate the local financial sector to help it combat current trends in money laundering. The IOM should act on the 2007 Consultative paper with the MSB/e-money regulation proposals that authorities have discussed, and implement the most effective. The IOM should also ensure that the obliged entities understand and respond to their new and revised responsibilities as delineated by the 2007 AML Code. To this end, the FSC should work to release the Anti-Money Laundering and Terrorist Financing Handbook as soon as possible in 2008. The authorities also should continue to work with international AML authorities to deter financial crime and the financing of terrorism and terrorists.

Israel

Among its Mediterranean neighbors, Israel stands out economically in terms of its high GDP, per capita income, developed financial markets and diverse capital markets. Nevertheless, Israel is not regarded as a regional financial center. It primarily conducts financial activity with the financial markets of the United States and Europe, and to a lesser extent with the Far East. Israeli National Police (INP) intelligence identifies illicit drugs, gambling, extortion, and fraud as the predicate offenses most closely associated with organized criminal activity. Recent studies conducted by the INP Research Department estimate illegal gambling profits at U.S. $2-3 billion per year and domestic narcotics profits at U.S. $1.5 billion per year. Human trafficking is considered the crime-for-profit with the greatest human toll in Israel, and public corruption the crime with the greatest social toll. As such, these areas are the targets of the most vigorous anti-money laundering (AML) enforcement activity. Israel does not have free trade zones and is not considered an offshore financial center, as offshore banks and other forms of exempt or shell companies are not permitted. Bearer shares, however, are permitted for banks and/or for companies.

In August 2000, Israel enacted its anti-money laundering legislation, the "Prohibition on Money Laundering Law" (PMLL), (Law No. 5760-2000). The PMLL established a framework for an anti-money laundering system, but required the passage of several implementing regulations before the law could fully take effect. Among other things, the PMLL criminalized money laundering and included 18 serious crimes, in addition to offenses described in the prevention of terrorism ordinance, as predicate offenses for money laundering even if committed in a foreign jurisdiction.

The PMLL also provided for the establishment of the Israeli Money Laundering Prohibition Authority (IMPA) under the Ministry of Justice, as the country's financial intelligence unit (FIU). IMPA became operational in 2002. The PMLL requires financial institutions to report "unusual transactions" to IMPA as soon as possible under the circumstances. Financial institutions must report all transactions that exceed a minimum threshold that varies based on the relevant sectors and the risks that may arise,

with more stringent requirements for transactions originating in a high-risk country or territory. IMPA has access to population registration databases, the Real-Estate Database, records of inspections at border crossings, court files, and Israel's Company Registrar.

In 2001, Israel adopted the Banking Corporations Requirement Regarding Identification, Reporting, and Record Keeping Order. The Order establishes specific procedures for banks with respect to customer identification, record keeping, and the reporting of irregular and suspicious transactions in keeping with the recommendations of the Basel Committee on Banking Supervision. The Supervisor of Banks at the Bank of Israel monitors compliance among banking institutions. Bankers and others are protected by law with respect to their cooperation with law enforcement entities.

Subsequent regulations established the methods of reporting to the Customs Authority (a part of the Israel Tax Authority) monies brought in or out of Israel, and criteria for financial sanctions for violating the law, as well as for appeals. The regulations require the declaration of currency transferred (including cash, travelers' checks, and banker checks) into or out of Israel for sums above 80,000 new Israeli shekels (NIS) (approximately U.S. $20,000). This applies to any person entering or leaving Israel, and to any person bringing or taking money into or out of Israel by mail or any other methods, including cash couriers. Failure to comply is punishable by up to six months imprisonment or a fine of NIS 202,000 (approximately $50,500), or ten times the amount that was not declared, whichever is higher. Alternatively, an administrative sanction of NIS 101,000 (approximately U.S. $25,250), or five times the amount that was not declared, may be imposed by the Committee for Imposition of Financial Sanctions. In 2003, the Government of Israel (GOI) lowered the threshold for reporting cash transaction reports (CTRs) to NIS 50,000 (approximately U.S. $12,250), lowered the document retention threshold to NIS 10,000 (approximately U.S. $2,500), and imposed more stringent reporting requirements.

Clarifications to the PMLL were approved in Orders 5761-2001 and 5762-2002 requiring that suspicious transactions be reported by members of the stock exchange, portfolio managers, insurers or insurance agents, provident funds and companies managing a provident fund, providers of currency services, and the Postal Bank. Portfolio managers and members of the stock exchange are supervised by the Chairman of the Israel Securities Authority; insurers and insurance agents are under the authority of the Superintendent of Insurance in the Ministry of Finance; provident funds and companies managed by a provident fund are overseen by the Commissioner of the Capital Market in the Ministry of Finance, and the Postal Bank is monitored by the Minister of Communications. The PMLL does not apply at this time to intermediaries, such as lawyers and accountants.

Other subsequent changes to the PMLL authorized: the issuance of regulations requiring financial service providers to identify, report, and keep records for specified transactions for seven years; the establishment of a mechanism for customs officials to input into the IMPA database; the creation of regulations stipulating the time and method of bank reporting; the creation of rules on safeguarding the IMPA database; and rules for requesting and transmitting information between IMPA, the INP and the Israel Security Agency (ISA, or Shin Bet). The PMLL also imposed an obligation on financial service providers to report any IMPA activities perceived as unusual.

Order 5762 added money services businesses (MSB) to the list of entities required to file cash transaction reports (CTRs) and suspicious transaction reports (STRs) by size and type, and required that they preserve transaction records for at least seven years. The PMLL mandates the registration of MSBs through the Providers of Currency Services Registrar at the Ministry of Finance. A person engaging in the provision of currency services without being registered is liable to one year of imprisonment or a fine of NIS 600,000 (U.S. $150,000). In 2004, Israeli courts convicted several MSBs for failure to register with the Registrar of Currency Services, and a number of indictments are still pending. The INP and the Financial Service Providers Regulatory Authority maintain a high level

of coordination, routinely exchange information, and have conducted multiple joint enforcement actions.

On July 11, 2007 a draft bill for PMLL (Amendment No. 7) 5776-2007 was published for the purpose of extending Israel's AML regime to the trade in precious stones (including Israel's substantial diamond trading industry). The bill passed the first vote in the Knesset on August 16, and has been submitted to committee for review. The amendment defines "dealers in precious stones" as those merchants whose annual transactions reach NIS 50,000 (approximately U.S. $11,800). It places significant obligations on dealers to verify the identity of their clients, report all transactions above a designated threshold (and all unusual client activity) to IMPA, as well as to maintain all transaction records and client identification for at least five years. The Customs Authority continues to intercept unreported diamond shipments, despite the fact that Israel imposes no tariffs on diamond imports.

In October 2006, the Knesset Committee on Constitution, Law and Justice approved an amendment to the Banking Order and the Regulations on the Prohibition on Financing Terrorism. The Order and Regulations were additional steps in the legislation intended to combat the financing of terrorism while maintaining correspondent and other types of banking relationships between Israeli and Palestinian commercial banks. Although the amendment to the Order and the Regulations impose serious obligations on banks to examine clients and file transaction reports, banks are still exempted from criminal liability if, inter alia, they fulfill all of their obligations under the Order (though they are not protected from civil liability). The Banking Order was expanded to cover the prohibition on financing terrorism and includes obligations to check the identification of parties to a transaction against declared terrorists and terrorist organizations, as well as obligations to report by size and type of transaction. The Banking Order sets the minimum size of a transaction that must be reported at NIS 5,000 (approximately U.S. $1,180) for transactions with a high-risk country or territory. The order also includes examples for unusual financial activity suspected to be related to terrorism, such as transfers from countries with no anti-money laundering or counterterrorist finance (AML/CTF) regime to nonprofit organizations (NGOs) within Israel and the occupied territories.

In 2007, Israel took steps to implement Cabinet Decision 4618, passed on January 1, 2006, by creating an interagency "fusion center" and six interagency task forces for pursuing financial crimes. The regulation explicitly instructs the INP and the Shin Bet to target illicit proceeds as a primary objective in the war on organized crime. As Israel does not have legislation preventing financial service companies from disclosing client and ownership information to bank supervisors and law enforcement authorities, the new regulation establishes conditions for the use of such information to avoid its abuse and to set guidelines for the police and security services.

Israel has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets, as well as assets derived from or intended for other serious crimes, including the funding of terrorism and trafficking in persons. The law also allows for civil forfeiture when ordered by the District Court. The identification and tracing of such assets is part of the ongoing function of the Israeli intelligence authorities and IMPA. The INP has responsibility for seizing assets and the State Attorney's Office has authority to freeze assets. Banking institutions cooperate fully, and often freeze suspicious assets according to guidance from the INP and Ministry of Defense. Israel's International Legal Assistance Law enables Israel to offer full and effective cooperation to authorities in foreign states, including enforcement of foreign forfeiture orders in terror financing cases (both civil and criminal).

In December 2004, the Israeli Parliament adopted the prohibition on terrorist financing law 5765-2004, which is geared to further modernize and enhance Israel's ability to combat terrorist financing and to cooperate with other countries on such matters. The Law went into effect in August 2005, criminalizing the financing of terrorism as required by United Nations Security Council Resolution (UNSCR) 1373. The Israeli legislative regime criminalizing the financing of terrorism includes

provisions of the Defense Regulations State of Emergency/1945, the Prevention of Terrorism Ordinance/1948, the Penal Law/1977, and the PMLL. Under the International Legal Assistance Law of 1998, Israeli courts are empowered to enforce forfeiture orders executed in foreign courts for crimes committed outside Israel.

In December 2007, the Knesset Law Committee approved new regulations enabling the declaration by a ministerial committee of foreign designated terrorists, and legally requiring financial institutions to comply with the foreign designations. The National Security Council legal counsel has responsibility for referring foreign designations to the committee for adoption under Israeli law, and is expected to include entities on the UNSCR 1267 Sanctions Committee consolidated list and entities on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. Once designated, identifying information for the terrorist entity is to be published on the Ministry of Defense website, in two daily newspapers, the Official Gazette of the Israeli Government, and distributed by email to financial institutions. Israel already enforces UNSCR 1267 under its Trade with the Enemy Ordinance of 1939, and regularly notifies financial institutions of restricted entities.

The ISA is responsible for investigating terrorist financing offenses, while the Israel Tax Authority handles investigations originating in customs offenses. Under Israeli law, it is a felony to conceal cash transfers upon entry to the West Bank or Gaza, and the agencies coordinate closely to track funds that enter Israeli ports. Customs and the Ministry of Defense also cooperate in combating trade-based terrorist financing, including goods destined for terrorist entities in the West Bank or Gaza.

The INP reports no indications of an overall increase in financial crime relative to previous years. In 2007, IMPA reported 56 arrests and five prosecutions relating to money laundering and/or terrorist financing. In 2007, IMPA received 10,597 suspicious transaction reports. During this period IMPA disseminated 552 intelligence reports to law enforcement agencies and to foreign FIUs in response to requests, and on its own initiative. In addition, eight different investigations yielded indictments (some of them multiple indictments) and ten resulted in convictions or plea bargains. In 2007, the INP seized approximately U.S. $9 million in suspected criminal assets, a decrease from U.S. $12 million in 2006 and U.S. $75 million seized in 2005.

Israel is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. In December 2006 Israel ratified the UN Convention against Transnational Organized Crime. The IMPA is a member of the Egmont Group, and Israel has been an active observer in MONEYVAL since 2006. Israel has signed but not yet ratified the UN Convention against Corruption. Israel is the only nonmember of the Council of Europe to become a party to the European Convention on Mutual Assistance in Criminal Matters (in 1967) and its Second Additional Protocol (in 2006), which is designed to provide more effective and modern means of assisting member states in law enforcement matters. There is a Mutual Legal Assistance Treaty in force between the United States and Israel, as well as a bilateral mutual assistance agreement in customs matters. Customs, IMPA, the INP and the Israel Securities Agencies routinely exchange information with U.S. agencies through their regional liaison offices, as well as through the Israel Police Liaison Office in Washington. In 2007, Israel provided unprecedented assistance in sharing evidence critical to the prosecution of terrorist financing cases in the United States, allowing for the first time the testimony of intelligence agents in U.S. courts.

The Government of Israel continued to make progress in strengthening its anti-money laundering and terrorist financing regime in 2007. Israel should continue the aggressive investigation of money laundering activity associated with organized criminal operations and syndicates. Israel should also continue its efforts to address the misuse of the international diamond trade to launder money by approving draft legislation. Under the new terrorist financing amendment, Israel should adopt appropriate foreign designations of terrorist entities in a timely manner.

Italy

Italy is fully integrated in the European Union (EU) single market for financial services. Money laundering is a concern both because of the prevalence of homegrown organized crime groups and the recent influx of criminal organizations from abroad, especially from Albania, Romania, Russia, China, and Nigeria.

The heavy involvement in international narcotics trafficking of domestic and Italian-based foreign organized crime groups complicates counternarcotics activities. Italy is both a consumer country and a major transit point for heroin coming from the Near East and Southwest Asia through the Balkans en route to Western/Central Europe and, to a lesser extent, the United States. Italian and ethnic Albanian criminal organizations work together to funnel drugs to Italy and, in many cases, on to third countries. Additional important trafficking groups include other Balkan organized crime entities, as well as Nigerian, Colombian, and other South American trafficking groups.

In addition to the narcotics trade, laundered money originates from a myriad of criminal activities, such as alien smuggling, pirated and counterfeited goods, extortion, and usury. Financial crimes not directly linked to money laundering, such as credit card and Internet fraud, are increasing. Italy is not an offshore financial center.

Money laundering occurs both in the regular banking sector and in the nonbank financial system, including casinos, money transfer houses, and the gold market. Money launderers predominantly use nonbank financial institutions for the illicit export of currency, primarily U.S. dollars and euros, to be laundered in offshore companies. There is a substantial black market for smuggled goods in the country, but it is not funded significantly by narcotics proceeds. According to Italy's Central Institute of Statistics (ISTAT), Italy's "underground" economic activity may be as large as 18 percent of the GDP. Much of this "underground activity is not related to organized crime, but is instead part of efforts to avoid taxation."

According to a 2006 International Monetary Fund evaluation, Italy's anti-money laundering and counter-terrorist financing system is comprehensive. Money laundering is defined as a criminal offense when laundering relates to a separate, intentional felony offense. All intentional criminal offenses are predicates to the crime of money laundering, regardless of the applicable sentence for the predicate offense. With approximately 600 money laundering convictions a year, Italy has one of the highest rates of successful prosecutions in the world.

Italy has strict laws on the control of currency deposits in banks. In June of 2007, the Ministry of Finance issued a decree bringing Italy into compliance with EU regulation 1889/2005 on controls of cash entering or leaving the European Community. Banks must identify their customers and record any transaction that exceeds 5000 euros (approximately U.S. $7,300). The previous threshold was 12,500 euros (approximately U.S. $18,250). Bank of Italy mandatory guidelines require the reporting of all suspicious cash transactions and other activity, such as a third party payment on an international transaction. Italian law prohibits the use of cash or negotiable bearer instruments for transferring money in amounts in excess of 5,000 euros (approximately U.S. $7,300), except through authorized intermediaries or brokers.

Banks and other financial institutions are required to maintain for ten years records necessary to reconstruct significant transactions, including information about the point of origin of funds transfers and related messages sent to or from Italy. Banks operating in Italy must record account data on their own standardized customer databases established within the framework of the anti-money laundering regulation. A "banker negligence" law makes individual bankers responsible if their institutions launder money. The law protects bankers and others with respect to their cooperation with law enforcement entities.

Italy has addressed the problem of international transportation of illegal-source currency and monetary instruments by applying the 10,000 euros (U.S. $14,700) equivalent reporting requirement to cross-border transport of domestic and foreign currencies and negotiable bearer instruments. Reporting is mandatory for cross-border transactions involving negotiable bearer monetary instruments. Financial institutions are required to maintain a uniform anti-money laundering database for all transactions (including wire transfers) over 5,000 euros ($7,300) and to submit this data monthly to the Italian Foreign Exchange Office (Ufficio Italiano dei Cambi, or UIC). The data is aggregated by class of transaction, and any reference to customers is removed. The UIC analyzes the data and can request specific transaction details if warranted. In 2008, this operation will be handled by the newly created Financial Intelligence Unit.

In 2005, the UIC received 8,576 suspicious transaction reports (STRs) related to money laundering and 482 related to terrorist financing. Italian law requires that the Anti-Mafia Investigative Unit (DIA) and the Guardia di Finanza (GdF) be informed about almost all STRs, including those that the UIC does not pursue further. The UIC does, however, have the authority to perform a degree of filtering before passing STRs to law enforcement. Law enforcement opened 328 investigations based on STRs, which resulted in 103 prosecutions.

Because of Italy's banking controls, narcotics traffickers are using different ways of laundering drug proceeds. To deter nontraditional money laundering, the Government of Italy (GOI) has enacted a decree to broaden the category of institutions and professionals subject to anti-money laundering regulations. The list now includes accountants, debt collectors, exchange houses, insurance companies, casinos, real estate agents, brokerage firms, gold and valuables dealers and importers, auction houses, art galleries, antiques dealers, labor advisors, lawyers, and notaries. The required implementing regulations for the decree, as far as nonfinancial businesses and professions are concerned, were issued in February 2006 and came into force in April 2006 (Ministerial Decrees no. 141, 142 and 143 of 3.02.2006). However, while Italy now has comprehensive internal auditing and training requirements for its (broadly-defined) financial sector, implementation of these measures by nonbank financial institutions lags behind that of banks, as evidenced by the relatively low number of STRs filed by nonbank financial institutions. As of 2005, according to UIC data, banking institutions submit about 80 percent of all STRs. Money remittance operators submit 13.5 percent of the total number of STRs, and all other sectors together account for less than ten percent.

Until January 1, 2008, the UIC served as Italy's financial intelligence unit (FIU). An arm of the Bank of Italy (BoI), the UIC received and analyzed STRs filed by covered institutions, and then forwarded them to either the Anti-Mafia Investigative Unit (DIA) or the Guardia di Finanza (GdF) (financial police) for further investigation. The UIC compiles a register of financial and nonfinancial intermediaries that carry on activities that could be exposed to money laundering. The UIC has access to banks' customer databases. Investigators from the GdF and other Italian law enforcement agencies must obtain a court order prior to being granted access to the archive. The UIC also performed supervisory and regulatory functions such as issuing decrees, regulations, and circulars. It does not require a court order to compel supervised institutions to provide details on regulated transactions. A special currency branch of the GdF is the Italian law enforcement agency with primary jurisdiction for conducting financial investigations in Italy. On January 1, 2008 Italy opened a Financial Intelligence Unit at the Bank of Italy that will assume the responsibilities of the UIC.

Italy has established reliable systems for identifying, tracing, freezing, seizing, and forfeiting assets from narcotics trafficking and other serious crimes, including terrorism. These assets include currency accounts, real estate, vehicles, vessels, drugs, legitimate businesses used to launder drug money, and other instruments of crime. Under anti-Mafia legislation, seized financial and nonfinancial assets of organized crime groups can be forfeited. The law allows for forfeiture in both civil and criminal cases. Through October 2004, Italian law enforcement seized more than 160 million euros (approximately $U.S. 233 million) in forfeited assets due to money laundering.

Italy does not have any significant legal loopholes that allow traffickers and other criminals to shield assets. However, the burden of proof is on the Italian government to make a case in court that assets are related to narcotics trafficking or other serious crimes. Law enforcement officials have adequate powers and resources to trace and seize assets; however, their efforts can be affected by which local magistrate is working a particular case. Funds from asset forfeitures are entered into the general State accounts. Italy shares assets with member states of the Council of Europe and is involved in negotiations within the EU to enhance asset tracing and seizure.

In October 2001, Italy passed a law decree (subsequently converted into law) that created the Financial Security Committee (FSC), charged with coordinating GOI efforts to track and interdict terrorist financing. FSC members include the Ministries of Finance, Foreign Affairs, Home Affairs, and Justice; the BoI; UIC; CONSOB (Italy's securities market regulator); GdF; the Carabinieri; the National Anti-Mafia Directorate (DNA); and the DIA. The Committee has far-reaching powers that include waiving provisions of the Official Secrecy Act to obtain information from all government ministries.

A second October 2001 law decree (also converted into law) made financing of terrorist activity a criminal offense, with prison terms of between seven and fifteen years. The legislation also requires financial institutions to report suspicious activity related to terrorist financing. Both measures facilitate the freezing of terrorist assets. Per FSC data as of December 2004, 57 accounts had been frozen belonging to 55 persons, totaling U.S. $528,000 under United Nations (UN) resolutions relating to terrorist financing. Data for 2005 through 2007 has not been reported. The GOI cooperates fully with efforts by the United States to trace and seize assets. Italy is second in the EU only to the United Kingdom in the number of individual terrorists and terrorist organizations the country has submitted to the UN 1267 Sanctions Committee for designation.

The UIC disseminates to financial institutions the EU, UN, and U.S. Government lists of terrorist groups and individuals. The UIC may provisionally suspend for 48 hours transactions suspected of involving money laundering or terrorist financing. The courts must then act to freeze or seize the assets. Under Italian law, financial and economic assets linked to terrorists can be directly frozen by the financial intermediary holding them, should the owner be listed under EU regulation. Moreover, assets can be seized through a criminal sequestration order. Courts may issue such orders when authorities are investigating crimes linked to international terrorism or by applying administrative seizure measures originally conceived to fight the Mafia. The sequestration order may be issued with respect to any asset, resource, or item of property, provided that these are goods or resources linked to the criminal activities under investigation.

Law no. 15 of January 29, 2006, gave the government authority to implement the EU's Third Money Laundering Directive (Directive 2005/60/EC) and to issue provisions to make more effective the freezing of nonfinancial assets belonging to listed terrorist groups and individuals. Legislative Decree 231 of November 21, 2007 implements elements of the Third Money Laundering Directive.

In Italy, the term "alternative remittance system" refers to regulated nonbank institutions such as money transfer businesses. Informal remittance systems do exist, primarily to serve Italy's significant immigrant communities, and in some cases are used by Italy-based drug trafficking organizations to transfer narcotics proceeds.

Italy does not regulate charities as such. Primarily for tax purposes, in 1997 Italy created a category of "not-for-profit organizations of social utility" (ONLUS). Such organizations can be associations, foundations or fundraising committees. To be classified as an ONLUS, the organization must register with the Finance Ministry and prepare an annual report. There are currently 19,000 registered entities in the ONLUS category. Established in 2000, the ONLUS Agency issues guidelines and drafts legislation for the nonprofit sector, alerts other authorities of violations of existing obligations, and confirms de-listings from the ONLUS registry. The ONLUS Agency cooperates with the Finance

Ministry in reviewing the conditions for being an ONLUS. The ONLUS Agency has reviewed 1,500 entities and recommended the dissolution of several that were not in compliance with Italian law. Italian authorities believe that there is a low risk of terrorist financing in the Italian nonprofit sector.

Italian cooperation with the United States on money laundering has been exemplary. The United States and Italy have signed a customs mutual assistance agreement, as well as extradition and mutual legal assistance treaties. Both in response to requests under the mutual legal assistance treaty (MLAT) and on an informal basis, Italy provides the United States records related to narcotics-trafficking, terrorism and terrorist financing investigations and proceedings. Italy also cooperates closely with U.S. law enforcement agencies and other governments investigating illicit financing related to these and other serious crimes. Currently, assets can only be shared bilaterally if agreement is reached on a case-specific basis. In May 2006, however, the U.S. and Italy signed a new bilateral instrument on mutual legal assistance as part of the process of implementing the U.S./EU Agreement on Mutual Legal Assistance, signed in June 2003. Once ratified, the new U.S./Italy bilateral instrument on mutual legal assistance will provide for asset forfeiture and sharing.

Italy is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Italy has also signed, but has not yet ratified, the UN Convention against Corruption.

Italy is an active member of the Financial Action Task Force (FATF). Italy co-chaired FATF's International Cooperation Working Group in 2007. Italy's FIU, the UIC, is a member of the Egmont Group. The UIC has been authorized to conclude information-sharing agreements concerning suspicious financial transactions with other countries. To date, the FIU has signed memoranda of understanding with 12 analogs, primarily in Europe and is negotiating agreements with 8 other FIUs, primarily in Asia. Italy has a number of bilateral agreements with foreign governments in the areas of investigative cooperation on narcotics trafficking and organized crime. Reportedly, there is no known instance of refusal to cooperate with foreign governments.

The Government of Italy is firmly committed to the fight against money laundering and terrorist financing, both domestically and internationally. However, given the relatively low number of STRs being filed by nonbank financial institutions, the GOI should improve its training efforts and supervision in this sector. Italian law enforcement agencies should take additional steps to understand and identify underground finance and value transfer methodologies employed by Italy's burgeoning immigrant communities. The GOI should also continue its active participation in multilateral efforts dedicated to the global fight against money laundering and terrorist financing.

Jamaica

Jamaica, the foremost producer and exporter of marijuana in the Caribbean, is also a major transit country for cocaine flowing from South America to the United States and other international destinations. In addition to profits from domestic marijuana trafficking, payments for cocaine and weapons pass through Jamaica in the form of bulk cash shipments back to South America. These illegal drug flows must be legitimated and therefore make Jamaica susceptible to money laundering activities and other financial crimes. In 2007, there was not a significant increase in the occurrence of financial crimes; however, there was a noticeable upsurge in advance fee scams and other related fraud schemes, including unregulated "investment clubs." The Government of Jamaica (GOJ) is also becoming increasingly concerned by the high rate of trade-based money laundering and has plans to attack this problem in 2008.

Jamaica is neither an offshore financial center, nor is it a major money laundering country. Currently, Jamaican banking authorities do not license offshore banks or other forms of exempt or shell

companies, nor are nominee or anonymous directors and trustees allowed for companies registered in Jamaica. Financial institutions are prohibited from maintaining anonymous, numbered or fictitious accounts under the 2007 Proceeds of Crime Act. As part of its political campaign, the new government, which took office in September, promoted the idea of turning Kingston into an offshore financial center. If this plan were to come to fruition, it could increase Jamaica's vulnerability to money laundering. The GOJ does not encourage or facilitate money laundering, nor has any senior official been investigated or charged with the laundering of proceeds from illegal activity. Public corruption, particularly in the Customs Service, provides opportunities for trade-based money laundering. The majority of funds being laundered in Jamaica are from drug traffickers and elements of organized crime, mainly the profits obtained in their overseas criminal activities. There is no evidence of terrorist financing in Jamaica.

Due to scrutiny by banking regulators, Jamaican financial instruments are considered an unattractive mechanism for laundering money. As a result, much of the proceeds from drug trafficking and other criminal activity are used to acquire tangible assets such as real estate or luxury cars, as well as legitimate businesses. Over the last year a significant amount of assets have flowed into new, unregulated financial investment clubs and loan schemes, which are ripe for exploitation by criminal elements. There is a significant black market for smuggled goods, which is due to tax evasion. Further complicating the ability of the GOJ to track and prevent money laundering and the transit of illegal currency through Jamaica are the hundreds of millions of U.S. dollars in remittances sent home by the substantial Jamaican population overseas.

There is a free trade zone in Montego Bay, which has a small cluster of information technology companies, and one gaming entity that focuses on international gambling. There is no indication that this free zone is being used for trade-based money laundering or terrorist financing. Domestic casino gambling, Para mutual wagering and lotteries are permitted in Jamaica, and are regulated by the Betting Gaming and Lotteries Commission.

The Proceeds of Crime Act (POCA), which became effective in May 2007, incorporates the existing provisions of its predecessor legislation (the Money Laundering Act and the Drug Offences Forfeiture of Proceeds Act), and now allows for both civil and criminal forfeiture of assets related to criminal activity. The POCA criminalizes money laundering related to narcotics offenses, fraud, firearms trafficking, human trafficking, terrorist financing and corruption, and applies to all property or assets associated with an individual convicted or suspected of involvement with a crime. This includes legitimate businesses used to launder drug money or support terrorist activity. Bank secrecy laws exist; however, there are provisions under GOJ law to enable law enforcement access to banking information.

The POCA establishes a five-year record-keeping requirement for both transactions and client identification records, and requires financial institutions to report all currency transactions over U.S. $15,000. Money transfer or remittance companies have a reporting threshold of U.S. $5,000, while for exchange bureaus the threshold is U.S. $8,000. The POCA requires banks, credit unions, merchant banks, wire-transfer companies, exchange bureaus, mortgage companies, insurance companies, brokers and other intermediaries, securities dealers, and investment advisors to report suspicious transactions of any amount to Jamaica's financial intelligence unit (FIU), which is a unit within the Ministry of Finance's Financial Investigations Division (FID). Based on its analysis of cash threshold reports and suspicious transaction reports (STRs), the FIU forwards cases to the Financial Crimes Unit of the FID for further investigation. There is also a Financial Crimes Division established within the Jamaica Constabulary Force, and it is unclear how its investigative responsibilities for financial crimes are shared with the Financial Crimes Unit of the FID.

Jamaica's central bank, the Bank of Jamaica, supervises the financial sector for compliance with anti-money laundering and counter-terrorist financing provisions. Although the POCA permits the Minister

of Finance to add nonbanking institutions to the list of obligated reporting entities, a court decision that has been pending for months has thus far tied the government's hands with respect to a growing number of currently unregulated "investment clubs, some of which are suspected to serve as covers for Ponzi schemes.

The FID was originally created by a merger, within the Ministry of Finance, the Revenue Protection Department, and the Financial Crimes Unit. The merger resulted in a division with seven distinct units. The FID currently consists of 14 forensic examiners, six police officers who have full arrest powers, a director and five administrative staff. The FID is working with the United Kingdom and Ireland to develop a comprehensive, in-house capacity for training the additional staff members it was authorized to meet its additional duties under POCA. The FID currently needs additional lawyers, forensic accountants, police officers and intelligence analysts. In the past, FID staff enjoyed a salary premium that made the positions more attractive. Recent changes have raised civil service salaries in line with current salary levels at the FID, and without revision to its pay scale, the FID's ability to recruit qualified and motivated staff will remain limited.

The FID has access to data from other government sources, which include the national vehicle registry, property tax rolls, duty and transfer rolls, various tax databases, national land register, and cross border currency declarations. Direct information access to these databases is limited to a small number of people within the FID. Indirect access is available through an internal mechanism that funnels requests to authorized users. Companion legislation to the POCA, the FID Act, which was supposed to have been enacted in 2007, remains stalled. The FID Act would bring Jamaica's regulations fully in line with the international standards of the Egmont Group, and allow for information exchange between the FID and other FIUs.

In mid-2007, the FID and the Tax Administrative Directorate (TAAD) signed a protocol for cooperation on investigations that have a nexus to criminal tax evasion. Because both entities suffer from a lack of adequate resources, it remains to be seen if the protocol can overcome competing priorities (such as revenue collection obligations, a main focus of the GOJ) and permit TAAD staff to assist the FID with money laundering investigations.

Jamaica has an ongoing education program to ensure compliance with the mandatory suspicious transaction reporting requirements. Reporting individuals are protected by law with respect to their cooperation with law enforcement entities. The FID reports that nonbank financial institutions have a 70 percent compliance rate with money laundering controls. There are currently no statistics available on the numbers of STRs, cases and convictions for 2007.

The Jamaican Parliament's 2004 amendments to the Bank of Jamaica Act, the Banking Act, the Financial Institutions Act, and the Building Societies Act improve the governance, examination and supervision of commercial banks and other financial institutions by the Bank of Jamaica. Amendments to the Financial Services Commission Act, which governs financial entities supervised by the Financial Services Commission, expand the powers of the authorities to share information, particularly with overseas regulators and law enforcement agencies. The amended Acts provide the legal and policy parameters for the licensing and supervision of financial institutions, and lay a complementary foundation to the POCA. Guidelines issued by the Bank of Jamaica caution financial institutions against initiating or maintaining relationships with persons or businesses that do not meet the standards of the Financial Action Task Force.

The GOJ requires customs declaration of currency or monetary instruments over U.S. $10,000 or its equivalent. The Kingston-based Airport Interdiction Task Force, a joint law enforcement effort by the United States, United Kingdom, Canada and Jamaica, began operations in mid-2007. The Task Force focuses, in part, on efforts to combat the movement of large amounts of cash often in shipments totaling hundreds of thousands of U.S. dollars through Jamaica.

The POCA expands the confiscation powers of the GOJ and permits, upon conviction, the forfeiture of assets assessed to have been received by the convicted party within the six years preceding the conviction. Under the POCA, the Office of the Public Prosecutor and the FID have the authority to bring asset freezing and forfeiture orders before the court. However, both agencies are lacking in staff and resources, and few of the prosecutors have received substantive training on financial crimes.

Under the POCA, the proposed division of forfeited assets would distribute assets equally among the Ministry of National Security, the Ministry of Finance, and the Ministry of Justice. An Assets Recovery Agency (ARA) will be established within the FID to manage seized and forfeited assets. There is currently no data available on the amount of seizures and forfeitures of assets for 2007. In 2006, U.S. $2 million was seized and U.S. $1.5 million was forfeited. Nondrug related assets go to a consolidated or general fund, while drug related assets are placed into a forfeited asset fund, which benefits law enforcement.

The Terrorism Prevention Act of 2005 criminalizes the financing of terrorism, consistent with UN Security Council Resolution 1373. Under the Terrorism Prevention Act, the GOJ has the authority to identify, freeze, and seize terrorist finance-related assets. The FID has the responsibility for investigating terrorist financing. The FID is currently updating its FIU database and will be implementing a system to cross-reference reports from the U.S. Treasury Department's Office of Foreign Asset Control (OFAC) and the UN Sanctions Committee. Additionally, the Ministry of Foreign Affairs and Foreign Trade circulates to all relevant agencies the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list. To date, no accounts owned by those included on the UN consolidated list have been identified in Jamaica, nor has the GOJ encountered any misuse of charitable or nonprofit entities as conduits for the financing of terrorism.

Jamaica and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995, as well as an agreement for the sharing of forfeited assets, which became effective in 2001. Jamaica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the Inter-American Convention against Corruption, and the UN Convention against Transnational Organized Crime. The GOJ has signed, but not ratified, the UN Convention against Corruption. Jamaica is a member of the Caribbean Financial Action Task Force (CFATF) and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Until the FID Act is passed, the FID will not meet the membership requirements of the Egmont Group.

The Government of Jamaica has moved forward in its efforts to combat money laundering and terrorist financing with the passage of the Proceeds of Crime Act, and should now ensure that the Act is fully implemented. The GOJ should resolve whether the POCA and other financial regulations apply to "investment clubs" and other alternative schemes. The GOJ should ensure the swift passage of the FID Act to qualify the FIU within the Financial Investigations Division to meet the international standards of the Egmont Group and exchange information with other FIUs. In addition, the GOJ should grant the FID adequate resources to enable it to hire an appropriate number of staff to allow for the additional work it now faces with the implementation of the POCA. The GOJ should also ensure that a duality of functions does not exist in the investigative responsibilities of the Financial Crimes Unit of the FID and the Financial Crimes Division of the Jamaican Constabulary Force. The GOJ should also ratify the UN Convention against Corruption.

Japan

Japan is the world's second largest economy and an important world financial center. Although the Japanese government continues to strengthen legal institutions to permit more effective enforcement of financial transaction laws, Japan still faces substantial risk of money laundering by organized crime

and other domestic and international criminal elements. The principal sources of laundered funds are drug trafficking and financial crimes: illicit gambling, loan-sharking, extortion, abuse of legitimate corporate activities, Internet fraud activities, and all types of property related crimes, which are often linked to Japan's criminal organizations. U.S. law enforcement investigations periodically show a link between drug-related money laundering activities in the U.S. and bank accounts in Japan.

On March 29, 2007, Japan's government enacted new money laundering "Law for Prevention of Transfer of Criminal Proceeds." Referred to in the press as the Gatekeeper Bill, after the Financial Action Task Force (FATF) Gatekeeper Initiative, and designed to bring Japan into closer compliance with the FATF Forty Recommendations, the bill's passage marked significant changes in Japan's anti-money laundering landscape. In addition to the financial institutions previously regulated, the new statutes expanded the types of nonfinancial businesses and professions under the law's purview, including real estate agents, private mail box agencies, dealers of precious metals and stones; and, certain types of trust and company service providers. They must conduct customer due diligence, confirm client identity, retain customer verification records, and report Suspicious Transaction Reports (STRs) to the authorities. Legal and accounting professionals such as judicial scriveners and certified public accounts are now subject to customer due diligence and record keeping, but not STR reporting. However, the bill stipulates that, "confirmation of the identity of the clients and retention of records (of transaction and identity verification) by lawyers shall be prescribed by the Japan Federation Bar Association's regulation," permitting lawyers to remain outside the law's new parameters. Accordingly, the bar association drafted and now enforces "Rules Regarding the Verification of Clients' Identity and Record-Keeping."

Drug-related money laundering was first criminalized under the Anti-Drug Special Law that took effect July 1992. This law also mandates the filing of STRs for suspected proceeds of drug offenses, and authorizes controlled drug deliveries. The legislation also creates a system to confiscate illegal profits gained through drug crimes. The seizure provisions apply to tangible and intangible assets, direct illegal profit, substitute assets, and criminally derived property that have been commingled with legitimate assets.

The narrow scope of the Anti-Drug Special Law and the burden required of law enforcement to prove a direct link between money and assets to specific drug activity limits the law's effectiveness. As a result, Japanese police and prosecutors have undertaken few investigations and prosecutions of suspected money laundering. Many Japanese officials in the law enforcement community, including Japanese Customs, believe that Japan's organized crime groups have been taking advantage of this limitation to launder money.

Japan expanded its money laundering law beyond narcotics trafficking to include money laundering predicate offenses such as murder, aggravated assault, extortion, theft, fraud, and kidnapping when it passed the 1999 Anti-Organized Crime Law (AOCL), which took effect in February 2000. The law extends the confiscation laws to include additional money laundering predicate offenses and value-based forfeitures, and enhances the suspicious transaction reporting system.

The AOCL was partially revised in June of 2002 by the "Act on Punishment of Financing to Offenses of Public Intimidation," which specifically added the financing of terrorism to the list of money laundering predicates. A further amendment to the AOCL submitted to the Diet for approval in 2004, designed to expand the predicate offenses for money laundering from approximately 200 offenses to nearly 350 offenses, with almost all offenses punishable by imprisonment, has yet to be approved.

Japan's Financial Services Agency (FSA) supervises all financial institutions and the Securities and Exchange Surveillance Commission supervises securities transactions. The FSA classifies and analyzes information on suspicious transactions reported by financial institutions, and provides law enforcement authorities with information relevant to their investigation. Japanese banks and financial institutions are required by law to record and report the identity of customers engaged in large

currency transactions. There are no secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement authorities.

To facilitate the exchange of information related to suspected money laundering activity, the FSA established the Japan Financial Intelligence Office (JAFIO) on February 1, 2000, as Japan's financial intelligence unit. Under the 2007 anti-money laundering law, on April 1, 2007, JAFIO relocated from the FSA to the National Police Agency, where it is known as the Japan Financial Intelligence Center (JAFIC). Correspondingly, JAFIC's staff grew from 17 to 43 personnel, with an emphasis on strengthened analytical functions. JAFIC receives STRs from specified business operators through the competent administrative authorities, analyzes them, and disseminates intelligence deemed useful to criminal investigations to the law enforcement community.

In 2006, JAFIC received 113,860 STRs, up from the 98,935 STRs received in 2005. In 2006, some 82 percent of the reports were submitted by banks, 7 percent by credit cooperatives, 9 percent from the country's large postal savings system, 0.7 percent from nonbank money lenders, and almost none from insurance companies. In 2006, JAFIC disseminated 71,241 STRs to law enforcement, up from 66,812 STRs disseminated in 2005. Of these, 143 money laundering cases went to prosecutors, up from 112 in 2005. The amount of money confiscated or forfeited in 2006 was 6.07 billion yen (U.S. $52 million), up from 4.46 billion yen (U.S. $39 million) in 2005.

As of 2007, JAFIC has concluded international cooperation agreements with numerous counterpart FIU's (Australia, Belgium, Brazil, Canada, Hong Kong, Indonesia, Malaysia, the Philippines, Singapore, Thailand, the United Kingdom, and the United States). These agreements establish cooperative frameworks for the exchange of financial intelligence related to money laundering and terrorist financing. Japanese financial institutions have cooperated with law enforcement agencies, including U.S. and other foreign government agencies investigating financial crimes related to narcotics.

In 2006, Japan concluded a Mutual Legal Assistance Treaty (MLAT) with the Republic of Korea, and is currently negotiating MLAT texts with China and Russia. In 2003, the United States and Japan concluded a Mutual Legal Assistance Treaty (MLAT), which took effect in July of 2006. In 2007 the U.S.-Japan MLAT was used for the first time in furtherance of two separate money laundering investigations where the predicate crimes (Nigerian bank fraud) first occurred overseas, then moved to the U.S., with the money subsequently laundered in Japan; the cases are still pending.

Although Japan has not adopted "due diligence" or "banker negligence" laws to make individual bankers legally responsible if their institutions launder money, there are administrative guidelines that require due diligence. In a high-profile 2006 court case, however, the Tokyo District Court ruled to acquit a Credit Suisse banker of knowingly assisting an organized crime group to launder money despite doubts about whether the banker performed proper customer due diligence. Japanese law does not protect bankers and other financial institution employees who cooperate with law enforcement entities.

In April 2002, the Diet enacted the Law on Customer Identification and Retention of Records on Transactions with Customers by Financial Institutions (a "know your customer" law). The law reinforced and codified the customer identification and record-keeping procedures that banks had practiced for years. The Foreign Exchange and Foreign Trade law was revised in January 2007, so that financial institutions are required to make positive customer identification for both domestic transactions and transfers abroad in amounts of more than 100,000 yen (approximately $900). Banks and financial institutions are required to maintain customer identification records for seven years. In January 2007, an amendment to the rule on Customer Identification by Financial Institutions came into force, whereby financial institutions are now required to identify the originators of wire transfers of over 100,000 yen.

In 2004, the FSA cited Citibank Japan's failure to properly screen clients under anti-money laundering mandates as one of a list of problems that caused the FSA to shut down Citibank Japan's private banking unit. In February 2004, the FSA disciplined Standard Chartered Bank for failing to properly check customer identities and for violating the obligation to report suspicious transactions. In January 2007, the Federal Reserve ordered Japan's Sumitomo Mitsui Banking Corp.'s New York branch to address anti-money laundering deficiencies, only a month after similarly citing Bank of Tokyo-Mitsubishi UFJ for anti-money laundering shortcomings.

The Foreign Exchange and Foreign Trade Law requires travelers entering and departing Japan to report physically transported currency and monetary instruments (including securities and gold weighing over one kilogram) exceeding one million yen (approximately U.S. $8,475), or its equivalent in foreign currency, to customs authorities. Failure to submit a report, or submitting a false or fraudulent one, can result in a fine of up to 200,000 yen (approximately $1,695) or six months' imprisonment. Efforts by authorities to counter bulk cash smuggling in Japan are not yet matched by a commensurate commitment in necessary resources.

In response to the events of September 11, 2001 the FSA used the anti-money laundering framework provided in the Anti-Organized Crime Law to require financial institutions to report transactions where funds appeared either to stem from criminal proceeds or to be linked to individuals and/or entities suspected to have relations with terrorist activities. The 2002 Act on Punishment of Financing of Offenses of Public Intimidation, enacted in July 2002, added terrorist financing to the list of predicate offenses for money laundering, and provided for the freezing of terrorism-related assets. Japan signed the UN International Convention for the Suppression of the Financing of Terrorism on October 30, 2001, and became a party on June 11, 2002.

After September 11, 2001, Japan has regularly searched for and designated for asset freeze any accounts that might be linked to all the suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of individuals and entities under UNSCR 1373.

Underground banking systems operate widely in Japan, especially in immigrant communities. Such systems violate the Banking Law. There have been a large number of investigations into underground banking networks. Reportedly, substantial illicit proceeds have been transferred abroad, particularly to China, North and South Korea, and Peru. In November 2004, the Diet approved legislation banning the sale of bank accounts, in a bid to prevent the use of purchased accounts for fraud or money laundering.

Japan has not enacted laws that allow for sharing of seized narcotics assets with other countries. However, the Japanese government fully cooperates with efforts by the United States and other countries to trace and seize assets, and makes use of tips on the flow of drug-derived assets from foreign law enforcement efforts to trace funds and seize bank accounts.

Japan is a party to the 1988 UN Drug Convention and has signed but not ratified the UN Transnational Organized Crime Convention. Ratification of this convention would require amendments to Japan's criminal code to permit charges of conspiracy, which is not currently an offense. Minority political parties and Japan's law society have blocked this amendment on at least three occasions. Japan is a member of the Financial Action Task Force. JAFIO (now JAFIC) joined the Egmont Group of FIUs in 2000. Japan is also a member of the Asia/Pacific Group against Money Laundering, and is scheduled for a second round mutual evaluation in 2008.

In 2002, Japan's FSA and the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission signed a nonbinding Statement of Intent (SOI) concerning cooperation and the exchange of information related to securities law violations. In January 2006 the FSA and the U.S. SEC and CFTC signed an amendment to their SOI to include financial derivatives. Japan is a signatory

but not a party to the UN Convention against Corruption. Japan is listed 17 out of 179 countries surveyed in Transparency International's 2007 Corruption Perception Index.

The Government of Japan has many legal tools and agencies in place to successfully detect, investigate, and combat money laundering. However, there have been few successful money laundering prosecutions and convictions. To strengthen its money laundering regime, Japan should stringently enforce the Anti-Organized Crime Law, and amend the law with regard to charges of conspiracy. The narrow scope of the Anti-Drug Special Law has limited the law's effectiveness. Japan should also enact penalties for noncompliance with the customer identification provisions of the Foreign Exchange and Trade Law, adopt measures to share seized assets with foreign governments, and enact banker "due diligence" provisions. Japan should continue to combat underground financial networks. Since Japan is a major trading power and the misuse of trade is often the facilitator in alternative remittance systems and value transfer schemes, Japan should take steps to identify and combat trade-based money laundering. Japan should also become a party to the UN Transnational Organized Crime Convention and the UN Convention against Corruption.

Jersey

The Bailiwick of Jersey (BOJ), one of the Channel Islands, is an international financial center offering a sophisticated array of offshore services. A Crown Dependency of the United Kingdom, it relies on the United Kingdom for its defense and international relations. Due to Jersey's investment services, most of the illicit money in Jersey is derived from foreign criminal activity. Domestically, local drug trafficking and corruption of politically exposed persons (PEPs) are sources of illicit proceeds found in the country. Money laundering mostly occurs within Jersey's banking system, investment companies, and local trust companies.

The financial services industry consists of 48 banks; 1,086 funds; 953 trust companies (2005 statistic), and 175 insurance companies (2006 statistic), which are largely captive insurance companies. The menu of services includes investment advice, dealing management companies, and mutual fund companies. In addition to financial services, companies offer corporate services, such as special purpose vehicles for debt restructuring and employee share ownership schemes. For high net worth individuals, there are wealth management services. All regulated entities can sell their services to both residents and nonresidents. All financial businesses must have a presence in Jersey, and management must also be in Jersey. However, although Jersey does not provide offshore licenses, it administers a number of companies registered in other jurisdictions. These companies, known as "exempt companies," do not pay Jersey income tax and their services are only available to nonresidents.

The Jersey Finance and Economics Committee is the government body responsible for administering the law, regulating, supervising, promoting, and developing the Island's finance industry. The financial Services Commission (FSC) is the financial services regulator. In 2003, the International Monetary Fund (IMF) assessed Jersey's anti-money laundering (AML) regime. The IMF reported that it found the FSC to be in compliance with international standards. The IMF has scheduled a review and assessment of Jersey's financial frameworks for October 2008.

Jersey's main AML laws are the Drug Trafficking Offenses (Jersey) Law of 1988, which criminalizes money laundering related to narcotics trafficking, and the Proceeds of Crime (Jersey) Law, 1999, which extends the predicate offenses for money laundering to all offenses punishable by at least one year in prison. The FSC has recently formed a dedicated AML Unit to lead the Island's operational AML and counter-terrorist financing (CTF) strategy. The AML Unit will devise and implement a registration scheme for currently unregulated nonfinancial services businesses and professions entering an oversight regime for the first time. Under amendments being made to the Proceeds of Crime (Jersey) Law 1999, businesses such as estate agents and dealers in high value goods will, for

the first time, have AML regulation. The AML Unit has also taken specific responsibility regulating money service business such as bureaux de change, check cashers, and money transmitters.

In May and July 2007, in preparation for the upcoming IMF assessment and with Council of Ministers approval, the AML/CTF Strategy Group issued three consultation papers proposing to extend and update Jersey's AML framework to comply with the international standards. In October 2007, the FSC published a Consultation Paper proposing amendments to current legislation and introducing new secondary legislation. The Consultation Paper discusses the proposed legislative changes with regard to the Trust Company Business and Investment Business secondary legislation on accounts, audits, and reports. The paper also discusses requirements on Trust Company Business with respect to the safekeeping of customer money.

Financial institutions must report suspicious transactions under the narcotics trafficking, terrorism, and anti-money laundering laws. There is no threshold for filing a suspicious transaction report (STR), and the reporting individual is protected from criminal and civil charges by safe harbor provisions in the law. Banks and other financial service companies must maintain financial records of their customers for a minimum of 10 years after completion of business. The FSC has issued AML Guidance Notes that the courts take into account when considering whether or not an offense has been committed under the Money Laundering Order. Upon conviction of money laundering, a person could receive imprisonment of one year or more.

After consultation with the financial services industry, the FSC issued a position paper (jointly with Guernsey and Isle of Man counterparts) proposing to further tighten the essential due diligence requirements that financial institutions must meet regarding their customers. The position paper states the FSC's intention to insist on the responsibility of all financial institutions to verify the identity of their customers, regardless of the action of intermediaries. The paper also states an intention to require a progressive program to obtain verification documentation for customer relationships established before the Proceeds of Crime (Jersey) Law came into force in 1999. Each year working groups review specific portions of these principles and draft AML Guidance Notes to incorporate changes.

Following the extensive consultation with the Funds Sector, and approval by the State of Jersey in November 2007, the FSC published Codes of Practice for Fund Services Business. The Code consists of seven high level principles for the conduct of fund services business, together with more detailed requirements in relation to each principle.

Approximately 30,000 Jersey companies have registered with the Registrar of Companies, which is the Director General of the FSC. In addition to public filing requirements relating to shareholders, the FSC requires each company to provide the Commission with details of the ultimate individual beneficial owner of each Jersey-registered company. The Registrar keeps the information in confidence.

The Joint Financial Crime Unit (JFCU), Jersey's financial intelligence unit (FIU), is responsible for receiving, investigating, and disseminating STRs. The unit includes Jersey Police and Customs officers and a financial crime analyst. In 2006, the JFCU received 1,034 STRs. Approximately 25 percent of the STRs filed result in further police investigations. Reports filed in the first six months of 2007 indicate a 32 percent increase in the number of STRs submitted to the JFCU by financial institutions compared to the three-year average for this same period. In the first six months of 2007, Jersey has held more than 2.5 million pounds (approximately $4.9 million) in bank or trust company accounts pending police investigation of suspicious activity. The FIU also responds to requests for financial information from other FIUs. In the first six months of 2007, the JFCU received 219 requests for assistance from counterparts in other jurisdictions.

The Enforcement Division of the Jersey's Financial Services Commission (FSC) responded to 10 requests for assistance from overseas regulators during 2006 and issued public statements concerning

nine illegal Internet based businesses that purported to have a Jersey connection. Jersey's law enforcement and regulatory agencies have extensive powers to cooperate with one another, and regularly do so. The FSC cooperates with regulatory authorities, for example, to ensure that financial institutions meet AML obligations.

The JFCU, in conjunction with the Attorney Generals Office, trace, seize and freeze assets. A confiscation order can be obtained if the link to a crime is proven. If the criminal has benefited from a crime, legitimate assets can be forfeited to meet a confiscation order. There is no period of time ascribed to the action of freezing until the assets are released. Frozen assets are confiscated by the Attorney Generals Office on application to the Court. Proceeds from asset seizures and forfeitures are placed in two funds. Drug-trafficking proceeds go to one fund, and the proceeds of other crimes go to the second fund. The drug-trafficking funds are used to support harm reduction programs, education initiatives, and to assist law enforcement in the fight against drug trafficking. Only limited civil forfeiture is allowed in relation to cash proceeds of drug trafficking located at the ports.

Alternate remittance systems do not appear to be prevalent in Jersey.

The Corruption (Jersey) Law 2005 was passed in alignment with the Council of Europe Criminal Law Convention on Corruption. The new corruption law came into force in February 2007. Articles 2, 3, and 4 of this law were amended in November 2007.

On July 1, 2005, the European Union Savings Tax Directive (ESD) came into force. The ESD is an agreement between the Member States of the European Union (EU) to automatically exchange information with other Member States about EU tax resident individuals who earn income in one EU Member State but reside in another. Although not part of the EU, the three UK Crown Dependencies (Jersey, Guernsey and Isle of Man) have voluntarily agreed to apply the same measures to those in the ESD and have elected to implement the withholding tax option (also known as the "retention tax option") within the Crown Dependencies.

Under the retention tax option, each financial services provider will automatically deduct tax from interest and other savings income paid to EU resident individuals. The tax will then be submitted to local and Member States tax authorities annually. The tax authorities receive a bulk payment but do not receive personal details of individual customers. If individuals elect the exchange of information option, then no tax is deducted from their interest payments, but details of the customer's identity, residence, paying agent, level and time period of savings, and income received by the financial services provider will be reported to local tax authorities where the account is held and then forwarded to the country where the customer resides.

Jersey signed the Tax Information Exchange Agreement (TIEA) with the United States in 2002, and plans to sign the same agreements with other countries, thus meeting international obligations to cooperate in financial investigations.

Jersey criminalized money laundering related to terrorist activity with the Prevention of Terrorism (Jersey) Law 1996. The Terrorism (Jersey) Law 2002, which entered into force in January 2003, enhances the powers of the Island authorities to investigate terrorist offenses, to cooperate with law enforcement agencies in other jurisdictions, and to seize assets. Jersey does not circulate the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, the EU designated list, or any other government's list. However, Jersey expects its institutions to gather information of designated entities from the Internet and other public sources. Jersey authorities have instituted sanction orders freezing accounts of individuals connected with terrorist activity.

The FSC has reached agreements on information exchange with securities regulators in Germany, France, and the United States. The FSC has a memorandum of understanding for information

exchange with Belgium. Registrar information is available, under appropriate circumstances and in accordance with the law, to U.S. and other investigators. In 2007, the FSC has signed a memorandum of understanding with British Virgin Islands Financial Services Commission that will further cooperation between the two regulatory bodies. Application of the 1988 UN Drug Convention was extended to Jersey on July 7, 1997.

Jersey is a member of the Offshore Group of Insurance Supervisors (OGIS) and the Offshore Group of Banking Supervisors (OGBS). It works with the Basel Committee on Banking Supervision and the Financial Action Task Force. The JFCU is a member of the Egmont Group.

The Bailiwick of Jersey should continue to enhance compliance with international standards. Jersey should ensure that all entities, within all sectors, are subject to reporting requirements. The FSC should work to ensure that the AML Unit has enough resources to function effectively, and to provide outreach and guidance to the sectors it regulates. This is especially true for the newest DNFBPs required to file reports. Jersey should mandate the same AML/CTF requirements over its "exempt" companies that it does over the rest of the obliged sectors. The FSC should distribute the UN, European Union and U.S. lists of designated suspected terrorist and terrorist-supporting entities to the obliged entities and not rely on the entities stay current through Internet research.

Jordan

Jordan is not a regional or offshore financial center and is not considered a major venue for international criminal activity. However, Jordan's long and often remote desert borders and proximity to Iraq make it susceptible to smuggling bulk cash, fuel, narcotics, cigarettes, and other contraband. The influx of refugees has caused an increase in cross border criminal activity. Jordan boasts a thriving "import-export" community of brokers, traders, and entrepreneurs that regionally are involved with value transfer via trade and customs fraud.

In August 2001, the Central Bank of Jordan, which regulates banks and financial institutions, issued anti-money laundering regulations designed to meet some of the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering. Since that time, money laundering has been considered an "unlawful activity" subject to criminal prosecution. After the lifting of Iraqi sanctions, there have been few reports of money laundering through Jordanian banks. On July 17, 2007, Jordan enacted a comprehensive anti-money laundering law (AML). The law, Law No. 46 for the Year 2007, created a committee known as the National Committee on Anti-Money Laundering (NCAML). The committee is chaired by the Governor of the Central Bank of Jordan and has as members: the Deputy Governor of the Central Bank named by the Governor of the Central Bank to serve as deputy chairman of the committee, the Secretary General of the Ministry of Justice, the Secretary General of the Ministry of the Interior, the Secretary General of the Ministry of Finance, the Secretary General of the Ministry of Social Development (which overseas charitable organizations), the Director of the Insurance Commission, the Controller General of Companies, a Commissioner of the Securities Commission, and the head of the Anti-Money Laundering Unit. The Anti-Money Laundering Unit (AMLU), formerly the Central Bank's Suspicious Transaction Follow-Up Unit, was formed immediately on passage of the law and designated as the Government of Jordan's (GOJ) financial intelligence unit (FIU). The AMLU is staffed with a director, outreach officer, chief counsel, and one analyst. It is anticipated that during 2008, the unit's staff will be augmented to include a minimum of seven analysts and liaison personnel from the two national law enforcement agencies, public prosecutors, and other regulatory entities.

The AMLU is designated as an independent entity, but is housed at present in the Central Bank of Jordan. It is organized on a general administrative FIU model. It is responsible for receiving suspicious activity reports (SARs) from obligated entities designated in the law, analyzing them, requesting additional information related to the activity and reporting it to the prosecutor general for

further action. Involvement of the AMLU in assisting criminal investigations is dependent on public prosecutors. At the end of 2007, the AMLU was working to establish formal ties through memoranda of understanding with competent GOJ authorities possessing the necessary databases and resources pertinent to pursuing financial intelligence analysis and money laundering investigations.

The 2007 AML law criminalizes money laundering and stipulates as predicate offenses any felony crime or any crime stated in international agreements to which Jordan is a party, whether such crimes are committed inside or outside the Kingdom, provided that the act committed is subject to penalty in the country in which it occurs. The Central Bank of Jordan previously instructed financial institutions to be particularly careful when handling foreign currency transactions, especially if the amounts involved are large or if the source of funds is in question. The new law requires obligated entities to: undertake due diligence in identifying customers; refrain from dealing with anonymous persons or shell banks; report to the AMLU any suspicious transaction, completed or not; and comply with instructions issued by competent regulatory parties to implement provisions of the law. The Ministries of Justice, Interior, Finance, and Social Development, as well as the Insurance Commission, Controller General of Companies, and Securities Commission all have a part in regulating various other nonfinancial institutions through issued regulations and instructions. The AMLU is obligated to work with these entities to ensure that a comprehensive approach to AML/CTF is undertaken in keeping with international standards and best practices.

Financial institutions are required under the new law to report all suspicious transactions whether the transaction was completed or not. This includes banks, foreign exchange companies, money transfer companies, stock brokerages, insurance companies, credit companies, and any company whose articles of association state that their activities include debt collection and payment services, leasing services, investment and financial asset management, real estate trading and development, and trading in precious metals and stones. Lawyers and accountants are not considered to be obligated entities under the law.

All obligated entities are required to conduct due diligence to identify customers, their activities, legal status, and beneficiaries and follow-up on transactions that are conducted through an ongoing relationship. Business dealings with anonymous persons, persons using fictitious names or shell banks are prohibited. Obligated entities are required to comply with instructions issued by competent regulatory authorities as listed in the law. Disclosure to the customer or the customer's beneficiary of STRs and/or verifications or investigations by competent authorities is prohibited. They are also required to respond to any inquiry from the AMLU regarding STRs or requests for assistance from other competent judicial, regulatory, administrative, or security authorities needing information to perform their responsibilities.

Jordanian officials report that financial institutions file suspicious transaction reports and cooperate with prosecutors' requests for information related to narcotics trafficking and terrorism cases. The AMLU received over 30 SARs in 2007, two of which were forwarded for prosecution. There were no arrests or convictions for money laundering or terrorist financing in Jordan in 2007. The standard for forwarding SARs is potentially a problem in the existing law.

The Banking Law of 2000 (as amended in 2003) allows judges to waive bank secrecy provisions in any number of criminal cases, including suspected money laundering and terrorist financing. An October 8, 2001 revision to the Penal Code criminalized terrorist activities, specifically financing of terrorist organizations. Guidelines issued by the Central Bank state that banks should research all sanctions lists relating to terrorist financing including those issued by individual countries and other relevant authorities. The Central Bank may not circulate names on sanctions lists to banks unless the names are included on the UNSCR 1267 Sanctions Committee's consolidated list. No such assets have been identified to date. Banks and other financial institutions are required to maintain records for a period of five years.

One significant challenge facing the GOJ is determining which law enforcement entity will be tasked to conduct financial investigations relating to AML/CTF. Since the AML law was only implemented in July 2007, law enforcement agencies and public prosecutors are still deliberating the issue.

There are six public free trade zones in Jordan: the Zarqa Free Zone, the Sahab Free Zone, the Queen Alia International Airport Free Zone; the Al-Karak Free Zone, the Al-Karama Free Zone and the Aqaba Free Zone. All of the six list their investment activities as "industrial, commercial, service, and touristic." There are 32 private free trade zones, a number of which are related to the aviation industry. Other free trade zones list their activities as industrial, agricultural, pharmaceutical, training of human capital, and multi-purpose. All free trade zones are regulated by the Jordan Free Zones Corporation in the Ministry of Finance and are guided by the Law of Free Zones Corporation No. 32 for 1984 (and amendments). Regulations state that companies and individuals using the zones must be identified and registered with the Corporation.

Although the 2007 AML law requires reporting of cross-border movement of money if the value exceeds a threshold amount set by the NCAML, no threshold amount was set by the end of 2007. The law also provides for the creation of cross-border currency and monetary instruments declaration forms, and the AMLU is working on the creation of the form. However, the declaration requirement applies only for the entry of money into the Kingdom and not outgoing. The Customs Department is responsible for archiving the declaration forms once implemented. In December 2004, the United States and Jordan signed an Agreement regarding Mutual Assistance between their Customs Administrations that provides for mutual assistance with respect to customs offenses and the sharing and disposition of forfeited assets. The AML law authorizes Customs "to seize or restrain" undeclared money crossing the border and report same to the AMLU which will decide whether the money should be returned or the case referred to the judiciary.

Jordan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Jordan has signed but has yet to ratify the UN Convention against Transnational Organized Crime. Jordan is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) and in 2007 Jordan held the presidency of MENAFATF. Jordan's AMLU aspires to membership in the Egmont Group of Financial Intelligence Units.

The new AML law provides judicial authorities the legal basis to cooperate with foreign judicial authorities in providing assistance in foreign investigations, extradition, and freezing and seizing of funds related to money laundering in accordance with current legislation and bilateral or multilateral agreements to which Jordan is a part based on reciprocity. Judicial authorities may order implementation of requests by foreign judicial authorities to confiscate proceeds of crime relating to money laundering and to distribute such proceeds in accordance with bilateral or multilateral agreements. Jordan's Anti-drugs Law allows the courts to seize proceeds of crime derived from acts proscribed by the law. The Economic Crimes Law gives both prosecutors and the courts the authority to seize the assets of any person who has committed a crime under that law for a period of three months while an investigation is underway. Jordan's penal code further provides prosecutors the authority to confiscate "all things" derived from a felony or intended misdemeanor.

In light of the 2007 AML law, the Government of Jordan's NCAML and the AMLU should conduct a comprehensive evaluation of Jordan's capabilities in preventing money laundering and enforcing its new law in accordance with international standards and best practices. Jordanian law enforcement and customs should examine forms of bulk cash smuggling relating to terrorist financing and trade-based money laundering and incorporate prevention and investigative strategies that meet the requirements of complex financial investigations. The GOJ should ratify the UN Convention against Transnational Organized Crime.

Kenya

Kenya is developing into a major money laundering country. As a regional financial and trade center for Eastern, Central, and Southern Africa, Kenya's economy has large formal and informal sectors. Kenya's use as a transit point for international drug traffickers is increasing. Domestic drug abuse is also increasing, especially in Coast Province. Narcotics proceeds are being laundered in Kenya, although the volume has not yet been determined. Kenya has no offshore banking or Free Trade Zones. There is no significant black market for smuggled goods in Kenya. However, Kenya serves as the major transit country for Uganda, Tanzania, Rwanda, Burundi, northern Democratic Republic of Congo (DRC), and Southern Sudan. Goods marked for transit to these northern corridor countries avoid Kenyan customs duties, but have been known to be sold in Kenya.

Many entities in Kenya are involved in exporting and importing goods, including a reported 800 registered, international nongovernmental organizations (NGOs) managing over U.S. $1 billion annually. International organizations operating in the conflict areas of the region—Southern Sudan, Somalia, Burundi and DRC—keep all their dollars in Kenyan banks.

Annual remittances from expatriate Kenyans are estimated at U.S. $680-780 million. Individual Kenyans and foreign residents also transfer money in and out of Kenya. Nairobi's Eastleigh Estate has become an informal hub for remittances by the Somalia Diaspora, transmitting millions of dollars every day from Europe, Canada and the U.S. to Mogadishu. Many transfers are executed via formal channels such as wire services and banks, but there is also a thriving network of cash-based, unrecorded transfers that the Government of Kenya (GOK) cannot track. Expatriates primarily use this system to send and receive remittances internationally. The large Somali refugee population in Kenya uses a hawala system to send and receive remittances. The GOK has no means to monitor hawala transfers. Kenya does not have an effective legal regime to address money laundering. The GOK has no regulations to freeze/seize criminal or terrorist accounts, and has not passed a law that explicitly outlaws money laundering and creates a financial intelligence unit (FIU).

Section 49 of the Narcotic Drugs and Psychotropic Substance Control Act of 1994 criminalizes money laundering related to narcotics trafficking. The offense is punishable by a maximum prison sentence of 14 years. However, Kenya has never seen a conviction for the laundering of proceeds from narcotics trafficking. Money laundering is a criminal offense, through a patchwork of laws and guidance that the GOK has cobbled together, including the 1994 Act, Legal Notice No. 4 of 2001, the Central Bank of Kenya (CBK) Guidelines on Prevention of Money Laundering, and enabling provisions of other laws. Kenya has not developed an effective anti-money laundering (AML) regime.

In November 2006, the GOK published a proposed Proceeds of Crime and Anti-Money Laundering Bill, a revised version of a 2004 law. The proposed law declares itself to be "An act of Parliament to provide for the offence of money laundering and to introduce measures for combating the offence, to provide for the identification, tracing, freezing, seizure and confiscation of the proceeds of crime." It defines "proceeds of crime" as any property or economic advantage derived or realized, directly or indirectly, as a result of or in connection with an offence. The draft legislation provides for criminal and civil restraint, seizure and forfeiture. In addition, the proposed bill authorizes the establishment of an FIU and requires financial institutions and nonfinancial businesses or professions, including casinos, real estate agencies, precious metals and stones dealers, and legal professionals and accountants, to file suspicious transaction reports above a certain threshold. The bill also identifies 30 other statutes for the GOK to amend so that they will be consistent with the bill when it is passed.

This bill has deficiencies. It does not mention terrorism, nor does it specifically define "offense" or "crime." The proposed legislation does not explicitly authorize the seizure of legitimate businesses used to launder money. The requirement that only suspicious transactions above a certain threshold are reported is inconsistent with international standards, which call for suspicious transaction reports to have no monetary threshold. The GOK tabled the bill in Parliament in November 2007, but Parliament

never took the bill up, and it lapsed when Parliament recessed on December 8. The government will need to republish and resubmit the bill in the Tenth Parliament in 2008.

The CBK is the regulatory and supervisory authority for Kenya's deposit-taking institutions and has oversight for more than 50 such entities, as well as mortgage companies and other financial institutions. The Minister of Home Affairs supervises casinos, although its regulation of this sector is ineffective.

CBK regulations require deposit-taking institutions to verify the identity of new customers opening an account or conducting a transaction. The Banking Act amendment of December 2001 authorizes the CBK to disclose financial information to any monetary or financial regulatory authority within or outside Kenya. In 2002, the Kenya Bankers Association (KBA) issued guidelines requiring banks to report suspicious transactions to the CBK. These guidelines do not have the force of law, and only a handful of suspicious transactions have been reported so far. Under the regulations, banks must maintain records of transactions over U.S. $100,000 and international transfers over U.S. $50,000, and report them to the CBK. A law enforcement agency can demand information from any financial institution, if it has obtained a court order. Some commercial banks and foreign exchange bureaus file suspicious transaction reports voluntarily, but they run the risk of civil litigation, as there are no adequate "safe harbor" provisions for reporting such transactions to the CBK. A court ruling to penalize a commercial bank in 2002 for disclosing information to the CBK in response to a court order, made banks wary of reporting suspicious transactions. In a November 2007 decision that will likely further chill banks' willingness to report suspicious transactions, a judge ordered Barclays Bank to pay a customer Kenya Shillings (Sh) 400,000 (approximately U.S. $6,107) for violating confidentiality by providing details on the customer's specimen signature to the British High Commission without her consent for processing a visa application.

These regulations do not cover nonbank financial institutions such as money remitters, casinos, or investment companies, and there is no enforcement mechanism behind the regulations. Kenya lacks the institutional capacity, investigative skill and equipment to conduct complex investigations independently. There have been no arrests or prosecutions for money laundering or terrorist financing.

There are 95 foreign exchange bureaus under GOK supervision. The Central Bank of Kenya Act (Cap 491) regulates forex bureaus, which are authorized dealers of currency. The CBK subsequently recognized that several bureaus violated the Forex Bureau Guidelines, including dealing in third party checks and executing telegraphic transfers without CBK approval. The checks and transfers may have been used for fraud, tax evasion and money laundering. In response, the CBK's Banking Supervision Department issued Central Bank Circular No. 1 of 2005 instructing all forex bureaus to immediately cease dealing in telegraphic transfers and third party checks. These new guidelines, which fall under Section 33K of the Central Bank of Kenya Act, took effect on January 1, 2007.

Kenya has little in the way of cross-border currency controls. GOK regulations require that any amount of cash above U.S. $5,000 be disclosed at the point of entry or exit for record-keeping purposes only, but this provision is rarely enforced, and authorities keep no record of cash smuggling attempts. The CBK guidelines call for currency exchange bureaus to furnish daily reports on any single foreign exchange transaction above U.S. $10,000, and on cumulative daily foreign exchange inflows and outflows above U.S. $100,000. Guidelines require that foreign exchange dealers ensure that cross-border payments have no connection to illegal financial transactions.

Recent investigations illustrate Kenya's vulnerability to money laundering. The Charterhouse Bank investigations in 2006 and 2007 revealed that the proceeds of large-scale evasion of import duties and taxes had been laundered through the banking system since at least 1999. In addition, the smuggled and/or under-invoiced goods may have also been marketed through the normal wholesale and retail sectors. Charterhouse Bank managers had conspired with depositors to evade import duties and taxes and launder the proceeds totaling approximately $500 million from 1999 to 2006. In June 2006, a

Member of Parliament tabled a 2004 initial investigation report on Charterhouse Bank by a special CBK investigations team indicating account irregularities, tax evasion and money laundering by some of the bank's clients. The Ministry of Finance temporarily closed the bank to prevent a run, and the CBK placed Charterhouse Bank under statutory management to preserve records and prevent removal of funds. Subsequent audits and investigations covering the period 1999-2006 found that Charterhouse Bank had violated the CBK's know-your-customer procedures in over 80 percent of its accounts, and were missing basic details such as the customer's name, address, ID photo, or signature cards. Charterhouse Bank also violated the Banking Act and the CBK's Prudential Guidelines by not properly maintaining records for foreign currency transactions. Available evidence makes clear that the bank management had, on a large scale, consistently evaded and ignored normal internal controls by allowing many irregular activities to occur. The bank management's continual violation of CBK prudential guideline CBK/PG/08 requirements to report suspicious transactions, and its efforts to conceal them from CBK examiners, also indicate that bank officials were complicit in these suspicious transactions. The perpetrators demonstrated an understanding of AML controls, transferring funds to the United States and the United Kingdom in increments just below reporting thresholds of the receiving banks for large currency transactions. The Minister of Finance advised Charterhouse and the CBK that the Ministry would not renew the bank's license to operate after December 31, 2006. (Bank licenses are annual and expire automatically at the end of each year if not renewed.) The courts rejected Charterhouse owners' legal challenges, and the bank remained closed.

This case illustrates that criminals have been taking advantage of Kenya's inadequate AML regime for years by evading oversight and/or by reportedly paying off enforcement officials, other government officials, and politicians. There are strong indications that other Kenyan banks are also involved in similar activities. Reportedly, Kenya's financial system may be laundering over U.S. $100 million each year. However, in 2006 and 2007 there were not any reported money laundering related arrests, prosecutions, or convictions.

Kenya has not criminalized the financing of terrorism as required by the United Nations Security Council Resolution 1373 and the UN International Convention for the Suppression of Financing of Terrorism, to which it is a party. In April 2003, the GOK introduced the Suppression of Terrorism Bill into Parliament. After objections from some public groups that the bill unfairly targeted the Muslim community and unduly restricted civil rights, the GOK withdrew the bill. The GOK drafted the Anti-Terrorism Bill in 2006, which contains provisions that would strengthen the GOK's ability to combat terrorism. It also revises the controversial text, but Muslim and human rights groups remain convinced the government could use it to commit human rights violations. The GOK published the bill and submitted it to Parliament in 2007, but Parliament took no action and the bill will have to be resubmitted to the tenth Parliament in 2008.

The GOK requires all charitable and nonprofit organizations to register with the government and submit annual reports to the GOK's oversight body, the National Non-Governmental Organization Coordination Bureau. NGOs that are noncompliant with the annual reporting requirements can have their registrations revoked; however, the government rarely imposes such penalties. The GOK revoked the registration of some NGOs with Islamic links in 1998 after the bombing of the U.S. Embassy in Nairobi, only to later re-register them. The Non-Governmental Organization Coordination Bureau lacks the capacity to monitor NGOs, and observers suspect that charities and other nonprofit organizations handling millions of dollars are filing inaccurate or no annual reports. The Bureau made some progress towards strengthening its capacity to review NGO registrations and annual reports for suspicious activities in 2007.

Drug trafficking-related asset seizure and forfeiture laws and their enforcement are weak and disjointed. With the exception of intercepted drugs and narcotics, seizures of assets are rare. At present, the government entities responsible for tracing and seizing assets are the Central Bank of Kenya Banking Fraud Investigation Unit, the Kenya Police Anti-Narcotics and Anti-Terrorism Police

Units, the Kenya Revenue Authority (KRA), and the Kenya Anti-Corruption Commission (KACC). To demand bank account records or to seize an account, the police must present evidence linking the deposits to a criminal violation and obtain a court warrant. This process is difficult to keep confidential, and as a result of leaks, serves to warn account holders of investigations. Account holders then move their accounts or contest the warrants.

The CBK does not circulate the list of individuals and entities on the United Nations (UN) 1267 Sanctions Committee's consolidated list or the United States Office of Foreign Asset Control (OFAC) designated list to the financial institutions it regulates. Instead, the CBK uses its bank inspection process to search for names on the OFAC list of designated people and entities. The CBK and the GOK have no authority to seize or freeze accounts without a court warrant. To date, the CBK has not notified the United States Government of any bank customers identified on the OFAC list. There is currently no law specifically authorizing the seizure of the financial assets of terrorists.

Kenya is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Kenya ranks 150 out of 180 countries on the 2007 Transparency International Corruption Perceptions Index. Kenya is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a Financial Action Task Force (FATF)-style regional body. Kenya has an informal arrangement with the United States for the exchange of information relating to narcotics, terrorist financing, and other serious crime investigations. Kenya has cooperated with the United States and the United Kingdom.

The GOK should criminalize the financing of terrorism and pass a law authorizing the government to seize the financial assets of terrorists and convict individuals or groups that finance terrorist activity. Kenyan authorities should take steps to ensure that NGOs and suspect charities and nonprofit organizations follow internationally recognized transparency standards and file complete and accurate annual reports. The GOK should pass and enact the proposed Proceeds of Crime and Anti-Money Laundering bill, including the creation of an FIU. The CBK, law enforcement agencies, and the Ministry of Finance should improve coordination to enforce existing laws and regulations to combat money laundering, tax evasion, corruption, and smuggling. The Minister of Finance should revoke or refuse to renew the license of any bank found to have knowingly laundered money, and encourage the CBK to tighten its examinations and audits of banks. Kenyan law enforcement should be more proactive in investigating money laundering and related crimes, and customs should exert control of Kenya's borders.

Korea, Democratic Peoples Republic of

For decades, citizens of the Democratic People's Republic of Korea (DPRK) have been apprehended in international investigations trafficking in narcotics and other forms of criminal behavior, including passing counterfeit U.S. currency (including U.S. $100 "super notes") and trading in counterfeit products, such as cigarettes and pharmaceuticals. There is substantial evidence that North Korean governmental entities and officials have been involved in the laundering of the proceeds of narcotics trafficking and other illicit activities and that they continue to be engaged in counterfeiting and other illegal activities through a number of front companies. The illegal revenue provides desperately needed hard currency for the economy of the DPRK. On October 25, 2006 the Standing Committee of the Supreme People's Assembly of the DPRK adopted a law "On the Prevention of Money Laundering." The law states the DPRK has made it its "consistent policy to prohibit money laundering," but the law is significantly deficient in most important respects and there is no evidence that it has been implemented.

On September 15, 2005, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) designated Macau-based Banco Delta Asia (BDA) as a primary money laundering

concern under Section 311 of the USA PATRIOT Act and issued a proposed rule regarding the bank, citing the bank's systemic failures to safeguard against money laundering and other financial crimes. In its designation of BDA as a primary money laundering concern, FinCEN cited in the Federal Register that "the involvement of North Korean Government agencies and front companies in a wide variety of illegal activities, including drug trafficking and the counterfeiting of goods and currency" and noted that North Korea has been positively linked to nearly 50 drug seizures in 20 different countries since 1990. Treasury finalized the Section 311 rule in March 2007, prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for or on behalf of BDA. This rule remains in effect. Following the Section 311 designation of BDA, the Macau Monetary Authority (MMA) froze approximately U.S. $25 million in North Korean-related accounts at the bank. The MMA subsequently lifted the freeze on these funds following the issuance of the final rule.

The DPRK became a party to the 1988 UN Drug Convention during 2007. It still is not a party to the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, or the UN International Convention for the Suppression of the Financing of Terrorism. North Korea is not a participant in any FATF-style regional body. The DPRK should develop a viable anti-money laundering/counter-terrorist financing regime that comports with international stands. The U.S. Department of State has designated North Korea as a State Sponsor of Terrorism.

Korea, Republic of

The Republic of Korea (ROK) has not been considered an attractive location for international financial crimes or terrorist financing due to foreign exchange controls that are gradually being phased out by 2009. Most money laundering appears to be associated with domestic criminal activity or corruption and official bribery. Laundering the proceeds from illegal game rooms, customs fraud, exploiting zero VAT rates applied to gold bars, trade-based money laundering, counterfeit goods and intellectual property rights violations are all areas of concern. Moreover, criminal groups based in South Korea maintain international associations with others involved in human trafficking, contraband smuggling and related organized crime. As law enforcement authorities have gained more expertise investigating money laundering and financial crimes, they have become more cognizant of the problem.

On the whole, the South Korean government has been a willing partner in the fight against financial crime, and has pursued international agreements toward that end. The Financial Transactions Reports Act (FTRA), passed in September 2001, requires financial institutions to report suspicious transactions to the Korea Financial Intelligence Unit (KoFIU), which operates within the Ministry of Finance and Economy. The KoFIU was officially launched in November 2001, and is composed of 60 experts from various agencies, including the Ministry of Finance and Economy, the Justice Ministry, the Financial Supervisory Commission, the Bank of Korea, the National Tax Service, the National Police Agency, and the Korea Customs Service. KoFIU analyzes suspicious transaction reports (STRs) and forwards information deemed to require further investigation to the Public Prosecutor's office, and, as of 2007, also to the Korean police. The Financial Transaction Reporting Act Amendment Bill was submitted to the National Assembly in January 2007. If passed, this bill will expand the coverage of AML measures to nonfinancial businesses and professions, including casinos, and require financial institutions to file an STR when it is suspected that those funds are related to terrorism.

In 2007, the KoFIU upgraded its anti-money-laundering monitoring system by introducing the Korea Financial Intelligence System based on scoring and data mining methods, in addition to continued Suspicious Transaction Reports (STR), Currency Transaction Reports (CTR) and Customer Due Diligence (CDD) reports. Beginning in January 2006, financial institutions have been required to report within 24 hours all cash transactions of 50 million Korean won (approximately U.S. $54,350) or more by individuals to KoFIU. That reporting threshold will be lowered to 30 million won (approximately U.S. $32,610) in 2008 and to 20 million won (approximately U.S. $21,740) in 2010.

Since January 2006, financial institutions have also been required to perform enhanced customer due diligence, thereby strengthening customer identification requirements set out in the Real Name Financial Transaction and Guarantee of Secrecy Act. Under the enhanced due diligence guidelines, financial institutions must identify and verify customer identification data, including address and telephone numbers, when opening an account or conducting transactions of 20 million won or more.

The STR system was strengthened in 2004 with the introduction of a new online electronic reporting system and the lowering of the monetary threshold under which financial institutions must file STRs from 50 to 20 million won. Reporting entities may file STRs regarding transactions below this threshold. In addition, KoFIU announced that it would consider lowering or removing the threshold for obligatory STR reporting. Improper disclosure of financial reports is punishable by up to five years imprisonment and a fine of up to 30 million won. Between January 1, 2002, and September 30, 2007, KoFIU received a total of 80,417 STRs from financial institutions. The number of such cases has continued to climb noticeably each year, from 275 STRs in 2002, to 1,744 in 2003, 4,680 in 2004, 13,459 in 2005, and 24,149 in 2006. In the first nine months of 2007, there were 36,110 STRs submitted to KoFIU, a 120 percent increase over the same period in 2006. Since 2002 through the end of September 2007, KoFIU has analyzed 79,325 of these reports and provided 7,184 reports to law enforcement agencies, including the Public Prosecutor's Office (PPO), National Police Agency (NPA), National Tax Service (NTS), Korea Customs Service (KCS), and the Financial Supervisory Commission (FSC). Of the 7,184 cases referred to law enforcement agencies, investigations have been completed in 3,661 cases, with 1,402 cases resulting in indictments and prosecutions for money laundering.

In addition, KoFIU supervises and inspects the implementation of internal reporting systems established by financial institutions and is charged with coordinating the efforts of other government bodies. Officials charged with investigating money laundering and financial crimes are beginning to widen their scope to include crimes related to commodities trading and industrial smuggling, and continue to search for possible links of such illegal activities to international terrorist activity. In 2007, KoFIU continued to strengthen advanced anti-money laundering measures (such as the STR and CTR systems), and became an observer to the Financial Action Task Force (FATF) in July 2006. The KoFIU also encouraged financial institutions including small-scale credit unions and cooperatives to adopt a differentiated risk-based due diligence system, focusing on types of customers and transactions, by offering them comprehensive training programs.

Money laundering controls are applied to nonbanking financial institutions, such as exchange houses, stock brokerages, casinos, insurance companies, merchant banks, mutual savings, finance companies, credit unions, credit cooperatives, trust companies, and securities companies. Following the late-2005 arrest of a Korean business executive charged with laundering 8.3 billion won (U.S. $8.17 million) to be used to bribe politicians and bureaucrats, the KoFIU in January 2007 submitted to the National Assembly a revision bill of the Financial Transaction Reports Act to impose anti-money laundering obligations on casinos. KOFIU plans to expand the obligation to intermediaries such as lawyers, accountants, or broker/dealers, currently not covered by Korea's money laundering controls. Any traveler carrying more than U.S. $10,000 or the equivalent in other foreign currency is required to report the currency to the Korea Customs Service.

Money laundering related to narcotics trafficking has been criminalized since 1995, and financial institutions have been required to report transactions known to be connected to narcotics trafficking to the Public Prosecutor's Office since 1997. All financial transactions using anonymous, fictitious, and nominee names have been banned since the 1997 enactment of the Real Name Financial Transaction and Guarantee of Secrecy Act. The Act also requires that, apart from judicial requests for information, persons working in financial institutions are not to provide or reveal to others any information or data on the contents of financial transactions without receiving a written request or consent from the parties

involved. However, secrecy laws do not apply when such information must be provided for submission to a court or as a result of a warrant issued by the judiciary.

In a move designed to broaden its anti-money laundering regime, the ROK also criminalized the laundering of the proceeds from 38 additional offenses, including economic crimes, bribery, organized crime, and illegal capital flight, through the Proceeds of Crime Act (POCA), enacted in September 2001. The POCA provides for imprisonment and/or a fine for anyone receiving, disguising, or disposing of criminal funds. The legislation also provides for confiscation and forfeiture of illegal proceeds.

South Korea still lacks specific legislation on terrorist financing although, as noted above, the Suppression of the Financing of Terrorism Bill was submitted to the National Assembly in January 2007. As of December 2007, three versions of the new counter-terrorism bill were pending in Korea's unicameral legislature, the National Assembly. The proposed Suppression of the Financing of Terrorism bill is crafted to allow the Korean Government additional latitude in fighting terrorism The Suppression of the Financing of Terrorism bill would also permit the government to seize legitimate businesses that support terrorist activity. Currently, under the special act against illicit drug trafficking and other related laws, legitimate businesses can be seized if they are used to launder drug money, but businesses supporting terrorist activity cannot be seized unless other crimes are committed.

Previous attempts to pass similar CTF legislation have not succeeded. Many politicians and nongovernmental organizations (NGOs), recalling past civil rights abuses in Korea by former administrations, oppose the passage of counterterrorism legislation because of fears about possible misuse by the National Intelligence Service and other government agencies.

If passed, the new laws amending the Financial Transactions Reporting Act and the bill Suppression of the Financing of Terrorism would not be enforceable for 12 months. Moreover, the legislation would not correct some potential shortcomings regarding key elements on the criminalization of terrorist financing and suspicious transaction reporting-including excessively high thresholds for reporting all types of suspicious activity. In addition, they may leave some gaps on existing requirements to identify beneficial owners.

Through KoFIU, the government circulates to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and those listed by the European Union under relevant authorities. Korea implemented regulations on October 9, 2001, to freeze financial assets of Taliban-related authorities designated by the UN Security Council. The government then revised the regulations, agreeing to list immediately all U.S. Government-requested terrorist designations under U.S. Executive Order 13224 of December 12, 2002. No listed terrorists are known to be maintaining financial accounts in Korea and there have been no cases of terrorist financing identified since 2002.

Korean government authorities continue to investigate the underground "hawala" system used primarily to send illegal remittances abroad by South Korea's approximately 30,000 foreigners from the Middle East as well as thousands of undocumented foreign workers (mainly ethnic Koreans from Mongolia, Uzbekistan, and Russia). Currently, gamblers who bet abroad often use alternative remittance and payment systems; however, government authorities have criminalized those activities through the Foreign Exchange Regulation Act and other laws. According to an October 2007 report by the Korea Customs Service, there were 1,311 investigations into underground remittances amounting to 2.2 trillion won (approximately U.S. $1.84 billion) in 2003, 1,917 cases totaling 3.66 trillion won (approximately U.S. $3.2 billion) in 2004, 1,901 cases worth 3.56 trillion won (approximately U.S. $3.47 billion) in 2005, 1,924 cases totaling 2.7 trillion (approximately U.S. $2.8 billion) in 2006, and 1,199 cases totaling 1.2 trillion won (approximately U.S. $1.3 billion) in the first half of 2007. The majority of early underground remittance cases were related to the U.S. through 2004; but between

2005 and June 2007, the bulk of cases involved China (35.4 percent, approximately U.S. $2.87 billion), followed by Japan (34.9 percent, approximately U.S. $2.83 billion) and the U.S. (18 percent, U.S. $1.46 billion).

South Korea actively cooperates with the United States and other countries to trace and seize assets. The Anti-Public Corruption Forfeiture Act of 1994 provides for the forfeiture of the proceeds of assets derived from corruption. In November 2001, Korea established a system for identifying, tracing, freezing, seizing, and forfeiting narcotics-related and/or other assets of serious crimes. Under the system, KoFIU is responsible for analyzing and providing information on STRs that require further investigation. The Bank Account Tracing Team under the Narcotics Investigation Department of the Seoul District Prosecutor's Office (established in April 2002) is responsible for tracing and seizing drug-related assets. The Korean Government established six additional new bank account tracking teams in 2004 to serve out of the District Prosecutor's offices in the metropolitan cities of Busan, Daegu, Kwangju, Incheon, Daejon, and Ulsan, to expand its reach. Its legal framework does not allow civil forfeiture.

Korea continues to address the problem of the transportation of counterfeit international currency. The Bank of Korea reported that through September 2007, there were 518 reported cases of counterfeit dollars worth U.S. $1,052,050. Bank experts confirm that the amount of forged U.S. currency is on a decline.

South Korea has a number of free economic zones (FEZs) that enjoy certain tax privileges. However, companies operating within them are subject to the same general laws on financial transactions as companies operating elsewhere, and there is no indication these FEZs are being used in trade-based money laundering schemes or for terrorist financing. Korea mandates extensive entrance screening to determine companies' eligibility to participate in FEZ areas, and firms are subject to standard disclosure rules and criminal laws. In 2007 Korea had seven FEZs, as a result of the June 2004 re-categorization of the three port cities of Busan, Incheon, and Kwangyang as FEZs. They were re-categorized from their previous designation of "customs-free areas" to avoid confusion from the earlier dual system of production-focused FEZs, and logistics-oriented "customs-free zones." Incheon International Airport is slated to become the eighth FEZ.

Korea is a party to the 1988 UN Drug Convention and, in December 2000, signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. Korea is a party to the UN International Convention for Suppression of the Financing of Terrorism. The ROK also signed in December 2003, but has not ratified, the UN Convention against Corruption. Korea is an active member of the Asia/Pacific Group on Money Laundering (APG). Korea also became a member of the Egmont Group in 2002. An extradition treaty between the United States and the ROK entered into force in December 1999. The United States and the ROK cooperate in judicial matters under a Mutual Legal Assistance Treaty, which entered into force in 1997. In addition, the FIU continues to actively pursue information-sharing agreements with a number of countries, and had signed memoranda of understanding with 34 countries-the latest being Malaysia-in April 2007.

The Government of Korea should continue to move forward to adopt and implement its pending counter-terrorism legislation and amendments to the Financial Transaction Reporting Act. Among other priorities, the government should extend its anti-money laundering regime to intermediaries such as lawyers, accountants, broker/dealers and informal lending widely recognized as potential blind spots. Korea should lower the high monetary threshold for reporting suspicious transactions and extend the reporting obligation to attempted transactions. The Republic of Korea should continue its policy of active participation in international anti-money laundering efforts, both bilaterally and in multilateral fora. Spurred by enhanced local and international concern, Korean law enforcement officials and policymakers now understand the potential negative impact of such activity on their country, and have begun to take steps to combat its growth. Their efforts will become increasingly

important due to the rapid growth and greater integration of Korea's financial sector into the world economy.

Kuwait

Kuwait continues to experience unprecedented economic growth that is enhancing the country's regional financial influence, which may make the market susceptible to money laundering. However, money laundering is not believed to be a significant problem, and reportedly that which does take place is generated largely as revenues from drug and alcohol smuggling into the country and the sale of counterfeit goods. However, Kuwait-based terrorist financing, specifically the ongoing threat of charity misuse, continues to be a concern.

Kuwait has ten private local commercial banks, including three Islamic banks, all of which provide traditional banking services comparable to Western-style commercial banks. Kuwait also has one specialized bank, the government-owned Industrial Bank of Kuwait, which provides medium and long-term financing. The three Islamic banks are the Kuwait Finance House (KFH), Boubyan Islamic Bank, and the Kuwait Real Estate Bank (KREB).

The Kuwaiti banking sector was opened to foreign competition in 2001 under the Direct Foreign Investment Law. The Central Bank of Kuwait (CBK) has granted licenses to five foreign banks: BNP Paribas, HSBC, Citibank, the National Bank of Abu Dhabi, and Qatar National Bank. However, the National Bank of Abu Dhabi and Qatar National Bank have not opened offices. Although foreign banks may operate in Kuwait, they are limited to one branch each.

On March 10, 2002, the Emir (Head of State) of Kuwait signed Law No. 35/2002, commonly referred to as Law No. 35, which criminalized money laundering. Law 35 does not criminalize terrorist financing. The law stipulates that banks and financial institutions may not keep or open anonymous accounts or accounts in fictitious or symbolic names and that banks must require proper identification of both regular and occasional clients. The law also requires banks to keep all records of transactions and customer identification information for a minimum of five years, conduct anti-money laundering and terrorist financing training to all levels of employees, and establish proper internal control systems.

Law No. 35 also requires banks to report suspicious transactions to the Office of Public Prosecution (OPP). The OPP is the sole authority that has been designated by law to receive suspicious transaction reports (STRs) and to take appropriate action on money laundering operations. Reports of suspicious transactions are then referred to the CBK for analysis. The anti-money laundering law provides for a penalty of up to seven years imprisonment in addition to fines and asset confiscation. The penalty is doubled if an organized group commits the crime, or if the offender took advantage of his influence or his professional position. Moreover, banks and financial institutions may face a steep fine (approximately $3.3 million) if found in violation of the law.

The law includes articles on international cooperation and the monitoring of cash and precious metals transactions. Currency smuggling into Kuwait is also outlawed under Law No. 35, although cash reporting requirements are not uniformly enforced at ports of entry. Provisions of Article 4 of Law No. 35 require travelers to disclose any national or foreign currency, gold bullion, or other precious materials in their possession valued in excess of 3,000 Kuwaiti dinars (approximately U.S. $10,000) to customs authorities upon entering the country. However, the law does not require individuals to file declaration forms when carrying cash or precious metals out of Kuwait. Several cases have been opened under Law No. 35, but only two cases have gone to court. The cases reportedly involved money smuggling and failure to report currency transactions and did not involve banks.

The National Committee for Anti-Money Laundering and the Combating of Terrorist Financing (AML/CTF) is responsible for administering Kuwait's AML/CTF regime. In April 2004, the Ministry

of Finance issued Ministerial Decision No. 11 (MD No. 11/224), which transferred the chairmanship of the National Committee, formerly headed by the Minister of Finance, to the Governor of the Central Bank of Kuwait. The Committee is comprised of representatives from the Ministries of Interior, Foreign Affairs, Commerce and Industry, Finance, and Labor and Social Affairs; the Office of Public Prosecution; the Kuwait Stock Exchange; the General Customs Authority; the Union of Kuwaiti Banks; and CBK.

Since its inception, the National Committee has pursued its mandate of drawing up the country's strategy and policy with regard to anti-money laundering and terrorist financing; drafting the necessary legislation and amendments to Law No. 35, along with pertinent regulations; coordinating between the concerned ministries and agencies in matters related to combating money laundering and terrorist financing; following up on domestic, regional, and international developments and making needed recommendations in this regard; setting up appropriate channels of communication with regional and international institutions and organizations; and representing Kuwait in domestic, regional, and international meetings and conferences. In addition, the Chairman is entrusted with issuing regulations and procedures that he deems appropriate for the Committee's duties, responsibilities, and organization of its activities.

Kuwait, however, has been unable to fully implement its anti-money laundering law stipulations due in part to structural inconsistencies within the law itself, and the unwillingness of government officials to undertake the necessary steps to rectify such shortfalls. Kuwait's financial intelligence unit (FIU) is not an independent body in accordance with international standards, but rather is under the direct supervision of the Central Bank of Kuwait. In addition, vague delineation of the roles and responsibilities of the government entities involved continues to hinder the overall effectiveness of Kuwait's anti-money laundering regime. Cognizant of these shortcomings, the National Committee continues to promise to revise Law No. 35 in a manner that would bring Kuwait into compliance with international standards, and would criminalize terrorist financing.

In addition to Law No. 35, anti-money laundering reporting requirements and other rules are contained in CBK instructions No. (2/sb/92/2002), which took effect on December 1, 2002, superseding instructions No. (2/sb/50/97). The revised instructions provide for, inter alia, customer identification and the prohibition of anonymous or fictitious accounts (Articles 1-5); the requirement to keep records of all banking transactions for five years (Article 7); electronic transactions (Article 8); the requirement to investigate transactions that are unusually large or have no apparent economic or lawful purpose (Article 10); the requirement to establish internal controls and policies to combat money laundering and terrorist financing, including the establishment of internal units to oversee compliance with relevant regulations (Article 14 and 15); and the requirement to report to the CBK all cash transactions in excess of the equivalent of $10,000 (Article 20). In addition, the CBK distributed detailed instructions and guidelines to help bank employees identify suspicious transactions. At the Central Bank's instructions, in an effort to avoid "tipping off" suspected accountholders, banks are no longer required to block assets for 48 hours on suspected accounts. The Central Bank, upon notification from the Ministry of Foreign Affairs (MFA), issues circulars to units subject to supervision requiring them to freeze the assets of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanctions Committee's consolidated list. Financial entities are instructed to freeze any such assets immediately and for an indefinite period of time, pending further instructions from the Central Bank, which in turn receives its designation guidance from the MFA.

On June 23, 2003, the CBK issued Resolution No. 1/191/2003, establishing the Kuwaiti Financial Inquiries Unit as the FIU within the Central Bank. The FIU is comprised of seven part-time Central Bank officials and headed by the Central Bank Governor. Among its responsibilities, the FIU is to receive and analyze reports of suspected money laundering activities from the OPP, establish a database of suspicious transactions, conduct anti-money laundering training, and carry out domestic and international exchanges of information in cooperation with the OPP. Law No. 35/2002 did not

mandate the FIU to act as the central or sole unit for the receipt, analysis, and dissemination of STRs; instead, these functions were divided between the FIU and OPP.

Banks in Kuwait are required to file STRs with the OPP, rather than directly with the FIU. However, based on a memorandum of understanding with the Central Bank, STRs are referred from the OPP to the FIU for analysis. The FIU conducts analysis and reports any findings to the OPP for the initiation of a criminal case, if necessary. The FIU's access to information is limited, due to its inability to share information abroad without prior approval from the OPP. Kuwaiti officials agree that the current limits on information sharing by the FIU will be addressed by draft amendments to the law, which was revised by the National Committee in 2006 and is currently under governmental review.

There are about 148 money exchange businesses (MEBs) operating in Kuwait that are authorized to exchange foreign currency only. MEBs are not formal financial institutions, so they fall under the supervision of the Ministry of Commerce and Industry (MOCI) rather than the Central Bank. The CBK has reached an agreement that tasks the MOCI with the enforcement of all anti-money laundering (AML) laws and regulations in supervising such businesses. This agreement also stipulates that the MOCI must encourage MEBs to apply for and obtain company licenses, and to register with the CBK.

The MOCI's Office of Combating Money Laundering Operations was established in 2003 and supervises approximately 2,500 insurance agents, brokers and companies; investment companies; exchange bureaus; jewelry establishments (including gold, metal and other precious commodity traders); brokers in the Kuwait Stock Exchange; and other financial brokers. All new companies seeking a business license are required to receive AML awareness training from the MOCI before a license is granted. These firms must abide by all regulations concerning customer identification, record keeping of all transactions for five years, establishment of internal control systems, and the reporting of suspicious transactions. MOCI conducts both mandatory follow-up visits and unannounced inspections to ensure continued compliance. The Office of Combating Money Laundering Operations is also actively engaged in a public awareness campaign to increase understanding about the dangers of money laundering.

Businesses found to be in violation of the provisions of Law No. 35/2002 receive an official warning from MOCI for the first offense. The second and third violations result in closure for two weeks and one month respectively. The fourth violation results in revocation of the license and closure of the business. Reportedly, four exchange houses were closed in 2006 for violating MOCI's instructions, and one case was referred to the Public Prosecutor's Office for violation of customer contracts.

In August 2002, the Kuwaiti Ministry of Social Affairs and Labor (MOSAL) issued a ministerial decree creating the Department of Charitable Organizations (DCO). The primary responsibilities of the department are to receive applications for registration from charitable organizations, monitor their operations, and establish a new accounting system to ensure that such organizations comply with the law both at home and abroad. The DCO has established guidelines for charities explaining donation collection procedures and regulating financial activities. The DCO is also charged with conducting periodic inspections to ensure that charities maintain administrative, accounting, and organizational standards in accordance with Kuwaiti law. The DCO mandates the certification of charities' financial activities by external auditors and limits the ability to transfer funds abroad only to select charities approved by MOSAL. MOSAL also requires all transfers of funds abroad to be made between authorized charity officials. Banks and money exchange businesses (MEBs) are not allowed to transfer any charitable funds outside of Kuwait without prior permission from MOSAL. In addition, any such wire transactions must be reported to the CBK, which maintains a database of all transactions conducted by charities. Unauthorized public donations, including Zakat (alms) collections in mosques, are also prohibited.

In 2005, MOSAL introduced a pilot program requiring charities to raise donations through the sale of government-provided coupons during the Muslim holy month of Ramadan. MOSAL continued this program and in 2007 implemented collection of donations through a voucher system and electronic bank transfers. Plans are underway to further encourage the electronic collection of funds using a combination of electronic kiosks, hand-held collection machines, and text messaging. These devices will generate an electronic record of the funds collected, which will then be subject to MOSAL supervision.

Kuwait is a member of the Gulf Cooperation Council (GCC), which is itself a member of the Financial Action Task Force (FATF). Kuwait is also a member of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body that was established in November 2004. Kuwait has played an active role in the MENAFATF through its participation in the drafting of regulations and guidelines pertaining to charities oversight and cash couriers

Kuwait is a party to the 1988 UN Drug Convention. In May 2006, Kuwait ratified the UN Convention against Transnational Organized Crime. In February 2007, Kuwait ratified the UN Convention against Corruption. Kuwait has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Kuwait should significantly accelerate its ongoing efforts to revise Law No. 35/2002 to criminalize terrorist financing; strengthen charity oversight, especially in overseas operations; develop an independent FIU that meets international standards including the sharing of information with foreign FIUs, as well as sharing between the government and financial institutions. Kuwait should implement and enforce a uniform cash declaration policy for inbound and outbound travelers. Kuwait, like many other countries in the Gulf, relies on STRs to initiate money laundering investigations. As a result, there are few investigations or prosecutions. Instead, Kuwaiti law enforcement and customs authorities should be proactive in identifying suspect behavior that could be indicative of money laundering and/or terrorist financing, such as the use of underground financial systems. Kuwait should become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Laos

Laos is neither an important regional financial center, nor an offshore financial center. Although the extent of the money laundering risks are unknown, illegal timber sales, corruption, cross-border smuggling of goods, illicit proceeds from the sale of methamphetamine (ATS) known locally as “ya ba” (crazy medicine), and domestic crime can be sources of laundered funds. There are continued reports of illicit funds being diverted into some hotel construction, resort development, and industrial tree cropping projects. Anecdotal evidence indicates that large cash deposits related to illicit activities are generally made across the border in Thailand.

The Lao banking sector is dominated by state-owned commercial banks in need of continued reform. Although some foreign banks have branches in Laos, the classic “offshore” banks are not permitted. The small scale and poor financial condition of Lao banks may make them more likely to be venues for certain kinds of illicit transactions. These banks are not optimal for moving large amounts of money in any single transaction, due to the visibility of such movements in the existing small-scale, low-tech environment. Reportedly, there has been no notable increase in financial crimes. There have been no money laundering investigations initiated to date. There is smuggling of consumer goods across the Mekong and in areas near the Chinese border in the north, which could be associated with trade-based money laundering. This smuggling activity is an easy way to avoid paying customs duties and the inconvenience of undergoing weigh station inspections near the Lao and Chinese borders. There are two special economic zones in Savannakhet Province, one each near the Thai and Vietnamese borders on the recently opened Danang-Bangkok highway. Both are awaiting tenants and

there is no indication they are currently used to launder money or finance terrorism. China has leased a similar special economic zone in Luang Nam Tha Province on the China-Thailand Highway at Boten. Within the zone is a casino that potentially could be utilized to launder funds, though there is no evidence that the gaming facility is currently being employed for that purpose. All foreign investment in Laos must first be approved by the government's Ministry of Planning and Investment, which provides due diligence on companies seeking to invest in Laos. Due to general poverty, lack of human capacity, and weak governance, the ability to successfully discover companies bent on illicit transactions is suspect.

Money laundering is a criminal offense in Laos and covered in at least two separate decrees. The penal code contains a provision adopted in November 2005 that criminalizes money laundering and provides sentencing guidelines. On March 27, 2006, the Prime Minister's Office issued a detailed decree, No. 55/PM, on anti-money laundering, based on a model law provided by the Asian Development Bank. Because of the unique nature of Lao governance, the decree is roughly equivalent to a law and is much easier to change than a law passed by the National Assembly. However, it is unclear if the decrees have the same legal effect as provisions in the penal code. One provision of the decree criminalizes money laundering in relation to all crimes with a prison sentence of a year or more. In addition, the decree specifically criminalizes money laundering with respect to: terrorism; financing of terrorism; human trafficking and smuggling; sexual exploitation; human exportation or illegal migration; the production, sales, and possession of narcotic drugs; illicit arms and dynamite trafficking; concealment and trafficking of people's property; corruption; the receipt and giving of bribes; swindling; embezzlement; robbery; property theft; counterfeiting money and its use; murder and grievous bodily injury; illegal apprehension and detention; violation of state tax rules and regulations; extortion; as well as check forgery and the illicit use of false checks, bonds, and other financial instruments. The GOL is considering drafting an AML/CTF law to create a comprehensive AML/CTF regime in line with the international standards as set out by the FATF.

A revision to the penal law in November 2005 includes Article 58/2 which makes financing terrorism punishable by fines of 10 to 50 million Kip (approximately U.S. $10,000-$50,000,), prison sentences from 10 to 20 years, and the possibility of the death penalty. The Bank of Laos has circulated lists of individuals and entities on the UN 1267 Sanctions Committee's consolidated list.

A six-person Anti-Money Laundering Intelligence Unit (AMLIU) was formally established as an independent unit within the Bank of Laos on May 14, 2007, replacing the previous ad hoc Financial Intelligence Unit (FIU). According to the GOL report presented at the July 2007 Asia-Pacific Group plenary, the AMLIU Director and staff "have an action plan to develop full functionality of the AMLIU and to implement provisions of the Decree on Prevention of Money Laundering". The AMLIU acts as an FIU and supervises financial institutions for their compliance with anti-money laundering/counter-terrorist financing decrees and regulations. The AMLIU has no criminal investigative responsibilities, nor does it have any agreements with other FIUs. It is currently beginning a process to set up a National Coordinating Committee that will allow the AMLIU to interact with other relevant Lao governmental agencies such as the Ministry of Public Security. It does not yet have the technology to access the databases of local banks directly. The AMLIU created a five-part, 48-question suspicious transaction report (STR) form and distributed it to all banks along with guidance on October 15, 2007. While banks are required to report suspicious transactions, there have been no reports in 2007 to date, nor have there been any arrests for terrorist financing or money laundering.

The guidance issued by the AMLIU related to suspicious transactions, Bank of Lao No. 66/AMLIU, dated October 15, 2007, does not contain any thresholds for reporting STRs. Instead, it requires financial institutions to take into account a wide range of factors that could indicate an illegal transaction. However, any transaction over U.S. $10,000 is in practice considered worthy of further investigation. Reporting officers are protected against any suit or action related to the reporting

process. While the 2006 decree on money laundering specifically applies to nonbank financial institutions (NBFI), the AMLIU is currently working only with commercial banks as it implements the STR form. It will expand its oversight once the necessary agreements with other supervising agencies are in place. Effective adoption of the STR system is likely to take a number of years. Cultural norms are such that it is unlikely that banks and NBFIs will soon begin generating reports related to customers perceived as being either influential, politically powerful, or coming from prominent families.

Lao law restricts the export of the national currency, the kip, limiting residents and nonresidents to 5,000,000 kip per trip (approximately U.S. $500). Larger amounts may be approved by the Bank of Laos. It is likely that the currency restrictions and undeveloped banking sector encourage the use of alternative remittance systems. When carrying cash across international borders, Laos requires a declaration for amounts over U.S. $5,000 when brought into the country and when being taken out. Failure to show a declaration of incoming cash when exporting it could lead to seizure of the money or a fine. As customs procedures in Laos are undeveloped and open to corruption, enforcing this decree will require political will, development of a professional customs service, compensation reform, further training, and increased capital investments. The Prime Minister's decree on money laundering specifically authorizes asset seizures when connected to money laundering and related crimes. The authority is broadly worded. It is not clear which government authority has responsibility for asset seizures; although indications are that the Ministry of Justice would take the lead. The Government of Laos continues to build a framework of law and institutions; however, at this stage of development, enforcement of enacted legislation and decrees is weak. No legal asset seizures related to narcotics trafficking or terrorism was reported in 2007. A considerable number of assets are reportedly seized by police counternarcotics units from suspected drug traffickers, but these assets usually remain in the custody of the police. Laos is currently drafting a law that will allow for the selling of such seized assets, but, until such a law is passed, most of these assets remain under police custody.

Laos' decree on money laundering authorizes the government to cooperate with foreign governments to deter money laundering of any sort, with caveats for the protection of national security and sovereignty. There are no specific agreements with the United States relating to the exchange of information on money laundering. The Bank of Laos has coordinated with the Embassy on a number of cases related to counterfeit U.S. currency.

The GOL is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The GOL participates in Association of Southeast Asian Nations (ASEAN) regional conferences on money laundering. Laos moved from observer status to membership in the Asia Pacific Anti-Money Laundering Group during the July 2007 Annual Meeting.

To comport with international standards, the Government of Laos should enact comprehensive anti-money laundering/counter-terrorist financing legislation, as decrees are not recognized by international organizations as having the force of law. Such legislation would include, but not be limited to, the promulgation of implementing regulations, the establishment of a viable financial intelligence unit, increasing the number and type of obligated entities, prohibition against "tipping-off", and safe harbor for those reporting suspicious financial transactions to the FIU. Laos should become a party to the UN International Convention for the Suppression of Financing of Terrorism and ratify the UN Convention against Corruption.

Latvia

Latvia is a growing regional financial center that has a large number of commercial banks with a sizeable nonresident deposit base. Sources of laundered money in Latvia primarily involve tax evasion, but also include counterfeiting, corruption, white-collar crime, extortion, financial/banking crimes, stolen cars, contraband smuggling, and prostitution. Some proceeds of tax evasion appear to

originate from outside of Latvia. A portion of domestically obtained criminal proceeds is thought to derive from organized crime. Reportedly, Russian organized crime is active in Latvia. State Narcotics Police have reportedly not found a significant link between smuggled goods on the black market and narcotics proceeds. Currency transactions involving international narcotics trafficking proceeds do not include significant amounts of United States currency and apparently do not derive from illegal drug sales in the United States. However, U.S. law enforcement agencies think that there are ties between U.S criminal elements and the Latvian financial sector, that involve the establishment of U.S.-based shell companies to launder narcotics money through the Latvian financial sector. U.S. law enforcement agencies continue to cooperate with Latvian counterparts on matters of money laundering and affiliated crimes. As Latvia's banking controls tighten, regulators report a pattern of certain accounts moving to Lithuania and Estonia. Regulators assert that alleged criminal activity is moving to these two countries as easier places to conduct business. However, there is insufficient data available for United States authorities to assess this claim.

Latvia is not an offshore financial center, although four special economic zones exist in Latvia providing a variety of significant tax incentives for the manufacturing, outsourcing, logistics centers, and transshipment of goods to other free trade zones. These zones are located at the free ports of Ventspils, Riga, and Liepaja, and in the inland city of Rezekne near the Russian and Belarusian borders. Though there have been instances of reported cigarette smuggling to and from warehouses in the free trade zones, there have been no confirmed cases of the zones being used for money laundering schemes or by the financiers of terrorism. Latvia's banking regulator, the Financial and Capital Market Commission (FCMC), states that the zones are covered by the same regulatory oversight and enterprise registration regulations that exist for nonzone areas.

The Government of Latvia (GOL) criminalized money laundering for all serious crimes in 1998. Latvia's new anti-money laundering (AML) law, The Law on Prevention of Money Laundering and Terrorist Financing is before the Parliament, which is expected to enact it in 2008. Entities subject to the law include credit and financial institutions, tax advisors, external accountants, sworn auditors and lawyers, notaries, company service providers, real estate agents, and lottery and gambling organizers. This new law introduces a risk-based approach, where entities must assess the client's risk for anti-money laundering and terrorist financing, then choose between simplified and enhanced customer due diligence. The law includes compulsory identification of customers who pay cash for transactions of 15,000 euros (approximately U.S. $21,600) or more.

The law requires financial institutions to gather customer identification and institutes record keeping requirements. Financial institutions must keep transaction and identification data for at least five years after ending a business relationship with a client. Institutions engaging in financial transactions must report both suspicious activities and unusual transactions, including large cash transactions, to the financial intelligence unit (FIU). Suspicious transactions must be reported immediately. Financial institutions receive a list of indicators that, when present, activate the reporting requirement for an unusual transaction. Obliged entities must also file an unusual activity report using the indicator list as a basis if there is suspicion regarding laundering or attempted laundering of the proceeds from crime or terrorist financing.

Obliged entities must also report cash transactions. This requirement applies regardless of whether there is one large transaction or several smaller transactions equal to or exceeding 40,000 lats (approximately U.S. $80,000). The new Law on Prevention of Money Laundering and Terrorist Financing will reduce this amount to 15,000 euros (approximately U.S. $21,600) if it passes the 2008 Parliament readings without modification. Financial institutions have the ability to freeze accounts if they suspect money laundering or terrorist financing. If a financial institution finds the activity of an account questionable, it may close the account on its own initiative. Negligent money laundering is illegal in Latvia, and deliberately providing false information about a beneficial owner to a credit or financial institution is also illegal.

Additional amendments to the criminal law enhance the ability of Latvian law enforcement agencies to share information with one another and with Latvia's FCMC. Latvia's Criminal Procedures Law removes many procedural hurdles that had previously served as obstacles to law enforcement agencies aggressively investigating and prosecuting financial crimes. For example, prosecutors no longer need to prove willful blindness of the criminal origin of funds before charging a person or institution with a financial crime.

Council of Ministers Regulation 55, which was replaced by 233, created what is now the Council for Development of the Financial Sector, a coordinator of AML and counter-terrorist financing (CTF) issues on the state level. The Prime Minister chairs this body.

Latvia underwent a joint Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)/ International Monetary Fund (IMF) evaluation in March 2006 which assessed the country's AML regulatory and legal framework. Approved as MONEYVAL's third-round evaluation of Latvia in September 2006, MONEYVAL published the mutual evaluation report (MER) report in June 2007. On the 49 recommendations, 47 of which were applicable, Latvia received 26 ratings of at least "largely compliant," and only five ratings of "noncompliant."

Latvian legislation instituting a cross-border currency declaration requirement took effect on July 1, 2006. The law obliges all persons transporting more than 10,000 euros (approximately U.S. $14,700) in cash or monetary instruments into or out of Latvia, with the exception of into or out of other European Union (EU) member states, to declare the money to a customs officer, or, where there is no customs checkpoint, to a border guard. People moving within the EU are not required to declare. Latvian government agencies share these declarations amongst themselves.

Banks are not allowed to open accounts without conducting customer due diligence and obtaining client identification documents for both residents and nonresidents. When conducting due diligence on legal entities, banks must collect information on incorporation and registration. Sanctions against banks for noncompliance provide for fines up to 100,000 lats (approximately U.S. $200,000). Latvia does not have secrecy laws that prevent the disclosure of client and ownership information to bank supervisors or law enforcement officers. Safe harbor provisions protect reporting individuals.

The Bank of Latvia supervises the currency exchange sector. The FCMC serves as the GOL's unified public financial services regulator, overseeing commercial banks and nonbank financial institutions, the Riga Stock Exchange, and insurance companies. The FCMC conducts regular audits of credit institutions. It also applies sanctions to companies that fail to file mandatory reports of unusual transactions and to those that submit incomplete or deficient information on both the economic activities of businesses, and deficiencies in internal controls of banks. The FIU also works to ensure accurate reporting by determining if it has received corresponding suspicious transactions reports (STRs) when suspicious transactions occur between Latvian banks.

The FCMC has distributed regulations for customer identification and detecting unusual transactions, as well as regulations regarding internal control mechanisms that financial institutions should have in place. The FCMC has the authority to share information with Latvian law enforcement agencies and receive data on potential financial crime patterns uncovered by police or prosecutors. New regulations, drafted by FCMC, in accordance with the adopted Law on the Prevention of Money Laundering and Terrorist Financing should be finalized in early 2008. The Gambling and Lotteries Law states gaming and lottery organizers' rights and obligations in relation to the prevention of legalization of proceeds from criminal activities. Organizers are subject to restrictions and must submit suspicious or unusual transaction reports. They also perform other AML activities as required by Latvian law. The MONEYVAL MER found compliance with requirements of both the European Parliament Directives and the Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations on Terrorist Financing.

In addition to the legislative and regulatory requirements in place, the Association of Latvian Commercial Banks (ALCB) plays an active role in setting standards on AML issues for Latvian banks. The ALCB has adopted the regulations on the "Prevention of Money Laundering" as guidance, as well as a "Declaration on Taking Aggressive Action against Money Laundering," which all Latvian banks signed. The ACLB has also adopted a voluntary measure, which all of the banks observe, to limit cash withdrawals from automated teller machines to 1,000 lats (approximately U.S. $2,000) per day. In October 2007, ALCB approved an "Action Plan to Enhance Transparency of Offshore Customers Serviced by Banks in Latvia on a Compliance Officers Level." Latvia expects to have fully implemented the action plan by July 2008. In addition to acting as an industry representative to government and the regulator, the ACLB organizes regular education courses on AML/CTF issues for bank employees. In the year and a half since the training program began, more than 110 AML/CTF professionals successfully passed a five-day extensive training program and examination. A total of 360 professionals have passed examinations for all of the offered AML/CTF training courses.

The Office for the Prevention of the Laundering of Proceeds Derived from Criminal Activity, known as the Control Service, is Latvia's FIU. Although it is part of the Latvian Prosecutor General's Office, its budget is separate. The Control Service has the overall responsibility for coordination, application and assessment of Latvia's AML policy and its effectiveness. The Control Service received approximately 27,000 reports in 2006. During the first 10 months of 2007 the Latvian FIU received 27,389 reports of suspicious and unusual financial transactions. The Control Service, between January and October, sent 126 cases, which include 1604 reports about suspicious and unusual financial transactions, to law enforcement authorities.

Latvia has taken steps to remedy the situation described by the MER, in which "The vast bulk of the suspicious transaction reports filed are based on the Cabinet of Ministers list of indicators of unusual transactions and the FIU list of indicators/examples. Only a very small minority of the reports are based on suspicions formed under other circumstances. The assessors were informed that the financial institutions follow the FIU list and automatically report transactions that meet at least one of the examples (although the indicators are only examples). This would suggest that the financial institutions may be relying too heavily on the lists provided and might not be exercising appropriate discretion on the circumstances that are not covered by the lists of indicators. This could result in overdependence on the indicators/examples results and submission to the Control Service of significant numbers of reports with little or no value for FIU analytical purposes. It was not possible for the assessors to determine whether or not financial institutions were giving sufficient attention to identifying and reporting real (as distinct from indicator-based) suspicious transactions, as there were some conflicting indications. The assessors were not provided by the Control Service with statistics separating indicator-based STRs from reports based on direct suspicion." The new draft legislation defines a suspicious transaction, but does not list indicators for determining suspicious transactions, forcing the obliged entities to themselves execute transaction analyses.

Latvia has also taken steps to ensure effective implementation of the draft law by providing training to explain the intent and issues to the law's subjects. Both individual financial institutions and entire sectors, such as tax consultants, have received this training. The ALCB organizes five-day seminars for this purpose, and certifies the attending staff. The ALCB provided two such trainings in 2007.

The Control Service conducts a preliminary investigation of the suspicious and unusual reports. It may then forward the information to law enforcement authorities that investigate money laundering cases. The Control Service can disseminate case information to a specialized Anti-Money Laundering Investigation Unit of the Economic Police within the State Police; and the Office for the Combat of Organized Crime. The FIU can also disseminate information to the Financial Police (under the State Revenue Service of the Ministry of Finance); the Bureau for the Prevention and Combat of Corruption (Anti-Corruption Bureau, KNAB) for crimes committed by public officials; the Security Police (for cases concerning terrorism and terrorist financing); and other law enforcement authorities. According

to the draft law, the FIU will have to decide within 14 days of receiving a report whether there are grounds to open a case. If the FIU decides to open a case, it will have the authority to suspend the transaction for 30 days. During the 30 days, the FIU will gather information on the transaction and the parties involved. If the FIU determines grounds for starting a criminal procedure, the FIU can further suspend the transaction for up to 45 days.

The Control Service has access to all state and municipal databases. It does not have direct access to the databases of financial institutions, but requests data as needed. The Control Service shares data with other FIUs and has cooperation agreements on information exchange with FIUs in sixteen countries. Latvia has also signed multilateral agreements with several EU countries to automatically exchange information with the EU financial intelligence units using FIU. The Control Service is a member of the Egmont Group of financial intelligence units.

In 2006, the Latvian FIU issued 125 orders to freeze assets, freezing a total of 12.6 million lats (approximately U.S. $23.5 million). During the first 10 months of 2007 the Latvian FIU issued 80 freezing orders for the total amount of U.S. $12.24 million. Latvia's FIU reports that cooperation from the banking community to trace and freeze assets has been excellent.

The adoption of Latvia's 2005 Criminal Procedures Law provides measures for the seizure and forfeiture of assets. The law enables law enforcement authorities to identify, trace, and confiscate criminal proceeds. Investigators can initiate an action for the seizure of assets recovered during a criminal investigation concurrently with the investigation itself—they do not need to wait until the investigation is complete. During the first 10 months of 2007, the courts returned 14 decisions, leading to the confiscation of approximately U.S. $2.57 million worth of assets on behalf of the state. Proceeds from asset seizures and forfeitures go into the state treasury.

The Prosecutor General's Office maintains a specialized staff to prosecute cases linked to money laundering. The seven staff prosecutors have undergone a special clearance process. In 2006, the Prosecutor General's Office received ten money laundering cases for the prosecution of 47 individuals. In three of the cases, four individuals received convictions and sentences including time in jail. During the first 10 months of 2007 the Prosecutor's Office received 11 money laundering cases for the prosecution of 40 individuals, and reviewed eight money laundering cases resulting in the sentencing of 12 people.

The GOL has initiated measures aimed at combating the financing of terrorism. Article 88-1 of the Criminal Code criminalizes terrorist financing, and meets the United Nations Security Council Resolution (UNSCR) 1373 requirements. It has issued regulations to implement the sanctions imposed by UNSCR 1267. The regulations require that financial institutions report to the Control Service, transactions related to any individual or organization on the UNSCR 1267 Sanctions Committee's consolidated list or on other terrorist lists, including those shared with Latvia by international partners. The Control Service maintains consolidated terrorist finance and watch-lists and regularly distributes these to financial and nonfinancial institutions, as well as to their supervisory bodies. On several occasions, Latvian financial institutions have temporarily frozen monetary funds associated with names on terrorist finance watch lists, including those issued by the U.S. Office of Foreign Assets Control (OFAC), although authorities have found no confirmed matches to names on the list. Article 17 of the AML law authorizes the Control Service to freeze the funds of persons included on one of the terrorist lists for up to six months. Latvia employs the same freezing mechanism with regard to terrorist assets as it uses with those relating to other crimes but includes involvement by the Latvian Security Police. Authorities handle associated investigations, asset and property seizures, in accordance with the Criminal Procedures Law.

Latvia took swift action to improve its AML/CTF regime after the United States outlined concerns in a Notices of Proposed Rulemaking against two Latvian banks on April 26, 2005, under Section 311 of the USA PATRIOT Act. According to the IMF/MONEYVAL MER, "At one point in 2005, 13 of the

23 Latvian banks were subject by the FCMC to the legal status of intensified supervision due to deficiencies in their AML/CTF systems, as the FCMC pursued strong measures to clean up the banking system." On August 14, 2006, the United States issued a final rule imposing a special measure against one of the two banks, VEF Banka, as a financial institution of primary money laundering concern. This measure, specific to VEF Banka, is still in effect.

Latvia permits only conventional money remitters (such as Western Union and Moneygram). The remitters work through the banks and not as separate entities. Alternative remittance services are prohibited in Latvia. The Control Service has not detected any cases of charitable or nonprofit entities used as conduits for terrorist financing in Latvia

Latvia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and eleven other multilateral counter-terrorism conventions. Latvia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. A Mutual Legal Assistance Treaty (MLAT) has been in force between the United States and Latvia since 1999. Latvia is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL).

The GOL should enact additional amendments to its legislation to tighten its AML framework. It should continue to implement and make full use of the 2005 amendments to its Criminal Procedures Law and upon enactment, actively implement and vigorously enforce the new AML law. Supervisory authorities should draft necessary implementing regulations in advance and perform outreach so that upon enactment of the legislation, the obliged entities will be able to comport with the law's requirements. Latvia needs to strengthen its risk-based approach to AML/CTF and take steps to further enhance the preventative aspects of its AML/CTF regime, including improved customer due diligence requirements and increased scrutiny of higher risk categories of transactions, clients and countries. The GOL should continue to take steps to increase information sharing and cooperation between law enforcement agencies at the working level. The GOL should also strengthen its ability to aggressively prosecute and convict those involved in financial crimes.

Lebanon

Lebanon is a financial hub for banking activities in the Middle East and eastern Mediterranean. It has one of the more sophisticated banking sectors in the region. The banking sector continues to record an increase in deposits. As of October 2007, there were 65 banks (51 commercial banks, 11 investment banks, and three Islamic banks) operating in Lebanon with total deposits of U.S. $70 billion. One U.S. bank (Citibank) and four U.S bank representative offices operate in Lebanon: American Express Bank, the Bank of New York, JP Morgan Chase Bank National Association, and Morgan Guarantee Trust Co. of New York.

The Central Bank of Lebanon, Banque du Liban, regulates all financial institutions and money exchange houses. Lebanon imposes no controls on the movement of capital. It has a substantial influx of remittances from expatriate workers and family members, estimated by banking sources to reach U.S. $4 to 5 billion yearly. Such family ties are reportedly involved in underground finance and trade-based money laundering.

Laundered criminal proceeds come primarily from domestic criminal activity, which is largely controlled by organized crime. In May 2007, members of the terrorist group Fatah Al-Islam stole $150,000 from a BankMed branch in Tripoli in northern Lebanon. There is some smuggling of cigarettes and pirated software, but this does not generate large amounts of funds that are laundered through the banking system. There is a black market for counterfeit goods and pirated software, CDs, and DVDs. Lebanese customs officials have had some recent success in combating counterfeit and pirated goods. The illicit narcotics trade is not a principal source of money laundering proceeds.

Offshore banking, trust and insurance companies are not permitted in Lebanon. Legislative Decree No. 46 of 1983 restricts offshore companies' activity to negotiating and signing advisory and services agreements, in addition to sale and purchase contracts of products and goods, all concerning business conducted outside of Lebanon or in the Lebanese Customs Free Zone. Thus, offshore companies are barred from engaging in activities such as industry, banking, and insurance. All offshore companies must register with the Beirut Commercial Registrar, and the owners of an offshore company must submit a copy of their identification. Moreover, the Beirut Commercial Registrar keeps a special register, in which all information about the offshore company is retained. A draft law amending legislation on offshore companies to comply with World Trade Organization's standards was still pending in Parliament as of early November 2007.

There are currently two free trade zones operating in Lebanon, at the Ports of Beirut and Tripoli. The free trade zones fall under the supervision of Customs. Exporters moving goods into and out of the free zones submit a detailed manifest to Customs. Customs is required to report suspected trade-based money laundering or terrorist financing to the Special Investigation Commission (SIC), Lebanon's financial intelligence unit (FIU). Companies using the free trade zone must be registered and must submit appropriate documentation, which is kept on file for a minimum of five years. Lebanon has no cross-border currency reporting requirements. However, since January 2003, Customs checks travelers randomly and notifies the SIC upon discovery of large amounts of cash.

In 2004, Lebanon passed a law requiring diamond traders to seek proper certification of origin for imported diamonds; the Ministry of Economy and Trade (MOET) is in charge of issuing certification for re-exported diamonds. This law was designed to prevent the trafficking of "conflict diamonds" and allowed Lebanon to join the Kimberley Process in September 2005. Prior to this, Lebanon passed a decree in August 2003 prohibiting imports of rough diamonds from countries that are not members of the Kimberley Process. However, in 2005, investigations by Global Witness, a nongovernmental organization, discovered that according to Lebanese customs data, Lebanon imported rough diamonds worth $156 million from the Republic of Congo (ROC), a country removed from the Kimberley Process Certification Scheme for having a "massive discrepancy" between its actual diamond production and declared exports. This documented example of suspect imports from the ROC throw serious doubts on Lebanon's commitment to counter the trade in conflict diamonds. Moreover, there have been consistent reports that many Lebanese diamond brokers in Africa are engaged in the laundering of diamonds—the most condensed form of physical wealth in the world. However, the Kimberley Process office in Lebanon stressed that importers or exporters of rough diamonds must submit an application to MOET to import or export rough diamonds according to the Kimberley Process procedure. The Beirut International Airport is the sole entry point for rough diamonds. The Kimberley Process office at the Beirut International Airport monitors and physically checks the quantities of rough diamonds imported, making sure that imports carry a Kimberley Process certification issued by the country of origin. It also checks on exports of rough diamonds from Lebanon to other member countries of the Kimberley Process. In 2007, Customs had two cases where they seized smuggled rough diamonds that were not carrying the Kimberley certification. Customs kept the rough diamonds in custody and notified the Kimberley Process office at MOET. The Kimberley Process Committee referred the two cases to the State Prosecutor, and both cases are now in the Lebanese court. Yet these safeguards do not address the issue of smuggled diamonds, the purchase of fraudulently obtained Kimberley Process certificates, the laundering of diamonds, or value transfer via the diamond trade.

Lebanon has a large expatriate community throughout the Middle East, Africa, and parts of Latin America. They often work as brokers and traders. Many Lebanese "import-export" concerns are found in free trade zones. Many of these Lebanese brokers network via family ties and are involved with underground finance and trade-based money laundering. Informal remittances and value transfer in the form of trade goods add substantially to the remittance flows from expatriates via official banking

channels. For example, expatriate Lebanese brokers are actively involved in the trade of counterfeit goods in the tri-border region of South America and the smuggling and laundering of diamonds in Africa. There are also reports that many in the Lebanese expatriate business community willingly or unwillingly give "charitable donations" to representatives of Hizballah (which is based in Lebanon). The funds are then repatriated or laundered back to Lebanon.

Lebanon has continued to make progress toward developing an effective money laundering and terrorist financing regime by incorporating the Financial Action Task Force (FATF) Recommendations. Lebanon enacted Law No. 318 in 2001. Law No. 318 created a framework for lifting bank secrecy, broadening the criminalization of money laundering beyond drugs, mandating suspicious transaction reporting, requiring financial institutions to obtain customer identification information, and facilitating access to banking information and records by judicial authorities. Under this law, money laundering is a criminal offense and punishable by imprisonment for a period of three to seven years and by a fine of no less than 20 million Lebanese pounds (approximately $13,270). The provisions of Law No. 318 expand the type of financial institutions subject to the provisions of the Banking Secrecy Law of 1956, to include institutions such as exchange offices, financial intermediation companies, leasing companies, mutual funds, insurance companies, companies promoting and selling real estate and construction, and dealers in high-value commodities. In addition, Law No. 318 requires companies engaged in transactions for high-value items (i.e., precious metals, antiquities) and real estate to also report suspicious transactions.

These companies are also required to ascertain, through official documents, the identity and address of each client and must keep photocopies of these documents as well as photocopies of the operation-related documents for a period of no less than five years. The Central Bank regulates private couriers who transport currency. Western Union and Money Gram are licensed by the Central Bank and are subject to the provisions of this law. Charitable and nonprofit organizations must be registered with the Ministry of Interior and are required to have proper corporate governance, including audited financial statements. These organizations are also subject to the same suspicious reporting requirements.

All financial institutions and money exchange houses are regulated by Law No. 318 which clarifies the Central Bank's powers to: require financial institutions to identify all clients, including transient clients; maintain records of customer identification information; request information about the beneficial owners of accounts; conduct internal audits; and exercise due diligence in conducting transactions for clients.

Law No. 318 also established the Special Investigation Commission (SIC), Lebanon's FIU. SIC is an independent entity with judicial status that can investigate money laundering operations and monitor compliance of banks and other financial institutions with the provisions of Law No. 318. The SIC serves as the key element of Lebanon's anti-money laundering regime and has been the critical driving force behind the implementation process. The SIC is responsible for receiving and investigating reports of suspicious transactions. The SIC is the only entity with the authority to lift bank secrecy for administrative and judicial agencies, and it is the administrative body through which foreign FIU requests for assistance are processed

Since its inception, the SIC has been active in providing support to international criminal case referrals. From January through October 2007, the SIC investigated 182 cases involving allegations of money laundering, terrorism, and terrorist financing activities. Two of the 182 cases were related to terrorist financing. Bank secrecy regulations were lifted in 41 instances. Four cases were transmitted by the SIC to the general state prosecutor for further investigation. As of November 2007, no cases were transmitted by the general state prosecutor to the penal judge. The general state prosecutor reported seven cases to the SIC. Four cases were related to embezzlement and counterfeiting charges, one case to fraud, another to terrorism, and the last one to Interpol intelligence. From January to

October 2007, the SIC froze the accounts of three individuals totaling approximately $50,000 in three of the 182 cases investigated.

During 2003, Lebanon adopted additional measures to strengthen efforts to combat money laundering and terrorist financing, such as establishing anti-money laundering units in customs and the police. In 2003, Lebanon joined the Egmont Group of financial intelligence units. The SIC has reported increased inter-agency cooperation with other Lebanese law enforcement units, such as Customs and Police, as well as with the office of the general state prosecutor. In 2005, a SIC Remote Access Communication system was put in place for the exchange of information between the SIC, Customs, the Internal Security Forces (ISF) anti-money laundering and terrorist financing unit, and the general state prosecutor. The cooperation led to an increase in the number of suspicious transactions reports (STRs), and, as a result, the SIC initiated several investigations in 2007.

To more effectively combat money laundering and terrorist financing, Lebanon also adopted two laws in 2003: Laws 547 and 553. Law 547 expanded Article One of Law No. 318, criminalizing any funds resulting from the financing or contribution to the financing of terrorism or terrorist acts or organizations, based on the definition of terrorism as it appears in the Lebanese Penal Code (which distinguishes between "terrorism" and "resistance"). Law 547 also criminalized acts of theft or embezzlement of public or private funds, as well as the appropriation of such funds by fraudulent means, counterfeiting, or breach of trust by banks and financial institutions for such acts that fall within the scope of their activities. It also criminalized counterfeiting of money, credit cards, debit cards, and charge cards, or any official document or commercial paper, including checks. Law 553 added an article to the Penal Code (Article 316) on terrorist financing, which stipulates that any person who voluntarily, either directly or indirectly, finances or contributes to terrorist organizations or terrorists acts is punishable by imprisonment with hard labor for a period not less than three years and not more than seven years, as well as a fine not less than the amount contributed but not exceeding three times that amount.

Lebanese law allows for property forfeiture in civil as well as criminal proceedings. The Government of Lebanon (GOL) enforces existing drug-related asset seizure and forfeiture laws. Current law provides for the confiscation of assets the court determines to be related to or proceeding from money laundering or terrorist financing. In addition, vehicles used to transport narcotics can be seized. Legitimate businesses established from illegal proceeds after passage of Law 318 are also subject to seizure. Forfeitures are transferred to the Lebanese Treasury. In cases where proceeds are owed to a foreign government, the GOL returns the proceeds to the concerned government.

Lebanon was one of the founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF) and assumed its presidency through 2005. There is no information available on Lebanon's mutual evaluation by MENAFATF.

The SIC circulates to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224 and those that European Union have designated under their relevant authorities. As of early November 2007, SIC signed seventeen memoranda of understanding with counterpart FIUs concerning international cooperation.

In September 2007 the Lebanese Cabinet established a national committee that is chaired by the Ministry of Interior to examine the financing of terrorism. The Cabinet also expanded membership of The National Committee for coordinating AML policies to include representatives from five Ministries: Justice, Finance, Interior, Foreign Affairs, and Economy, in addition to a representative from Beirut Stock Exchange. Yet prosecutions and convictions are still lacking. The end of the Syrian military occupation in April 2005 and the gradual decline of Syrian influence over the economy (both licit and illicit), security services, and political life in Lebanon may present an opportunity for the GOL to further strengthen its efforts against money laundering, corruption, and terrorist financing.

Lebanon is a party to the 1988 UN Drug Convention, although it has expressed reservations to several sections relating to bank secrecy. It has signed and ratified the UN Convention against Transnational Organized Crime. Lebanon is not a party to the UN Convention against Corruption or the UN International Convention for the Suppression of the Financing of Terrorism.

The GOL should encourage more efficient cooperation between financial investigators and other concerned parties, such as police and customs, which could yield significant improvements in initiating and conducting investigations. It should become a party to the UN Convention against Corruption and the UN International Convention for the Suppression of Terrorist Financing. Per FATF Special Recommendation Nine on bulk cash smuggling, the GOL should mandate and enforce cross-border currency reporting. Lebanese law enforcement authorities should examine domestic ties to the international network of Lebanese brokers and traders that are commonly found in underground finance, trade fraud, and trade-based money laundering.

Liechtenstein

The Principality of Liechtenstein has a well-developed offshore financial services sector, liberal incorporation and corporate governance rules, relatively low tax rates, and a tradition of strict bank secrecy. All of these conditions have contributed significantly to the ability of financial intermediaries in Liechtenstein to attract funds from abroad. These same conditions have historically made the country attractive to money launderers using the system to launder their proceeds from fraud. Although accusations of misuse of Liechtenstein's banking system persist, the principality has made substantial progress in its efforts against money laundering in recent years.

Liechtenstein's financial services sector includes 16 banks, three nonbank financial companies, 16 public investment companies, and a number of insurance and reinsurance companies. The three largest banks control ninety percent of the market. Liechtenstein's 230 licensed fiduciary companies and 60 lawyers serve as nominees for or manage more than 75,000 entities (mostly corporations or trusts) available primarily to nonresidents of Liechtenstein. Approximately one third of these entities hold controlling interests in separate entities chartered outside of Liechtenstein. Laws permit corporations to issue bearer shares.

Narcotics-related money laundering has been a criminal offense in Liechtenstein since 1993, and the number of predicate offenses for money laundering has increased over time. The Government of Liechtenstein (GOL) is reviewing the Criminal Code to further expand the list of predicate offenses. Article 165 criminalizes laundering one's own funds and imposes penalties for money laundering.

Liechtenstein enacted its first general anti-money laundering (AML) legislation in 1996. Although this law applied some money laundering controls to financial institutions and intermediaries operating in Liechtenstein, the AML regime at that time suffered from serious systemic problems and deficiencies. In response to international pressure, beginning in 2000, the GOL took legislative and administrative steps to improve its AML regime.

Liechtenstein's primary piece of AML legislation, the Due Diligence Act (DDA), applies to banks, e-money institutions, casinos, dealers in high-value goods, and a number of other entities. Along with the Due Diligence Ordinance, the DDA sets out the basic requirements of the AML regime in accordance with the Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations on Terrorist Financing in the areas of customer identification, suspicious transaction reporting, and record keeping. The DDA prohibits banks and postal institutions from engaging in business relationships with shell banks and from maintaining bearer-payable passbooks, accounts, and deposits. Legislation does not, however, address negligent money laundering. The suspicious-transaction reporting requirement applies to banks, insurers, financial advisers, postal services, exchange offices, attorneys, financial regulators, casinos, and other entities. The GOL has

reformed its suspicious transaction reporting system to permit reporting for a much broader range of offenses than in the past. The reporting requirement now uses the basis of a suspicion, rather than the previous standard of "a strong suspicion."

The GOL announced in August 2007, that it would implement legislation enacting EU regulations requiring that money transfers above 15,000 euros (U.S. $17,678) include information on the identity of the sender, including his or her name, address, and account number. The proposed measures, to take effect by early 2008, will ensure that this information will be immediately available to appropriate law enforcement authorities. The information will assist them in detecting, investigating, and prosecuting money launderers, terrorist financiers, and other criminals.

The Financial Market Authority (FMA) serves as Liechtenstein's central financial supervisory authority. FMA has assumed the responsibilities of several former administrative bodies, including the Financial Supervisory Authority and the Due Diligence Unit, both of which once exercised responsibility over money laundering issues. FMA reports exclusively to the Liechtenstein Parliament, making it independent from Liechtenstein's government. The FMA supervises a large variety of financial actors, including banks, finance companies, insurance companies, currency exchange offices, and real estate brokers. FMA works closely with Liechtenstein's financial intelligence unit (FIU), the Office of the Prosecutor, and the police.

Liechtenstein's FIU, known as the Einheit fuer Finanzinformationen (EFFI), receives, analyzes and disseminates suspicious transaction reports (STRs) relating to money laundering and terrorist financing. The EFFI became operational in March 2001. The EFFI has its own database as well as access to various governmental databases. However, EFFI cannot seek additional financial information unrelated to a filed suspicious transaction reports (STR.)

In 2006, the FIU received 163 STRs. Of the total of 163 STRs, banks submitted 84, professional trustees submitted 65, lawyers submitted nine, and investment companies and the Postal Service submitted one apiece. Three STRs were submitted by Liechtenstein authorities or the FMA. U.S. nationals identified as subjects of STRs comprised four percent. In 2006, the FIU received 139 inquiries from 21 different FIUs and sent 158 inquiries to 23 different FIUs. Information regarding the number of STRs received in 2007 is not yet available.

STRs have generated several successful money laundering investigations. EFFI works closely with the prosecutor's office and law enforcement authorities, in particular with a special economic and organized crime unit of the National Police known as EWOK. Police can use special investigative measures when authorized to do so by a Special Investigative Judge.

Liechtenstein has legislation to seize, freeze, and share forfeited assets with cooperating countries. The Special Law on Mutual Assistance in International Criminal Matters gives priority to international agreements. Money laundering is an extraditable offense, and Liechtenstein grants legal assistance on the basis of dual criminality. Article 235A provides for the sharing of confiscated assets. Liechtenstein has not adopted the EU-driven policy of reversing the burden of proof (i.e., forcing a defendant to prove assets were legally obtained instead of the state being required to prove their illicit nature.)

A series of amendments to Liechtenstein laws, along with amendments to the Criminal Code and the Code of Criminal Procedure, criminalize terrorist financing. Liechtenstein has implemented United Nations Security Council Resolutions (UNSCRs) 1267 and 1333. The GOL can freeze the accounts of individuals and entities that are designated pursuant to these UNSCRs. The GOL updates its implementing ordinances regularly.

The GOL has improved its international cooperation provisions in both administrative and judicial matters. A mutual legal assistance treaty (MLAT) between Liechtenstein and the United States entered into force on August 1, 2003. The U. S. Department of Justice has acknowledged Liechtenstein's

cooperation in the Al-Taqwa Bank case and in other fraud and narcotics cases. The FIU has in place memoranda of understanding (MOUs) with nine FIUs, and seven others are under negotiation.

Liechtenstein is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), which discussed the most recent Liechtenstein assessment at its September 2007 plenary. However, the report is not yet available. EFFI is a member of the Egmont Group. The GOL is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and the UN International Convention for the Suppression of the Financing of Terrorism. On March 9, 2007, Liechtenstein acceded to the 1988 UN Drug Convention. Liechtenstein has also signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Liechtenstein has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and has adopted the EU Convention on the Suppression of Terrorism.

The Government of Liechtenstein has made consistent progress in addressing the shortcomings in its AML regime. It should continue to build upon the foundation of its evolving anti-money laundering and counter-terrorist financing regime. Liechtenstein should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Liechtenstein should enact and implement legislation requiring the reporting of cross-border currency movements and ensure that trustees and other fiduciaries comply fully with all aspects of AML legislation and attendant regulations, including the obligation to report suspicious transactions. The GOL should prohibit the issuance and use of corporate bearer shares. The FIU should have access to additional financial information. While Liechtenstein recognizes the rights of third parties and protects uninvolved parties in matters of confiscation, the government should distinguish between bona fide third parties and others. Liechtenstein should consider discarding its list of predicate offenses in favor of an all-crimes approach.

Luxembourg

Despite its standing as the second-smallest member of the European Union (EU), Luxembourg is one of the largest financial centers in the world. While Luxembourg is not a major hub for illicit narcotics distribution, the size and sophistication of its financial sector create opportunities for money laundering, tax evasion, and other financial crimes. Luxembourg is an offshore financial center. Although there are a handful of domestic banks operating in the country, the majority of banks registered in Luxembourg are foreign subsidiaries of banks in Germany, Belgium, France, Italy, and Switzerland. A significant share of Luxembourg's suspicious transaction reports (STRs) are generated from transactions involving clients in these countries.

Luxembourg's strict bank secrecy laws allow international financial institutions to benefit from and operate a wide range of services and activities. With over U.S. $3.1 trillion in domiciled assets, Luxembourg is the second largest mutual fund investment center in the world, after the United States. As of October 2007, 157 registered banks existed, with a collective balance sheet total reaching approximately U.S. $1.38 trillion. In addition, as of January 2007, a total of 2,238 "undertakings for collective investment" (UCIs), or mutual fund companies, whose net assets had reached over approximately U.S. $2.66 trillion operated from Luxembourg or traded on the Luxembourg stock exchange. Luxembourg has approximately 15,000 holding companies, 95 insurance companies, and 260 reinsurance companies. In January 2006, the Luxembourg Stock Exchange listed over 39,000 securities issued by nearly 4,100 entities from 105 countries. Luxembourg also has 116 registered venture capital funds (Societe d'investissement en capital a risqué, or "SICAR").

The Law of July 7, 1989, updated in 1998 and 2004, serves as Luxembourg's primary anti-money laundering (AML) and counter-terrorist financing (CTF) law, criminalizing the laundering of proceeds for an extensive list of predicate offenses, including narcotics trafficking. The laws implement the

EU's money laundering directives and provide customer identification, recordkeeping, and suspicious transaction reporting requirements. Corruption, weapons offenses, fraud committed against the EU and organized crime are on Luxembourg's list of predicate offenses for money laundering. The entities subject to money laundering regulations include banks, pension funds, insurance brokers, UCIs, management companies, external auditors, accountants, notaries, lawyers, casinos, gaming establishments, real estate agents, tax and economic advisors, domiciliary agents, insurance providers, and dealers in high-value goods such as jewelry and vehicles All obliged entities are required to file STRs with the financial intelligence unit (FIU). The current AML law does not cover SICAR entities.

The law also imposes strict "know your customer" (KYC) requirements on obliged entities for all customers, including beneficial owners, trading in goods worth at least 15,000 euros (U.S. $21,900). If the transaction or business relationship is remotely based, the law details measures required for customer identification. Entities must proactively monitor their customers for potential risk. Luxembourg's laws also prohibit "tipping off". Financial institutions must also ensure adequate internal organization and employee training, and must cooperate with authorities, The banking community generally cooperates with enforcement efforts to trace funds and seize or freeze bank accounts.

Although Luxembourg is well known for its strict banking secrecy laws, banking secrecy laws do not apply in investigations and prosecutions of money laundering and other criminal cases. A court order is not necessary for the competent authorities to investigate account information in suspected money laundering cases or in response to an STR. Financial professionals have a legal obligation to cooperate with the public prosecutor in investigating such cases. To obtain a conviction for money laundering, prosecutors must prove criminal intent rather than negligence. Negligence, however, is subject to scrutiny by competent authority, with sanctions for noncompliance varying from 1,250 to 1,250,000 euros (U.S. $1,825 to $1,825,000) and, potentially, forfeiture of the professional license. Luxembourg's regulatory authorities believe these fines to be stiff enough so as to encourage strict compliance.

On November 9, 2007, the Council of Government approved Bill 5811 to implement the Third EU Money Laundering directive. However, by year's end, the bill had not gone to the full chamber for deliberation.

At the close of 2007, Parliament was considering Bill 5756, which would bring Luxembourg into conformity with the first recommendation of the Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations. This recommendation encourages countries to criminalize money laundering and "apply the crime of money laundering to all serious offenses, with a view to including the widest range of predicate offenses." Bill 5756, when enacted, will widen the scope of predicate offenses in Luxembourg law and set forth minimum sentence guidelines for money laundering offenses to comport with the FATF recommendations. This bill was introduced into Parliament in August 2007, but was not scheduled for a vote at the end of 2007.

The Financial Supervision Commission (Commission de Surveillance du Secteur Financier or CSSF) is an independent body under the Ministry of Finance that acts as the supervisory authority for banks, credit institutions, the securities market, some pension funds, financial sector professionals, and other financial sector entities covered by the country's AML/CTF laws. Banks must undergo audits under CSSF supervision. All entities involved in oversight functions, including registered independent auditors, in-house bank auditors, and the CSSF, can obtain the identities of the beneficial owners of accounts. The CSSF establishes the standards for and grants "financial sector professional" ("professionnel du secteur fiancier," or PSF) status to financial sector entities. Originally covering only individual financial sector professionals having access to customer information subject to bank secrecy laws, the CSSF recently established a sub-category for service providers with potential access to that information, such as transaction-clearing houses, information technology consultants, and data

warehousing services. With this status, banks have the flexibility to outsource some services while guaranteeing continued compliance with banking secrecy laws to their customers. The CSSF regulates the PSF status tightly, frequently issuing circulars and updating accreditation requirements. Accordingly, the PSF holds coveted status in the Luxembourg financial community.

The Luxembourg Central Bank oversees the payment and securities settlement system, and the Insurance Commissioner's Office (Commissariat aux Assurances or CAA), also under the Ministry of Finance, is the regulatory authority for the insurance sector.

Under the direction of the Ministry of the Treasury, the CSSF has established a committee, the Anti-Money Laundering Steering Committee (Comite de Pilotage Anti-Blanchiment or COPILAB), composed of supervisory and law enforcement authorities, the financial intelligence unit (FIU), and financial industry representatives. The committee meets monthly to develop a common public-private approach to strengthen Luxembourg's AML regime.

Luxembourg's laws and regulations do not distinguish between onshore and offshore activities. Foreign institutions seeking establishment in Luxembourg must demonstrate prior establishment in a foreign country and meet stringent minimum capital requirements. Nominee (anonymous) directors are not permitted. Companies must maintain a registered office in Luxembourg, and authorities perform background checks on all applicants. A government registry publicly lists company directors.

Luxembourg permits bearer shares. Officials contend that bearer shares do not pose a money laundering concern because of KYC laws that require banks to know the identities of beneficial owners. Banks must undergo annual audits under CSSF supervision.

Luxembourg's FIU, (Cellule de Renseignement Financier), is part of the State Prosecutor's Office and housed within Luxembourg's Ministry of Justice. The FIU consists of three State Prosecutors and one analyst. The FIU State Prosecutors pursue economic and financial crimes in Luxembourg, and spend significant portions of their time preparing for cases involving financial crimes. They are also occasionally called upon to prosecute cases not involving financial crimes.

The FIU receives and analyzes the STRs from all obliged entities. The FIU provides members of the financial community with access to updated information on money laundering and terrorist financing practices. The FIU issues circulars to all financial sector-related professionals who are not regulated under the CSSF as well as notifies the financial sector about terrorist financing designations promulgated by the EU and United Nations (UN).

By late November 2007, obliged institutions filed a total of 679 STRs, compared to a total of 754 in 2006. The number of individuals referenced in STRs has decreased dramatically from 2,471 in 2004 to 1,452 in 2006, which the FIU attributes to increased financial sector confidence in KYC practices. Among the individuals referenced in STRs in 2006, 28 resided in the United States. Of 255 confirmed cases of suspicious activity in 2006, 34 related to organized crime (including terrorist financing), 14 to narcotics-related money laundering, and 24 were related to corruption.

The FIU works with the AML Unit of the Judicial Police. Luxembourg prosecuted three money laundering cases in 2006 and four in 2007. Three were of particular note: In May 2006, two individuals were convicted of laundering narcotics-trafficking proceeds and received sentences of 72 months and 12 months of imprisonment respectively. In November 2006, five individuals were acquitted of money laundering charges when the court found that the State had not sufficiently established the linkage between the funds and either narcotics trafficking or an organized crime enterprise. The government seeks to close this legal vulnerability with Bill 5756, which expands the list of predicate offenses. Also in November 2006, a Dutch lawyer for a convicted drug trafficker was acquitted of attempted money laundering charges in November 2006, but an appellate court overturned the acquittal in May 2007. The defendant appealed his conviction to Luxembourg's Supreme Court, which should reach a judgment in 2008.

Luxembourg law only allows for criminal forfeitures and public takings. Narcotics related proceeds are pooled in a special fund to invest in anti-drug abuse programs. Luxembourg can confiscate funds found to be the result of money laundering even if they are not the proceeds of a crime. The Government of Luxembourg (GOL) can, on a case-by-case basis, freeze and seize assets, including assets belonging to legitimate businesses used for money laundering. The FIU freezes assets and issues blocking orders when necessary. The government has adequate police powers and resources to trace, seize, and freeze assets without undue delay. Luxembourg has independently frozen several accounts. This has resulted in court challenges by the account holders, after which nearly all of the assets were subsequently released. Luxembourg has a comprehensive system not only for the seizure and forfeiture of criminal assets, but also for the sharing of those assets with other governments. Bill 5019, of August 2007, allows Luxembourg to seize assets on the basis of a foreign criminal conviction, even when there is no specific treaty in place with that country.

The Ministry of Justice studies and reports on potential abuses of charitable and nonprofit entities. Justice and Home Affairs ministers from Luxembourg and other EU member states agreed in early December 2005, to take into account five principles with regard to implementing FATF Special Recommendation VIII on nonprofit organizations: safeguarding the integrity of the sector; dialogue with stakeholders; continuing knowledge development of the sector; transparency, accountability and good governance; and effective, proportional oversight.

Luxembourg's authorities have not found evidence of the widespread use of alternative remittance systems or trade-based money laundering. Luxembourg government officials maintain that because AML rules would apply to such systems, they are not considering separate legislative or regulatory initiatives to address them.

The GOL actively disseminates to its financial institutions information concerning suspected individuals and entities on the United Nations Security Council Resolution 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to Executive Order 13224. Luxembourg's authorities can and do take action against groups targeted through the EU designation process and the UN. Luxembourg does not have legal authority to independently designate terrorist groups or individuals. The government has been working on legislation with regard to this issue for more than three years, but the legislation remains in the drafting process. Government prosecutors are confident that they could use existing judicial authority if any institution were to identify a terrorist financier. Although bilateral freeze requests have a limit of three months, designations under the EU, UN, or international investigation processes continue to be subject to freezes for an indefinite time period. .

Luxembourg's laws facilitating international cooperation in money laundering include the Act of August 8, 2000, which enhances and simplifies procedures on international judicial cooperation in criminal matters; and the Law of June 14, 2001, which ratifies the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. During its EU Presidency, Luxembourg shepherded the draft of the Third Money Laundering and Terrorist Financing Directive through the EU's legislative process. Luxembourg expects to transpose this Directive into national law in 2008 with the passage of Bill 5811.

Luxembourg cooperates with, and provides assistance to foreign governments in their efforts to trace, freeze, seize and forfeit assets. During 2007, Luxembourg responded to four mutual legal assistance treaty requests from the U.S. and in return requested U.S. government assistance in three cases. Dialogue and other bilateral proceedings between Luxembourg and the United States have been extensive. Upon request from the United States, Luxembourg froze the bank accounts of individuals suspected of involvement in terrorism. Luxembourg also worked closely with the U.S. Department of Justice throughout 2007, on several drug-related money laundering cases as well as one possible terrorist financing case. In October 2006, the United States and Luxembourg announced a sharing

agreement in which they would divide equally 11,366,265 euros (then approximately $14,548,820) of forfeited assets of two convicted American narcotics traffickers who had deposited the monies in Luxembourg bank accounts. Luxembourg has placed a priority on progressing with the legal instruments implementing the extradition and mutual legal assistance agreements the United States signed with the European Union in 2003. In December 2007, the Luxembourg Parliament gave final approval to both the bilateral U.S.-Luxembourg and multilateral U.S.-EU extradition and mutual legal assistance agreements.

Luxembourg is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism but has not yet ratified the UN Convention against Transnational Organized Crime. On November 6, 2007, Luxembourg ratified the UN Convention against Corruption.

Luxembourg is a member of the Financial Action Task Force (FATF), which, in a 2004 report, commented that Luxembourg was "broadly compliant with almost all of the FATF Recommendations." The Luxembourg FIU is a member of the Egmont Group. Luxembourg and the United States have had a mutual legal assistance treaty (MLAT) since February 2001. Luxembourg has consistently provided training and assistance in money laundering matters to officials in countries whose regimes are in the development stage.

The Government of Luxembourg has enacted laws and adopted practices that help prevent the abuse of its bank secrecy laws and has enacted a comprehensive legal and supervisory anti-money laundering regime. Luxembourg has steadily enacted AML/CTF laws, policies, and procedures. However, the scarce number of financial crime cases is of concern, particularly for a country that has such a large financial sector. Luxembourg should take action to delineate in legislation regulatory, financial intelligence, and prosecutorial activities among governmental entities in the fight against money laundering and terrorist financing. The situation is most acute regarding the lack of a distinct legal framework for the FIU whose staff, activities, and authorities are divided among at least four different ministries. The State Prosecutors in the FIU should be exempt from nonfinancial crime duties and the FIU should increase the number of analytical staff to effectively analyze and disseminate the volume of STRs that the FIU receives. Luxembourg should pass legislation creating the authority for it to independently designate those who finance terrorism. Luxembourg would be well served to have the authority to designate suspected terrorists. Luxembourg should also enact legislation to address the continued use of bearer shares and consider specifically extending AML legislation to include SICAR entities. Luxembourg should become a party to the UN Convention against Transnational Organized Crime.

Macau

Under the one country/two systems principle that underlies Macau's 1999 reversion to the People's Republic of China, Macau has substantial autonomy in all areas of governance except defense and foreign affairs. Macau's free port, a lack of foreign exchange controls, limited institutional capacity and a rapidly expanding economy based on gambling and tourism create an environment that can be exploited for money laundering purposes. Macau is a gateway to China, and can be used as a transit point to remit funds and criminal proceeds to and from China. Macau's economy is heavily dependent on gaming. The gaming sector continues to be a significant vulnerability. Macau's offshore financial sector is not fully developed.

The primary money laundering methods in Macau's financial system are wire transfers; currency exchange/cash conversion; bulk movement of cash; the use of casinos to remit or launder money; and the use of nominees, trusts, family members, or third parties to transfer cash. Most of these cases are related to financial fraud, bribery, embezzlement, organized crime, counterfeiting, and drug-related

crimes. There have been no reported instances of terrorism-related financial crimes. Crimes related to financial fraud appear to be increasing, while drug-related crimes are becoming less common.

Macau has taken several steps over the past three years to improve its institutional capacity to tackle money laundering. On March 23, 2006, the Macau Special Administrative Region (MSAR) Government passed a 12-article bill on the prevention and repression of money laundering that incorporates aspects of the revised FATF Forty Recommendations. The law expands the number of sectors covered by Macau's previous anti-money laundering (AML) legislation, includes provisions on due diligence, and broadens the definition of money laundering to include all serious predicate crimes. The AML law also authorizes the establishment of a financial intelligence unit (FIU), which began operations in November 2006. The law provides for 2-8 years imprisonment for money laundering offenses, and if a criminal is involved in organized crime or triad-related money laundering, increases the penalties by one-half. The new law also allows for fines to be added to the time served and eliminates a provision reducing time served for good behavior.

The 2006 law also extends the obligation of suspicious transaction reporting to lawyers, notaries, accountants, auditors, tax consultants and offshore companies. Covered businesses and individuals must meet various obligations, such as the duty to confirm the identity of their clients and the nature of their transactions. Businesses must reject clients that refuse to reveal their identities or type of business dealings. The law obliges covered entities, including casinos, to send suspicious transaction reports (STRs) to the relevant authorities and cooperate in any follow-up investigations.

On March 30, 2006, the MSAR also passed new counterterrorism legislation aimed at strengthening measures to counter terrorist financing (CTF). The law partially implements UNSCR 1373 by making it illegal to conceal or handle finances on behalf of terrorist organizations. Individuals are liable even if they are not members of designated terrorist organizations themselves. The legislation also allows prosecution of persons who commit terrorist acts outside of Macau in certain cases, and would mandate stiff penalties. However, the legislation does not authorize the freezing of terrorist assets outside normal legal channels, nor does it discuss international cooperation on terrorist financing. In January 2005, the Monetary Authority of Macau issued a circular to all banks and other authorized institutions requiring them to maintain a database of suspected terrorists and terrorist organizations.

Macau's financial system is governed by the 1993 Financial System Act and amendments, which lay out regulations to prevent use of the banking system for money laundering. The Act imposes requirements for the mandatory identification and registration of financial institution shareholders, customer identification, and external audits that include reviews of compliance with anti-money laundering statutes. The 1997 Law on Organized Crime criminalizes money laundering for the proceeds of all domestic and foreign criminal activities, and contains provisions for the freezing of suspect assets and instrumentalities of crime. Legal entities may be civilly liable for money laundering offenses, and their employees may be criminally liable.

The 1998 Ordinance on Money Laundering sets forth requirements for reporting suspicious transactions to the Judiciary Police and other appropriate supervisory authorities. These reporting requirements apply to all legal entities supervised by the regulatory agencies of the MSAR, including pawnbrokers, antique dealers, art dealers, jewelers, and real estate agents. In October 2002, the Judiciary Police set up the Fraud Investigation Section to receive suspicious transaction reports (STRs) in Macau and to undertake subsequent investigations. In 2006, the newly established Financial Intelligence Unit (FIU) assumed responsibility for receiving STRs and forwarding actionable reports to the Judiciary Police for investigation. In November 2003, the Monetary Authority of Macau issued a circular to banks, requiring that STRs be accompanied by a table specifying the transaction types and money laundering methods, in line with the collection categories identified by the Asia/Pacific Group on Money Laundering. Macau law provides for forfeiture of cash and assets that assist in or are

intended for the commission of a crime. There is no significant difference between the regulation and supervision of onshore and of offshore financial activities.

On September 15, 2005, the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) designated Macau-based Banco Delta Asia (BDA) as a primary money laundering concern under Section 311 of the USA PATRIOT Act and issued a proposed rule regarding the bank, In its designation of BDA as a primary money laundering concern, FinCEN cited in the Federal Register that "the involvement of North Korean Government agencies and front companies in a wide variety of illegal activities, including drug trafficking and the counterfeiting of goods and currency" and noted that North Korea has been positively linked to nearly 50 drug seizures in 20 different countries since 1990. Following an investigation of BDA conducted with the cooperation of the Macanese authorities, Treasury finalized the Section 311 rule in March 2007, prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for or on behalf of BDA. This rule remains in effect.

Shortly after the U.S. designation, The Monetary Authority took control of Banco Delta Asia and froze approximately U.S. $25 million in accounts linked to North Korea. The Government of Macau announced in March 2007 that it would continue to maintain control over Banco Delta Asia for at least six more months to resolve the Banco Delta Asia situation. In April, 2007, the Macanese authorities released the $25 million North Korean-related funds frozen at BDA. In September, 2007, The Treasury Department's Financial Crimes Enforcement Network denied two petitions filed on behalf of BDA and its owners to lift the Section 311 Final Rule designating BDA as a "primary money laundering concern." On September 30, 2007 Macau Monetary Authority announced that Banco Delta Asia would be returned immediately to its shareholders, but continued international restrictions on BDA and its subsidiaries outside of Macau that limit BDA to pataca currency business in Macau.

A Macau Monetary Authority official serves as the head of the FIU. As of October 2007, in addition to the FIU Head, the staff consisted of two officials (seconded from the Insurance Bureau and the Monetary Authority), a judiciary police official, and two information technology staff. The FIU works with the Macau Judicial Police on investigation of suspicious transaction reports (STRs) and with the Public Prosecutors Office on prosecution of offenders. The FIU moved into permanent office space in January 2007 and is accepting STRs from banks, financial institutions and the Gaming Inspectorate.

The gaming sector and related tourism are critical parts of Macau's economy. Taxes from gaming in the first eleven months of 2007 increased by 48.3 percent from the same period in 2006 and comprised 71percent of government revenue in the first eleven months of 2007. Gaming revenue in the first nine months of 2007 exceeded the 2006 total and account for well over 50 percent of Macau's GDP. The MSAR ended a long-standing gaming monopoly early in 2002 when it awarded concessions to two additional operators, the U.S.-based Las Vegas Sands and Wynn Corporations. Macau now effectively has six separate casino licensees operating 28 casinos: three concession holders Sociedade de Jogos de Macau (SJM), Galaxy and Wynn: and three sub concession holders: Las Vegas Sands, MGM and PBL/Melco. Las Vegas Sands opened its first casino, the Sands, on May 18, 2004 and its second the Venetian-Macao in September 2007. MGM opened its first Macau casino in December 2007. Wynn opened its casino in September 2006. A consortium including Australia's PBL and Macau's Melco operates the Crown casino, which opened in May 2007 and runs several slot machine rooms in Macau. Rapid expansion of the gaming industry in Macau continues; several additional casinos are expected to open in the next few years.

Under the old monopoly framework, organized crime groups were closely associated with the gaming industry through their control of VIP gaming rooms and activities such as racketeering, loan sharking, and prostitution. The VIP rooms catered to clients seeking anonymity within Macau's gambling establishments, and received minimal official scrutiny. As a result, the gaming industry provided an avenue for the laundering of illicit funds and served as a conduit for the unmonitored transfer of funds out of China. VIP rooms continue to operate and are the primary revenue generators for Macau's

casinos. Although the arrival of international gaming companies has improved management and governance in all aspects of casino operations, concerns about organized crime groups and poorly regulated junket operators associations with VIP rooms remain. The MSAR's money laundering legislation aims to make money laundering by casinos more difficult by improving oversight, and tightening reporting requirements. On June 7, 2004, Macau's Legislative Assembly passed legislation allowing casinos and junket operators to make loans, in chips, to customers, in an effort to prevent loan-sharking. The law requires both casinos and junket operators to register with the government.

The Macau criminal code (Decree Law 58/95/M of November 14, 1995, Articles 22, 26, 27, and 286) criminalizes terrorist financing. Macau does not have any provision or procedures for freezing terrorist related funds or assets to fully implement UNSCRs 1267 and 1373. However, although no special mechanism exists and a judicial order is required, the general framework of seizure and forfeiture of funds and assets under the Criminal Code and Criminal Procedure Code do provide the MSAR the authority to freeze terrorist assets. Macau financial authorities direct the institutions they supervise to conduct searches for terrorist assets, using the consolidated list provided by the UN 1267 Sanctions Committee and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. No terrorist assets were identified in 2007.

The Macau legislature passed a counter-terrorism law in April 2002 to facilitate Macau's compliance with UNSCR 1373. The legislation criminalizes violations of UN Security Council resolutions, including counterterrorism resolutions, and strengthens counter-terrorist financing provisions. When China ratified the UN International Convention for the Suppression of the Financing of Terrorism, China stipulated that the Convention would apply to the MSAR

Increased attention to financial crimes in Macau since the events of September 11, 2001, has led to a general increase in the number of suspicious transaction reports (STRs); however, the number of STRs remains relatively low. Macau's Judiciary Police received 109 STRs in 2004, 194 in 2005, 396 STRs from January to September 2006, and 557 STRs from January to September 2007. In 2004 Macau opened ten money laundering cases but prosecuted none. In 2005 Macau opened nine money laundering cases and prosecuted two. Since the entry into force of the new AML law in April 2006, the Macau Public Prosecutions office has received 23 suspected cases of money laundering from the FIU. Of these, 14 have been referred for investigation by the Judicial Police or the Commission Against Corruption. Since 2005, the Judicial Police have referred three money laundering cases to the Public Prosecutions office.

In May 2002, the Macau Monetary Authority revised its anti-money laundering regulations for banks to bring them into greater conformity with international practices. Guidance also was issued for banks, moneychangers, and remittance agents, addressing record keeping and suspicious transaction reporting for cash transactions over U.S. $2,500. For such transactions, banks, insurance companies, and moneychangers must perform customer due diligence. However for casinos, Macau requires customer due diligence only for transactions above U.S. $62,500. In 2003, the Macau Monetary Authority examined all moneychangers and remittance companies to determine their compliance with these regulations. The Monetary Authority of Macau, in coordination with the IMF, updated its bank inspection manuals to strengthen anti-money laundering provisions. The Monetary Authority inspects banks every two years, including their adherence to anti-money laundering regulations. There is no requirement to report large sums of cash carried into Macau. The Macau Customs Service has the authority to conduct physical searches and detain suspicious persons and executes random checks on cross-border movement of cash, including record keeping when the amount of cash carried over the border exceeds US$38,500. However, there is no central database for such reports. Mainland China does restrict the transport of RMB out of China. Persons may carry no more than RMB 20,000 (approximately U.S. $2,750) per day out of China. According to the Macau Prosecutors Office, this Chinese requirement limits the number of people carrying large amounts of cash into Macau.

The United States has no law enforcement cooperation agreements with Macau, though informal cooperation between the United States and Macau routinely takes place. The Judiciary Police have been cooperating with law enforcement authorities in other jurisdictions through the Macau branch of Interpol, to suppress cross-border money laundering. In addition to Interpol, the Fraud Investigation Section of the Judiciary Police has established direct communication and information sharing with authorities in Hong Kong and Mainland China. In July 2006, the MSAR enacted the Law on Judicial Cooperation in Criminal Matters, enabling the MSAR to enter into more formal judicial and law enforcement cooperation relationships with other countries. The law became effective in November 2006. Macau's FIU has not yet established MOUs on information sharing with other jurisdictions but is currently negotiating with FIUs from Hong Kong, China, Portugal, Japan, Korea, and Sri Lanka.

The Monetary Authority of Macau also cooperates internationally with other financial authorities. It has signed memoranda of understanding with the People's Bank of China, China's Central Bank, the China Insurance Regulatory Commission, the China Banking Regulatory Commission, the Hong Kong Monetary Authority, the Hong Kong Securities and Futures Commission, the Insurance Authority of Hong Kong, and Portuguese bodies including the Bank of Portugal, the Banco de Cabo Verde and the Instituto de Seguros de Portugal.

Macau participates in a number of regional and international organizations. It is a member of the Asia/Pacific Group on Money Laundering (APG), the Offshore Group of Banking Supervisors, the International Association of Insurance Supervisors, the Offshore Group of Insurance Supervisors, the Asian Association of Insurance Commissioners, the International Association of Insurance Fraud Agencies, and the South East Asia, New Zealand and Australia Forum of Banking Supervisors (SEAZA). In 2003, Macau hosted the annual meeting of the APG, which adopted the revised FATF Forty Recommendations and a strategic plan for anti-money laundering efforts in the region from 2003 to 2006. In ratifying the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption China in each case specified that the treaty would apply to the MSAR. Macau officials have taken a number of steps in the past three years to raise industry awareness of money laundering. The Macau Monetary Authority trains banks on anti-money laundering measures on a regular basis.

In December 2006, the Asia Pacific Group (APG) and Offshore Group of Banking Supervisors (OGBS) conducted a joint Mutual Evaluation of the anti-money laundering and combating the financing of terrorism measures in place in Macau The Mutual Evaluation Report stated that Macau was noncompliant with FATF Special Recommendation IX, in that Macau should have measures in place to detect the physical cross border transport of currency and bearer-negotiable instruments. Macau does not require reporting of the movement of currency above any threshold level across its borders, or reporting of large currency transactions above any threshold level. Macau's AML/CTF regime is also deficient in a number of other respects, including: the lack of a mechanism to confiscate, freeze, and forfeit proceeds of crime independent of criminal process; the lack of ability to freeze terrorist funds; failure to establish an independent FIU, which was established only as a special project entity with a term of three years; the lack of requirements for financial institutions to verify the identify of persons on whose behalf a customer is acting to understand the ownership and control structure of customers, or to examine the background and purpose of transactions with no economic or visible lawful purpose; the failure to develop a risk assessment of, and risk based approach to the gaming sector; and the lack of adequate legal framework for requiring Designated Non-Financial Business and Professions, including casinos and gaming concessionaires to report suspicious transactions.

Macau should continue to improve its ability to implement and enforce existing laws and regulations. Macau should ensure that regulations, structures, and training are adequate to prevent money laundering in the gaming industry, including implementing regulations to prevent money laundering in casinos, especially regulations to improve oversight of VIP rooms. The MSAR should take steps to

implement the new FATF Special Recommendation IX, adopted by the FATF in October 2004, requiring countries to put in place detection and declaration systems for cross-border bulk currency movement. Macau should establish asset freezing mechanisms and procedures to fully implement UN Security Council Resolutions 1267 and 1373. This process should not be linked to the criminal process and should include the ability to freeze terrorist assets without delay. Macau should increase public awareness of the money laundering problem, improve interagency coordination and training, and boost cooperation between the MSAR and the private sector in combating money laundering. Macau should institutionalize its Financial Intelligence Unit by making it a permanent, statutory body and ensure the FIU meets Egmont Group standards for information sharing. Macau's Judicial Police have limited resources devoted to AML/CTF investigations. Additional manpower would allow for more investigations and enforcement action.

Malaysia

Malaysia is not a regional center for money laundering. A range of significant money laundering and terrorist financing risks in Malaysia are being addressed through the implementation of the country's Anti-Money Laundering Act and other AML/CTF measures. Malaysia has long porous land and sea borders and its open economy and strategic geographic position influence money laundering and terrorist finance in the region. Drug trafficking is the main source of illegal proceeds in Malaysia. Malaysia is primarily used as a transit country to transfer drugs originating from the Golden Triangle and Europe, including heroin, amphetamine type substances and ketamine. Authorities also highlight illegal proceeds from corruption as well as a wide range of predicate offenses including fraud, illegal gambling, credit card fraud, counterfeiting, forgery, human trafficking, extortion, and smuggling. Money laundering techniques include placing criminal proceeds into the banking system, using nominees, the use of front companies, purchasing insurance products and high value goods and real property, investment in capital markets, and the use of moneychangers. Smuggling of goods subject to high tariffs is a major source of illicit funds. Malaysia has a significant informal remittance sector.

The GOM has a well-developed AML/CTF framework. Malaysia's National Coordination Committee to Counter Money Laundering (NCC), comprised of members from 13 government agencies, oversaw the drafting of Malaysia's Anti-Money Laundering Act of 2001 (AMLA). The NCC is responsible for the development of the national AML/CTF program, including the coordination of national-wide AML/CTF efforts.

In February 2007, the APG conducted its second Mutual Evaluation on Malaysia. The evaluation was based on all FATF recommendations; Malaysia received ratings of "compliant" or "largely compliant" on 33 of the 49 FATF Recommendations, 15 ratings of "partially compliant;" and one rating of "noncompliant" with Special Recommendation on Terrorist Financing IX on cash couriers.

Subsequent to the mutual evaluation, the NCC established a task force comprised of the Royal Malaysian Customs, Immigration Department, Ministry of Internal Security, and Bank Negara Malaysia to formulate action plans to achieve full compliance with Special Recommendation IX. Malaysia's relatively lax customs inspection at ports of entry and its extensive coastlines, particularly along the east coast of Sabah in Borneo, serve to increase its vulnerability to smuggling, including cash smuggling.

On March 6, 2007, Malaysia enacted amendments to five different pieces of legislation: the AMLA, now called the Anti-Money Laundering and Anti-Terrorism Financing Act (AMLATF), the Penal Code, the Subordinate Courts Act, the Courts of Judicature Act, and the Criminal Procedure Code. These amendments impose penalties for terrorist acts, allow for the forfeiture of terrorist-related assets, allow for the prosecution of individuals who have provided material support for terrorists, expand the use of wiretaps and other surveillance of terrorist suspects, and permit video testimony in terrorist cases.

In 2002, the AMLA provided for the establishment of a financial intelligence unit in Malaysia. The Unit Perisikan Kewangan (UPW), located in the Central Bank, Bank Negara Malaysia (BNM), is tasked with receiving and analyzing information, and sharing financial intelligence with the appropriate enforcement agencies for further investigations. The UPW cooperates with other relevant agencies to identify and investigate suspicious transactions. A comprehensive supervisory framework has been implemented to audit financial institutions' compliance with the AMLA and its subsidiary legislation and relevant guidelines. Currently, BNM maintains 383 examiners who are responsible for money laundering inspections for both onshore and offshore financial institutions.

Malaysia's financial institutions have strict "know your customer" rules under the AMLA. Every transaction, regardless of its size, is recorded. Reporting institutions must maintain records for at least six years and report any suspicious transactions to the UPW. If the reporting institution deems a transaction suspicious it must report that transaction to the UPW promptly regardless of the transaction size. In addition, cash threshold reporting (CTR) requirements above RM 50,000 (approximately U.S. $14,900) were imposed upon banking institutions effective as of September 2006. UPW officials indicate that they receive regular reports from the AMLA reporting institutions. Reporting individuals and their institutions are protected by statute with respect to their cooperation with law enforcement. While Malaysia's bank secrecy laws prevent general access to financial information, those secrecy provisions are overridden in the case of reporting of suspicious transactions or criminal investigations.

Malaysia has adopted banker negligence (due diligence) laws that make individual bankers responsible if their institutions launder money or finance terrorists. Both reporting institutions and individuals are required to adopt internal compliance programs to guard against any offense. Under the AMLA, any person or group that engages in, attempts to engage in, or abets the commission of money laundering or financing of terrorism is subject to criminal sanction. All reporting institutions are subject to review by the UPW. Under the AMLA, reporting institutions include financial institutions from the conventional, Islamic, and offshore sectors as well as nonfinancial businesses and professions such as lawyers, notaries public, accountants, company secretaries, and Malaysia's one licensed casino. In 2005, reporting obligations were imposed upon licensed gaming outlets, notaries public, offshore trading agents, and listing sponsors. Phased-in reporting requirements for stock brokers and futures brokers were expanded in 2005, and in 2006, reporting requirements were extended to money lenders, pawnbrokers, registered estate agents, trust companies, unit trust management companies, fund managers, futures fund managers, nonbank remittance service providers, and nonbank affiliated issuers of debit and credit cards. In 2007, the AMLA was further extended to insurance financial advisers, moneylenders in the state of Sabah, E-money issuers and leasing and factoring businesses.

In mid-2007, Islamic banking assets were RM 144 billion (approximately U.S. $43 billion), accounting for 12 percent of the total assets in the banking sector, up from 11.8 percent in mid-2006 and 11.6 percent in mid-2005. Malaysia's growing Islamic finance sector is subject to the same supervision to combat financial crime as the commercial banks.

In 1998, Malaysia imposed foreign exchange controls that restricted the flow of the local currency from Malaysia. Onshore banks must record cross-border transfers over RM 10,000 (approximately U.S. $3,000). An individual form is completed for each transfer above RM 200,000 (approximately U.S. $60,000). The thresholds for the bulk register for transactions were raised in October 2007. Recording is now done in a bulk register for transactions between U.S. $3,000 and $60,000. Banks are obligated to record the amount and purpose of these transactions.

While Malaysia's offshore banking center on the island of Labuan has different regulations for the establishment and operation of offshore businesses, it is subject to the same anti-money laundering laws as those governing onshore financial service providers. Malaysia's Labuan Offshore Financial Services Authority (LOFSA) serves as a member of the Offshore Group of Banking Supervisors. Offshore banks, insurance companies, trust companies, trading agents, and listing sponsors are

required to file suspicious transaction reports under the country's anti-money laundering law. LOFSA is under the authority of the Ministry of Finance and works closely with BNM. LOFSA licenses offshore banks, banking companies, trusts, and insurance companies and performs stringent background checks before granting an offshore license. The financial institutions operating in Labuan are generally among the largest international banks and insurers. Nominee (anonymous) directors are not permitted for offshore banks, trusts or insurance companies. Labuan had 6,152 registered offshore companies as of September 30, 2007. Bearer instruments are strictly prohibited in Labuan.

Offshore companies must be established through a trust company. Trust companies are required by law to establish true beneficial owners and submit suspicious transaction reports. There is no requirement to publish the true identity of the beneficial owner of international corporations; however, LOFSA requires all organizations operating in Labuan to disclose information on its beneficial owner or owners, as part of its procedures for applying for a license to operate as an offshore company. LOFSA maintains financial information on licensed entities, releasing it either with the consent of those entities or upon investigation.

In November 2005, LOFSA revoked the license of the "Blue Chip Pathfinder" Private Fund for "evidence that Swift Securities Investments Ltd had contravened the terms of the consent and acted in a manner that was detrimental to the interests of mutual fund investors." The Fund has since been terminated. Also in 2005, LOFSA revoked the investment banking license of Swift Securities Investments Ltd for "contravening the provisions of the license."

In April 2006, LOFSA announced that it had subscribed to a service which provides structured intelligence on high and heightened risk individuals and entities, including terrorists, money launderers, politically exposed persons, arms dealers, sanctioned entities, and others, to gather information on their networks and associates. LOFSA now uses this service as part of its licensing application process.

The Free Zone Act of 1990 is the enabling legislation for free trade zones in Malaysia. The zones are divided into Free Industrial Zones (FIZ), where manufacturing and assembly takes place, and Free Commercial Zones (FCZ), generally for warehousing commercial stock. The Minister of Finance may designate any suitable area as an FIZ or FCZ. Currently there are 13 FIZs and 12 FCZs in Malaysia. The Minister of Finance may appoint any federal, state, or local government agency or entity as an authority to administer, maintain, and operate any free trade zone. Companies wishing to operate in an FTZ or FCZ must apply for a license and be approved. The time needed to obtain such licenses from the administrative authority to operate in a particular free trade zone depends on the type of activity. Clearance time ranges from two to eight weeks. There is no indication that Malaysia's free industrial and free commercial zones are being used for trade-based money laundering schemes or by the financiers of terrorism. Rather, these zones are dominated by large international manufacturers such as Dell and Intel, which are attracted to the zones because they offer preferential tax and tariff treatment.

The UPW has been a member of the Egmont Group since July 2003. Prior to 2007, UPW had signed memoranda of understanding (MOUs) on the sharing of financial intelligence with the FIUs of Australia, Indonesia, Thailand, the Philippines and China. In 2007,and early 2008, an additional seven MOUs were signed with the United Kingdom, United States, Japan, Republic of Korea, Sweden, Chile and Sri Lanka. Malaysia is a member of the Asia/Pacific Group (APG) on Money Laundering, a FATF-style regional body.

In April 2002, the GOM passed the Mutual Assistance in Criminal Matters Act (MACMA), and in July 2006 concluded a Mutual Legal Assistance Treaty with the United States. Malaysia concluded a similar treaty among like-minded ASEAN member countries in November 2004. In October 2006, Malaysia ratified treaties with China and Australia regarding the provision of mutual assistance in criminal matters. An extradition treaty was also signed with Australia. The mutual assistance treaties enable States Parties to assist each other in investigations, prosecutions, and proceedings related to

criminal matters, including terrorism, drug trafficking, fraud, money laundering and human trafficking.

Malaysia made its first money laundering arrest in 2004. As of October 2007, the Attorney General's Chambers had prosecuted 29 money laundering cases, involving a total of 829 charges with a cumulative total of RM 273.6 million (approximately U.S. $83.7 million). Out of the 29 cases, there were three convictions.

Malaysia is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Malaysia has signed but has not yet ratified the UN Convention against Corruption. On May 29, 2007, the Government of Malaysia (GOM) became a party to the UN International Convention for the Suppression of the Financing of Terrorism.

The GOM has cooperated closely with U.S. law enforcement in investigating terrorist-related cases since the signing of a joint declaration to combat international terrorism with the United States in May 2002. The GOM recently improved legislation enabling it to comprehensively freeze assets under the UNSCRs 1267 and 1373. The Ministry of International Security has the authority to identify and freeze the assets of terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and, whenever a new designee is added, the UPW issues immediate orders to all licensed financial institutions, both onshore and offshore, to do so. At the same time, the UPW also disseminates information on persons and entities designated unilaterally by other countries, including the United States, to these institutions. Since 2003 Bank Negara Malaysia has issued 43 circulars and nine accounts have been frozen amounting to approximately U.S. $76,400.

Malaysian authorities have highlighted risks from terrorist groups and terrorist financing. A number of terrorist organizations have been active on Malaysian territory, and authorities have taken action against Jemaah Islamiah. Terrorist financing in Malaysia is predominantly carried out using cash and relies on trusted networks. While Malaysia has recently improved the legislative framework to criminalize terrorist financing, there have been no investigations, prosecutions or convictions relating to terrorist financing under this new scheme. The Ministry of Foreign Affairs opened the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) in August 2003. SEARCCT coordinates courses and seminars on combating terrorism and terrorist finance.

The GOM has rules regulating charities and other nonprofit entities. The Registrar of Societies is the principal government official who supervises and controls charitable organizations, with input from the Inland Revenue Board (IRB) and occasionally the Companies Commission of Malaysia (CCM). The Registrar mandates that every registered society of a charitable nature submit its annual returns, including its financial statements. Should activities deemed suspicious be found, the Registrar may revoke the nonprofit organization's (NPO) registration or file a suspicious transaction report. Registering as a NPO can be bureaucratic and time-consuming. One organization reported that getting registered took nine months and required multiple personal interviews to answer questions about its mission and its methods. Some NPOs reportedly register as "companies" instead, a quick and inexpensive process requiring capital of approximately 60 cents and annual financial statements.

In March 2006, the UPW completed a review of the nonprofit sector with the Registrar, the IRB, and the CCM, in an effort to ensure that the laws and regulations were adequate to mitigate the risks of nonprofit organizations as conduits for terrorist financing. BNM reports that the review did not show any significant regulatory weaknesses; however, the GOM is considering measures to enhance the monitoring of fundraising, including increased disclosure requirements of how funds are spent.

Malaysia's tax law allows a tax credit, which encourages the reporting of contributions, for Zakat (alms) to mosques or registered Islamic charitable organizations. Islamic Zakat contributions can be taken as payroll deductions, which help prevent the abuse of charitable giving. There is no similar tax credit for nonMuslims.

The Government of Malaysia should continue to enhance its cooperation on a regional, multilateral, and international basis. The GOM should improve enforcement of regulations regarding its free trade zones, which remain vulnerable to the financing of terrorism and money laundering. Given that cash smuggling is a major method used by terrorist financers to move money in support of their activities, as a priority matter, Malaysian authorities should establish and adhere to a cross border currency declaration system that meets purpose and intent of the FATF Special Recommendation IX on bulk cash smuggling. There is a significant informal remittance sector in Malaysia that is not subject to AML/CTF controls and which may be vulnerable to misuse for money laundering and terrorist financing. Law enforcement and customs authorities should examine trade based money laundering and invoice manipulation and their relationship to underground finance and informal remittance systems. Malaysia should ratify the UN Convention against Corruption.

Mexico

Mexico is a major drug-producing and drug-transit country. It also serves as one of the major conduits for proceeds from illegal drug sales leaving the United States. The illicit drug trade is the principal source of funds laundered through the Mexican financial system. Other major sources of illegal proceeds being laundered include corruption, kidnapping, trafficking in firearms and immigrants, and other crimes. The smuggling of bulk shipments of U.S. currency into Mexico and the movement of the cash back into the United States via couriers, armored vehicles, and wire transfers remain favored methods for laundering drug proceeds.

According to U.S. law enforcement officials, Mexico remains one of the most challenging money laundering jurisdictions for the United States, especially with regard to the investigation of money laundering activities involving the cross-border smuggling of bulk currency derived from drug transactions and other transnational criminal activity. Sophisticated and well-organized drug trafficking organizations based in Mexico are able to take advantage of the extensive U.S.-Mexico border and the large flow of licit remittances. In addition, the combination of a sophisticated financial sector and relatively weak regulatory controls facilitates the concealment and movement of drug proceeds. U.S. officials estimate that since 2003, as much as U.S. $22 billion may have been repatriated to Mexico from the United States by drug trafficking organizations. In April 2006, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued a warning to the U.S. financial sector on the potential use of certain Mexican financial institutions, including Mexican casas de cambio (licensed foreign exchange offices) and centros cambiarios (unlicensed foreign exchange offices), to facilitate bulk cash smuggling. Corruption is also a concern: in recent years, various Mexican officials have come under investigation for alleged money laundering activities.

Currently, there are 39 commercial banks and 71 foreign financial representative offices operating in Mexico, as well as 94 insurance companies, 160 credit unions, and 25 casas de cambio. Commercial banks, foreign exchange companies, and general commercial establishments are allowed to offer money exchange services. Although the underground economy is estimated to account for 20-40 percent of Mexico's gross domestic product, the informal economy is considered to be much less significant with regard to money laundering than the criminal-driven segments of the economy. Beginning in 2005, permits were issued for casinos to operate in Mexico. National lotteries, horse races, and sport pools are also legal. Casinos, as well as offshore banks, lawyers, accountants, couriers, and brokers, are currently not subject to anti-money laundering reporting requirements.

From 2000 to 2006, remittances from the United State to Mexico grew from U.S. $6.6 billion to nearly U.S. $24 billion a year; in 2007, the increase is estimated at less than two percent. Many U.S. banks have partnered with their Mexican counterparts to develop systems to simplify and expedite the transfer of money, including wider acceptance by U.S. banks of the "matricula consular," an identification card issued by Mexican consular offices to Mexican citizens residing in the United

States that has been criticized as insecure. In some cases, the sender or the recipient can simply provide the matricula consular as identification to execute a remittance, often without having to open a bank account. While this makes licit remittances more accessible, it also leaves the system open to potential money laundering and exploitation by organized crime groups. The U.S. Embassy estimates that in 2007, electronic transfers accounted for 90 percent of all remittances to Mexico. It is likely that few first-tier commercial banks will reach down to serve low-income clients who receive such remittances, with cajas populares and cajas solidarias (financial cooperatives that function as credit unions) being the likely candidates to fill this gap. This presents a new set of concerns over whether this system will present potential money laundering opportunities for bulk currency transactions.

The Tax Code and Article 400 bis of the Federal Penal Code criminalize money laundering related to any serious crime. Money laundering is punishable by imprisonment of five to fifteen years and a fine. Penalties are increased when a government official in charge of the prevention, investigation, or prosecution of money laundering commits the offense. Mexico's all-crimes approach to money laundering criminalizes the laundering of the proceeds of any intentional act or omission, regardless of whether or not that act or omission carries a prison term. Rather than applying to proceeds of criminal offenses, the statute applies to "the proceeds of an illicit activity", which is defined as resources, rights, or goods of any nature for which there exists well-founded certainty that they are derived directly or indirectly from or represent the earnings derived from the commission of any crime, and for which no legitimate origin can be established. This construction of the predicate offense allows prosecutors, upon demonstrating criminality, to shift the burden of proof to the defendant to establish the legitimate origin of the property. An offense committed outside of Mexico may also constitute a predicate for money laundering offense. Because criminal proceeds generated abroad would have an effect in Mexico when laundered in or through its national territory, the laundering of those proceeds could be prosecuted under Mexican law.

The Banking and Securities Commission (CNBV) regulates and supervises banks, limited scope financial companies, securities brokerage firms, foreign exchange firms, and mutual funds. The Tax Authority (SAT) supervises nonlicensed foreign exchange retail centers and money remitters. The CNBV has the remit to impose administrative sanctions for noncompliance, revoke licenses, and conduct on-site inspections and off-site monitoring of regulated entities. The CNBV is also responsible for issuing regulations. Regulations require banks and other financial institutions (including mutual savings companies, insurance companies, securities brokers, retirement and investment funds, financial leasing and factoring funds, casas de cambio, centros cambiarios, and money remittance businesses) to know and identify customers and maintain records of transactions.

In 2004, the Ministry of the Treasury (SHCP) reorganized and renamed its financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF). The UIF's personnel number approximately 50 and are comprised mostly of forensic accountants, lawyers, and analysts. Regulated entities must report to the UIF any suspicious transactions, currency transactions over U.S. $10,000 (except for centros cambiarios, which are subject to a U.S. $3,000 threshold), and transactions involving employees of financial institutions who engage in suspicious activity. Banks also require occasional customers performing transactions equivalent to or exceeding U.S. $3,000 in value to be identified, so that the transactions can be aggregated daily to prevent circumvention of the requirements to file cash transaction reports (CTRs) and suspicious transaction reports (STRs). A 2005 provision of the tax law requires real estate brokerages, attorney, notaries, accountants, and dealers in precious metals and stones to report all transactions exceeding U.S. $10,000 to the SAT, which shares that information with the UIF. In 2006, nonprofit organizations were made subject to reporting requirements for donations greater than U.S. $10,000. Financial institutions have also implemented programs for screening new employees and verifying the character and qualifications of their board members and high-ranking officers.

In 2000, Mexico amended its Customs Law to reduce the threshold for reporting inbound cross-border transportation of currency or monetary instruments from $20,000 to $10,000. At the same time, it established a requirement for the reporting of outbound cross-border transportation of currency or monetary instruments of U.S. $10,000 or more. These reports are received by the UIF and cover a wider range of monetary instruments (e.g. bank drafts) than those required by the United States. As a result of the cooperation between Mexican Customs, the Financial Crimes Unit of the Office of the Deputy Attorney General against Organized Crimes (SIEDO), and various U.S. agencies, Mexico has seized over U.S. $60 million in bulk currency shipments leaving Mexico City's international airport since 2002.

The UIF is responsible for receiving, analyzing, and disseminating STRs and CTRs, as well as reports on the cross-border movements of currency. The UIF also reviews all crimes linked to Mexico's financial system and examines the financial activities of public officials. In 2007, the UIF received approximately 38,400 STRs and 5,607,000 CTRs. Following the analysis of CTRs, STRs, and reports on the cross-border movements of currency, the UIF sends reports that are deemed to merit further investigation, and have been approved by the SHCP's legal counsel, to the Office of the Attorney General (PGR). From 2004 to December 2007, the UIF sent 89 cases to the PGR for its consideration for prosecution. The PGR's special financial crimes unit (within SIEDO) works closely with the UIF in money laundering investigations. UIF personnel also have working-level relationships with other federal law enforcement entities, including the Federal Investigative Agency (AFI) and the Federal Police (PFP), to help it support the PGR's investigations of criminal activities with ties to money laundering. In 2006, the UIF signed Memoranda of Understanding (MOUs) with the Economy Secretariat and the Mexican immigration authorities that provide access to their databases. The UIF has also signed agreements with the CNBV and the National Commission of Insurance and Finance (CNSF) to coordinate to prevent money laundering and terrorist financing. The UIF is currently finalizing similar negotiations with the SHCP and the National Savings Commission (CONSAR).

In 2007, U.S. authorities observed a significant increase in the number of complex money laundering investigations by SIEDO, with support from the UIF and coordinated with U.S. officials. As of November 2007, SIEDO had initiated 142 criminal investigations into money laundering cases, 77 of which were brought to trial. One high profile case was the September 2007 arrest of

Sandra Avila Beltran (also known as the "Queen of the Pacific"), who was indicted in the United States in 2004 on separate drug smuggling charges. Avila Beltran is the niece of drug-kingpin Miguel Angel Felix Gallardo, who is serving a long sentence for drug smuggling and for the 1985 murder of DEA agent Enrique Camarena. She is also the niece of Juan José Quintero Payan, who was extradited to the United States on drug smuggling charges. Avila Beltran shielded her narcotics-related financial activities behind legitimate and successful businesses in Mexico, including a string of tanning and beauty salons and a real estate company with multiple locations. The Government of Mexico (GOM) demonstrated that she had forged cocaine trafficking and financial deals between Mexican and Colombian traffickers over the last decade. The Avila Beltran case highlighted the difficulty of prosecuting those involved in the financial aspects of the drug trade.

Another complex case was the GOM-initiated raids in December against Victor Emilio Cazares Salazar (also known as Victor Emilio Cazares Gastellum), at the same time as the U.S. Treasury's Office of Foreign Assets Control (OFAC) designated his sister, Mexican money launderer Blanca Margarita Cazares Salazar, as a specially designated narcotics traffickers subject to sanctions pursuant to the Foreign Narcotics Kingpin Designation Act. The sequencing represents Mexico's aggressive pursuit of an important money laundering function in conjunction with U.S. Government (USG) efforts, including the February 2007 U.S. indictment of Victor Cazares Salazar. Blanca Cazares Salazar and her widespread money laundering organization acted as fronts for her brother and Mexican drug kingpin Ismael Zambada Garcia (also known as "Mayo Zambada"), leaders of Mexico's Sinaloa Cartel. Victor Emilio Cazares Salazar's narcotics funds spawned a complex, interlocking

network of businesses located throughout Mexico, including three Tijuana-based money service businesses and a chain of approximately 20 jewelry and cosmetics boutiques located in eight Mexican states, as well as importation firms, restaurants, mobile phone services, and money service businesses in Sinaloa, Jalisco, Baja California, and Mexico City.

Although the United States and Mexico both have asset forfeiture laws and provisions for seizing assets abroad derived from criminal activity, U.S. requests of Mexico for the seizure, forfeiture, and repatriation of criminal assets have rarely met with success. Currently, Mexico does not have a civil forfeiture regime and can only forfeit assets upon a final criminal conviction; it can also seize assets administratively if they are deemed to be "abandoned" or unclaimed. Draft legislation pending in the Mexican Congress includes constitutional changes that would enable a forfeiture regime similar to Colombia's law of extinguishment of ownership ("extinción de dominio"). If passed, any asset seizure regime will require considerable implementation efforts.

In 2001, pursuant to a USG request, the GOM seized assets valued at millions of dollars in Mexico from Alyn Richard Wage, who was charged in the United States in a major fraud case (the "Tri-West" case). These assets were found by a U.S. court to be proceeds of the fraud and were the subject of a final order of forfeiture in the United States. For several years, the USG has sought the assistance of the Mexican courts to enforce the U.S. forfeiture order and repatriate the assets to the United States to compensate the victims of the fraud. In October 2007, the PGR filed a petition, with supporting documents from the USG, asking the court to recognize and enforce the U.S. forfeiture order, employing the argument of "abandoned funds." The case remains without resolution.

Another significant case involves Zhenli Ye Gon. Approximately $207 million was seized in March 2007 from his Mexico City residence. The funds seized reportedly included dollars, Mexican pesos, euros, Hong Kong dollars, and Mexican gold bullion coins. GOM authorities also seized two dwellings and seven vehicles. The Drug Enforcement Administration (DEA) has described the seizure as the largest ever of drug money anywhere in the world. These funds have been forfeited under the same argument of "abandoned funds". Zhenli was arrested in the United States in July 2007 and is accused of trafficking tons of pseudoephedrine and other chemicals to supply Mexican methamphetamine labs.

In 2007, after nearly three years of consideration, Mexico criminalized terrorist financing, with punishments of up to 40 years in prison. The new law amends the Federal Penal Code to link terrorist financing to money laundering and establish international terrorism as a predicate crime when it is committed in Mexico to inflict damage on a foreign state. The GOM has responded positively to international and USG efforts to identify and block terrorist-related funds, and it continues to monitor suspicious financial transactions, although no such assets have been frozen to date.

Mexico has developed a broad network of bilateral agreements and regularly meets in bilateral law enforcement working groups with its counterparts within the U.S. law enforcement community. The U.S.-Mexico Mutual Legal Assistance Treaty (MLAT) entered into force in 1991. Mexico and the United States also implement other bilateral treaties and agreements for cooperation in law enforcement issues, including the Financial Information Exchange Agreement (FIEA) and the Memorandum of Understanding (MOU) for the exchange of information on the cross-border movement of currency and monetary instruments.

Mexico is a member of the Financial Action Task Force (FATF) and the Financial Action Task Force for South America (GAFISUD). The GOM currently holds the GAFISUD presidency. In addition to its membership in the FATF and GAFISUD, Mexico participates in the Caribbean Financial Action Task Force (CFATF) as a cooperating and supporting nation. Mexico will undergo a FATF mutual evaluation in January 2008. The UIF is a member of the Egmont Group, and Mexico participates in the Organization of American States' Inter-American Drug Abuse Control Commission's (OAS/CICAD) Experts Group to Control Money Laundering. The GOM is a party to the 1988 UN

Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the UN International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention against Terrorism.

The GOM has made fighting money laundering and drug trafficking one of its top priorities, and has made progress in combating these crimes over the course of 2007. However, Mexico continues to face challenges with respect to is anti-money laundering and counter-terrorist financing regime, particularly with its ability to prosecute and convict money launderers. To create a more effective regime, Mexico should fully implement and improve its mechanisms for asset forfeiture; increase personnel responsible for the initiation, investigation, and prosecution of money laundering cases; control the bulk smuggling of currency across its borders; monitor remittance systems for possible exploitation; and improve the regulation of centros cambiarios. The GOM should also ensure that its newly-adopted counter-terrorist financing law is fully implemented.

Moldova

Moldova is not considered an important regional financial center. The Government of Moldova (GOM) monitors money flows through right-bank Moldova (the territory it controls), but does not exercise control over the breakaway region of Transnistria. Transnistrian authorities do not submit to GOM financial controls and maintain an independent banking system not licensed by the National Bank of Moldova. Moldovan incomes are generally low. Criminal proceeds laundered in Moldova derive substantially from tax evasion, contraband smuggling, foreign criminal activity, and, to a lesser extent, domestic criminal activity and corruption. Money laundering proceeds are controlled by small, poorly-organized domestic criminal groups. These small groups are in turn supervised by larger and better-organized foreign crime syndicates from Russia, Ukraine, and Israel, among others.

Money laundering has occurred in the banking system and through exchange houses in Moldova, and in the offshore financial centers in Transnistria and throughout the region. The amount of money laundering occurring via alternative remittance systems is reportedly not significant. The number of financial crimes unrelated to money laundering, such as bank fraud, embezzlement, corruption, and forgery of bankcards, especially through international offshore zones, has decreased. During 2006, several cases involved bank fraud and the misuse of bankcards. Although the number of financial crimes has not increased, investigations have revealed a diversification of financial and economic-related crimes.

Although a significant black market exists in Moldova, especially smuggling of goods at the Moldovan-Ukrainian border alongside Transnistria, narcotics proceeds are not a significant funding source of this market. Contraband smuggling generates funds that are laundered through the banking system. Often funds are first laundered through Transnistrian banks, next transferred to Moldovan institutions, and then transferred to other countries.

Moldova is not considered an offshore financial center. The Moldovan financial system has 15 banks, including three foreign-owned banks that are regulated in the same manner as Moldovan commercial banks. Offshore banks are not permitted to operate in Moldova. Shell companies are not allowed by law, although they exist on a de facto basis. Nominee directors and trustees are not allowed. Internet gaming sites do exist, although no statistics are currently available on the number of sites in operation. Internet gaming is subject to the same regulations as domestic casinos. The Ministry of Finance currently licenses five casinos, although they are reportedly not well regulated or controlled.

Moldova currently has six free trade zones (FTZs). Certain free-trade zones are infrequently used. Goods from abroad are imported to the free economic zones and resold without payment of customs duties of the country of origin or of Moldova. The goods are then exported to other countries with documentation, indicating Moldovan origin. According to the Moldova's financial intelligence unit

(FIU), the Service for Preventing and Combating Money Laundering and Terrorism Financing, no reports have been filed alleging that the free zones have been used in trade-based money laundering schemes or for terrorist financing. Supervision of the FTZs is conducted by a GOM agency, the Free Trade Zone Administration (FTZA). Companies operating in free-trade zones are also subject to inspections, controls, and investigations by inspectors from the Customs Service and the Center for Combating Economic Crime and Corruption (CCECC).

Money laundering is a separate criminal offense in the Moldovan Criminal Code, Art. 243, and under the Law on Preventing and Combating Money Laundering and Terrorism, No.190-XVI, passed on July 26, 2007. The legislation takes an "all serious crimes" approach. Serious crimes are defined as those punishable by a fine of 500 to 1,000 conventional units (U.S. $900 to $1,800) or by imprisonment of up to five years. The fine or imprisonment may be accompanied by a prohibition to hold certain positions or to practice a certain activity for a period of two to five years.

On April 10, 2007, President Vladimir Voronin proposed to the Moldovan Parliament draft amendments to the tax code and other financial regulations aimed at "liberalizing the economy." On April 27, the Parliament adopted these tax-code amendments intended to regulate Moldova's informal economy, forgive tax debts and stimulate investments. Some provisions of the financial package raised concerns as they could facilitate money laundering and terrorist financing. Of particular concern was a capital-amnesty provision allowing individuals and legal entities (corporations, partnerships, etc.) to legalize previously undeclared cash and noncash assets, including real estate and stocks. According to the proposed legislation, the GOM would encourage asset declaration by ensuring the confidentiality of all transactions and protecting filers from any future fiscal investigations. Additionally, those taking advantage of the amnesty would be under no obligation to declare the origins of their declared assets. The law also stipulated that transaction information could not be shared with the CCECC or the Moldovan Tax Inspectorate. Most worrisome, the legislation exempted declared assets from Moldova's fiscal, customs and current money laundering and terrorist financing legislation.

Following recommendations from the international community, on July 20, 2007, the Moldovan Parliament adopted Law 2298, a package of tax-code reforms, which included amendments to the capital-amnesty law. The amendment closed loopholes in the capital-amnesty law, eliminating explicitly the exemption of amnesty-related transactions from Moldova's anti-money laundering law. A week later, Parliament separately adopted the new anti-money laundering bill, the Law on Preventing and Combating Money Laundering and Terrorism. Since their passage, GOM authorities have issued numerous regulations, decisions, and laws that are related to the tax-amnesty/capital-legalization law and the new money laundering law. On August 15, 2007, the National Bank of Moldova issued two decisions focusing on the activity of financial institutions related to capital legalization and the transfer or export from the Republic of Moldova of legalized funds by individuals.

Article 12 of the Law on Preventing and Combating Money Laundering and Terrorism regulates the limitations of bank secrecy. Thus, information obtained from reporting entities can be used only with the purpose of preventing money laundering and terrorist financing. The forwarding of information regarding clients or ownership information to the CCECC, criminal investigative authorities, prosecutorial entities, or to the courts in an effort to prevent or combat money laundering activities is not classified as disclosure of commercial bank or professional secrets, as long as the forwarding of information is carried out in accordance with legal provisions.

All banks and nonbanking financial institutions are supervised and examined for compliance with anti-money laundering/counter-terrorist financing (AML/CTF) laws and regulations by the CCECC, which has the authority to investigate money laundering and terrorist financing. Under the Law on Preventing and Combating Money Laundering and Terrorism, the National Bank of Moldova (NBM) supervises banks, exchange houses, and representatives of foreign banks. Moreover, based on the July 2007 amendment of Law No. 192 from December 11, 1998, on the Securities Commission, three

institutions dealing with oversight of financial markets—the National Commission on Securities, the Inspectorate for Supervision of Insurance Companies and Retirement Funds, and the National Service for Supervision of Citizen's Savings and Lending Associations—were merged into one agency, the National Commission on Financial Markets (NCFM). The NCFM's jurisdiction includes nonbanking financial entities, such as institutions issuing securities, investors, the National Bureau of Insurance of Vehicles of Moldova, members of saving and lending associations, and clients of micro-financing organizations. Additionally, the NCFM oversees professional participants in the nonbanking financial sector that have license to carry out activities in the following fields: securities market, insurance market, micro-financing, private pension funds, mortgage organizations, and credit-history bureaus. The Licensing Chamber checks the compliance of companies applying for business licenses, and specifically oversees casinos and gambling facilities.

Banks, exchange houses, stock brokerages, casinos, insurance companies, lawyers, notaries, accountants, and lotteries and institutions organizing or displaying lotteries are required to know, record, and report the identity of customers engaging in significant transactions. The reporting entities are obligated to report suspicious transactions to the FIU within 24 hours. In addition, single transactions or multiple transactions undertaken in 30 calendar days that exceed MDL 500,000 (approximately U.S. $45,000) must be reported to the FIU. The Law on Preventing and Combating Money Laundering and Terrorism also requires that financial institutions maintain records and documentation of accounts account holders and basic documentation (including business correspondence) for a period of at least seven years after the termination of business relations or the closing of the account.

Moldova's FIU is a quasi-independent unit within the CCECC. Decree No. 111 of September 15, 2003, establishes the FIU as an administrative and analytical body that collects, maintains, and analyzes reports from reporting institutions. It also conducts criminal investigations and has regulatory authority to develop draft laws. The FIU is staffed with 14 inspectors. Although housed within the CCECC building, a separate locked door separates its offices from other CCECC employees. The heads of the FIU and the CCECC maintain that other CCECC employees have no access to records collected by the FIU. However, the leadership of the FIU is ultimately under the supervision of the director of the CCECC. While the CCECC budget covers the financial needs of the FIU, the FIU is also supported technically and financially by international organizations. The head of the FIU reports that the unit is adequately staffed, with low turnover, good working conditions and newly renovated offices. However, it analytical functions are limited without a database, which it currently cannot afford.

The CCECC and the FIU are the lead agencies responsible for investigating financial crimes, including money laundering. Other agencies that share jurisdiction over the investigation of financial crimes include the Prosecutor General's Office, the Ministry of Interior and the Customs Service. The Security and Intelligence Service (SIS) investigates terrorist financing. The FIU has formed a task force with the Prosecutor General's Office, the Ministry of the Interior (MOI), the Customs Service, the NBM, the National Securities Commission, the SIS, and the Ministry of Information Development to share information and discuss investigations. The FIU has signed interagency agreements with other law enforcement agencies and ministries with databases to exchange law-enforcement information.

In 2007, the FIU received reports on approximately 9 million financial transactions, of which 165,199 were considered suspicious. This number of suspicious transactions is misleading, however, since GOM officials categorize all transactions involving Transnistria as suspicious.

In 2007, the FIU initiated eleven criminal cases related to financial fraud; four cases carried money laundering charges. The FIU identified two major types of criminal activity in 2006 and during the first six months of 2007. In the first instance, criminals used financial transactions that appeared to be legitimate to launder or clean criminal proceeds. In the second instance, criminals used the FTZs to

create illegal profits by reducing the value of imported goods. In 2007, the FIU imposed fines and sanctions totaling MDL 550,000 (approximately U.S. $49,600). The FIU reports that no arrests of individuals were conducted in 2006 or during the first six months of 2007 for money laundering violations. Late in 2007, a Moldovan court tried a criminal case charging the defendant with money laundering violations. The defendant was found guilty and sentenced to 15 years imprisonment. The FIU and CCECC have made no arrests nor pursued prosecutions involving terrorist financing.

Law No. 1569 of December 2002 on the transportation of currency stipulates that persons are obliged to report in writing to Moldovan customs officials the amount of currency that they are transporting when that amount exceeds 10,000 euros. If the amount of outbound currency is more than 10,000 euros, the carrier of the currency will have to report the outbound currency in a special declaration form provided by customs officials at the border. In addition to the special declaration, the currency carrier must provide documents detailing the source of the money. The carrier also must present a special permission for outbound cash currency transportation issued by a duly authorized bank or by the NBM. The Customs Service operates a special database that includes all declarations. The Customs Service shares the information in the database with other governmental agencies, including the FIU.

The Moldovan Criminal Code provides for the seizure and confiscation of assets related to all serious crimes, including terrorist financing. The provisions may be applied to goods belonging to persons who knowingly accepted things acquired illegally, even when the state declines to prosecute. However, it remains unclear whether asset forfeiture may be invoked against those unwittingly involved in or tied to an illegal activity. If it can be shown that the assets were used in the commission of a crime or result from a crime, they can be confiscated. Legitimate businesses can be seized if they were used to launder drug money, support terrorist activity, or are otherwise related to other criminal proceeds. The Criminal Code allows for civil as well as criminal forfeiture.

The Prosecutor General's Office has expressed its willingness to pursue an initiative to amend the Constitution to allow a more effective use of asset forfeiture. The Constitution currently incorporates a presumption that any property owned by an individual was legally acquired. This presumption has acted to inhibit the use of the existing asset forfeiture laws. Subsequent to a constitutional amendment, the Prosecutor General's Office plans generally to update the laws governing the identification of criminal assets and the use of asset forfeiture.

The FIU, CCECC, Tax Inspectorate, Customs Service and prosecutor's offices to the extent of their jurisdiction are responsible for tracing, seizing and freezing assets. Assets seized by law enforcement are incorporated into the state budget, not a separate fund. In 2007, issued decisions freezing and seizing assets totaling MDL 14.8 million (approximately U.S. $1.3 million).

The banking community generally cooperates with enforcement efforts of the FIU and the CCECC to trace funds and seize or freeze bank accounts. However, the GOM currently lacks adequate resources, training, and experience to trace and seize assets effectively. The GOM does not have a national system for freezing terrorist assets. The GOM has no separate law providing for the sharing with other countries of assets seized from narcotics and other serious crimes. However, nothing in the current legal structure would prohibit such activity.

Article 279 of the Moldovan Criminal Code criminalizes terrorist financing. It is defined as a "serious crime." Moldova regulates efforts to combat terrorist financing in the Law on Combating Terrorism, enacted on November 12, 2001. Article 2 defines terrorist financing, and Article 8/1 authorizes suspension of terrorist and related financial operations. This statute is separate from the aforementioned money laundering law, which contains other relevant provisions.

In 2007, the CCECC issued a decree on actions to be taken to enforce the provisions of the Law on Preventing and Combating Money Laundering and Terrorism. The CCECC decree listed groups

worthy of particular focus given possible money laundering or terrorist financing concerns. These groups included countries that may produce narcotics; countries that do not have legal provisions against money laundering and terrorist financing; countries with a high crime rate and corruption; countries operating offshore centers; and persons, groups, and entities identified as participating in terrorist activities. The decree was developed on the basis of Moldova's national interests and U.S. and UN lists of designated terrorists. Currently, the Moldovan authorities have not frozen, seized, or forfeited assets related to terrorism and terrorist financing. Reportedly, no indigenous alternative remittance systems exist in Moldova, although the use of cash couriers is common. No special measures have been taken to investigate misuse of charitable or nonprofit entities.

In December 2006, the GOM signed a $24.7 million Threshold Country Program with the Millennium Challenge Corporation that focuses on anti-corruption measures. The GOM requested funding to address areas of persistent corruption including the judiciary, health care system, tax, customs and law enforcement. Moldova is listed as 111 out of 180 countries in Transparency International's 2007 Corruption Perception Index.

The GOM has no bilateral agreement with the United States for the exchange of information regarding money laundering, terrorism, or terrorist financing investigations and proceedings. However, Moldovan authorities continue to solicit USG assistance on individual cases and cooperate with U.S. law enforcement personnel when presented with requests for information or assistance. The FIU has entered into bilateral agreements to exchange information with financial intelligence units of Albania, Belarus, Bulgaria, Croatia, Estonia, Georgia, Indonesia, Korea, Lebanon, Lithuania, Macedonia, Romania, Russia, and Ukraine.

Moldova is a party to the 1988 UN Drug Convention, the International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. On October 1, 2007, the GOM ratified the UN Convention against Corruption. Moldova has signed an agreement with CIS member states for the exchange of information on criminal matters, including money laundering. In 2004, the CCECC was accepted as an observer at the Eurasian Group on Combating Money Laundering. Moldova is a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The FIU is currently pursuing membership in the Egmont Group of financial intelligence units.

The Government of Moldova should continue to enhance its existing anti-money laundering and counter-terrorist financing regime. The GOM should ensure that the FIU and law enforcement agencies have sufficient resources, training, and tools to adequately analyze and investigate suspected cases of money laundering and terrorist financing. Moldova should improve the mechanisms for sharing information and forfeiting assets. Border enforcement and antismuggling enforcement should be priorities. The GOM should continue the momentum of its anticorruption efforts.

Monaco

The second-smallest country in Europe, the Principality of Monaco is known for its tradition of bank secrecy, network of casinos, and favorable tax regime. Money laundering offenses relate mainly to offenses committed abroad. Russian organized crime and the Italian Mafia reportedly have laundered money in Monaco. The Principality is also reported not to face the ordinary forms of organized crime. Existing crime does not seem to generate significant illegal proceeds, with the exception of fraud and offenses under the "Law on Checks." Monaco remains on an Organization for Economic Cooperation and Development (OECD) list of so-called "noncooperative" countries in terms of provision of tax information.

Monaco has a population of approximately 32,000, of which fewer than 7,000 are Monegasque nationals. Monaco's approximately 60 banks and financial institutions hold more than 300,000

accounts and manage total assets of about 70 billion euros (approximately U.S. $102.8 billion). Approximately 85 percent of the banking customers are nonresident. In 2005, the financial sector represented 15 percent of Monaco's economic activity. The high prices for land throughout the Principality result in a real estate sector of considerable import. There are five casinos run by the Société des Bains de Mer, in which the state holds a majority interest.

Monaco's banking sector is linked to the French banking sector through the Franco-Monegasque Exchange Control Convention, signed in 1945 and supplemented periodically, most recently in 2001. Through this convention, Monaco operates under the banking legislation and regulations issued by the French Banking and Financial Regulations Committee, including Article 57 of France's 1984 law regarding banking secrecy. The majority of entities in Monaco's banking sector concentrate on portfolio management and private banking. Subsidiaries of foreign banks operating in Monaco may withhold customer information from their parent banks.

Banking laws do not allow anonymous accounts, but Monaco does permit the existence of alias accounts, which allow account owners to use pseudonyms in lieu of their real names. Cashiers do not know the clients, but the banks know the identities of the customers and retain client identification information. Article 8 of Sovereign Order 632 of August 2006 clarifies the circumstances under which pseudonyms can be used by banks.

Prior approval is required to engage in any economic activity in Monaco, regardless of its nature. The Monegasque authorities issue approvals based on the type of business to be engaged in, the location, and the length of time authorized. This approval is personal and may not be re-assigned. Any change in the terms requires the issuance of a new approval.

Although the French Banking Commission supervises Monegasque credit institutions, Monaco shoulders the responsibility for legislating and enforcing measures to counter money laundering and terrorist financing. The Finance Counselor, located within the Government Council, is responsible for anti-money laundering and counter-terrorist financing (AML/CTF) implementation and policy.

Money laundering in Monaco is a crime under Act 1.162 of July 7, 1993, "On the Participation of Financial Institutions in the Fight against Money Laundering," and Section 218-3 of the Criminal Code, amended by Act 1.253 of July 12, 2002, "Relating to the Participation of Financial Undertakings in Countering Money Laundering and the Financing of Terrorism." On November 9, 2006, Section 218-3 of the Criminal Code was modified to adopt an "all crimes" approach to money laundering.

Monaco's anti-money laundering legislation, as amended, requires banks, insurance companies, stockbrokers, corporate service providers, portfolio managers, some trustees, and institutions within the offshore sector to report suspicious transactions to Monaco's financial intelligence unit (FIU), and to disclose the identities of those involved. Casino operators must alert the government of suspicious gambling payments possibly derived from drug trafficking or organized crime. The law imposes a five to ten-year jail sentence for anyone convicted of using illicit funds to purchase property, which itself is subject to confiscation. Act 1.162, as amended, institutes procedural requirements regarding internal compliance, client identification, and retention and maintenance of records. Sovereign Order 16.615 of January 2005 and Sovereign Order 631 of August 2006 mandate additional customer identification measures. Designated nonfinancial businesses and professions, such as lawyers, notaries, accountants, real estate brokers, and dealers in precious metals and stones, are not subject to reporting or record-keeping requirements.

Offshore companies are subject to the same due diligence and suspicious reporting obligations as banking institutions, and Monegasque authorities conduct on-site audits. Act 1.253 strengthens the "know your client" obligations for casinos and obliges companies responsible for the management and

administration of foreign entities not only to report suspicions to Monaco's FIU, but also to implement internal AML/CTF procedures. The FIU monitors these activities.

Monaco's FIU, the Service d'Information et de Controle sur les Circuits Financiers (SICCFIN), receives suspicious transaction reports, analyzes them, and forwards them to the prosecutor when they relate to drug trafficking, organized crime, terrorism, terrorist organizations, or the funding thereof. SICCFIN also supervises the implementation of AML legislation. Under Article 4 of Law 1.162, SICCFIN may suspend a transaction for twelve hours and advise the judicial authorities to investigate. SICCFIN has received between 200 and 400 suspicious transaction reports (STRs) annually from 2000 to 2006. In 2006, SICCFIN received 395 STRs, about 50 percent of which were submitted by banks and other financial institutions. SICCFIN received 60 requests for financial information from other FIUs in 2006. No statistics are currently available on the number of reports or requests received by SICCFIN in 2007.

Investigations and prosecutions are handled by the two-officer Money Laundering Unit (Unite de Lutte au Blanchiment) within the police. The Organized Crime Group (Groupe de Repression du Banditisme) may also handle cases. Seven police officers have been designated to work on money laundering cases. Four prosecutions for money laundering have taken place in Monaco, which have resulted in three convictions.

Monaco's legislation allows for the confiscation of property of illicit origin as well as a percentage of co-mingled illegally acquired and legitimate property. Authorities must obtain a court order to confiscate assets. Confiscation of property related to money laundering is restricted to the offenses listed in the Criminal Code. Authorities have seized assets exceeding 11.7 million euros (approximately U.S. $17 million) in value as of year-end 2006. Monaco and the United States signed a seized asset sharing agreement in March 2007.

In July and August 2002, the Government of Monaco (GOM) passed Act 1.253 and promulgated two Sovereign Orders intended to implement United Nations Security Council Resolution 1373 by outlawing terrorism and its financing. Monaco passed additional Sovereign Orders in April and August of that year, importing into Monegasque law the obligations of the UN International Convention for the Suppression of the Financing of Terrorism. In 2006, Monaco further amended domestic law to implement these obligations.

The Securities Regulatory Commissions of Monaco and France signed a memorandum of understanding (MOU) in March 2002 on the sharing of information between the two bodies. The GOM considers this MOU an important tool to combat financial crime, particularly money laundering. SICCFIN has signed information exchange agreements with over 20 foreign FIUs. In March 2007, Monaco ratified the European Convention on Mutual Assistance in Criminal Matters. Monaco has neither signed nor ratified the European Convention on Extradition, although it has concluded 15 extradition treaties with various countries. To date, there have been no extraditions on the grounds of money laundering, although the GOM has extradited criminals guilty of other offenses, mainly to Russia.

Monaco is a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). SICCFIN is a member of the Egmont Group of financial intelligence units. Monaco is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. The GOM has neither signed nor ratified the UN Convention against Corruption.

The Government of Monaco should amend its legislation to implement full corporate criminal liability. The Principality should continue to enhance its anti-money laundering and confiscation regimes by fully applying its AML/CTF reporting, customer identification, and record-keeping

requirements to all trustees and gaming houses. The GOM should also consider extending AML/CTF regulations to designated nonfinancial businesses and professions. SICCFIN should have the authority to forward reports and disseminate information to law enforcement even when the report or information obtained does not relate specifically to drug trafficking, organized crime, or terrorist activity or financing. Monaco should become a party to the UN Convention against Corruption.

Morocco

Morocco is not a regional financial center, but money laundering is a concern due to its narcotics trade, vast informal sector, trafficking in persons, and large level of remittances from Moroccans living abroad. According to the 2007 World Drug Report by the United Nations Office on Drugs and Crime (UNODC), Morocco remains a principal producer and exporter of cannabis, while credible estimates of Morocco's informal sector range between 17 and 40 percent of GDP. In 2006, remittances from Moroccans living abroad valued $5.4 billion, approximately nine percent of GDP. Although the true extent of the money laundering problem in the country is unknown, conditions exist for it to occur. In the past few years, the Kingdom of Morocco has taken a series of steps to address the problem, most notably the enactment of a comprehensive anti-money laundering (AML) bill in May 2007 and the establishment of a Financial Intelligence Unit, expected to become operational in Rabat in early 2008.

The predominant use of cash, informal value transfer systems and remittances from abroad all help fuel Morocco's informal sector. Bulk cash smuggling is also a problem. There are unverified reports of trade-based money laundering, including under-and over-invoicing and the purchase of smuggled goods. Most businesses are cash-based with little invoicing or paper trail. Cash-based transactions in connection with cannabis trafficking are of particular concern. According to the UNODC, Morocco remains the world's principal producer of cannabis, with revenues estimated at over $13 billion annually. While some of the narcotics proceeds are laundered in Morocco, most proceeds are thought to be laundered in Europe.

Unregulated money exchanges remain a problem in Morocco and were a prime impetus for Morocco's recent AML legislation. Although the legislation targets previously unregulated cash transfers, the country's vast informal sector creates conditions for this practice to continue. The Moroccan financial sector is underdeveloped, consisting of 16 banks, five government-owned specialized financial institutions, approximately 30 credit agencies, and 12 leasing companies. The monetary authorities in Morocco are the Ministry of Finance and the Central Bank—Bank Al Maghrib—that monitors and regulates the banking system. A separate Foreign Exchange Office regulates international transactions.

Since 2003, Morocco has taken a series of steps to tighten its AML controls. In December 2003, the Central Bank issued Memorandum No. 36, in advance of pending AML legislation that instructed banks and other financial institutions under its control to conduct internal analysis and investigations into financial transactions. The measures called for the reporting of suspicious transactions, retention of suspicious activity reports, and mandated "know your customer" procedures. In 2007, Morocco's AML efforts took a significant step forward with parliamentary passage and promulgation of a comprehensive AML law, which draws heavily from Financial Action Task Force (FATF) recommendations. The law requires the reporting of suspicious financial transactions by all responsible parties, both public and private, who in the exercise of their work, carry out or advise on the movement of funds possibly related to drug trafficking, human trafficking, arms trafficking, corruption, terrorism, tax evasion, or forgery. There were no prosecutions for money laundering in Morocco in 2007.

Morocco has a free trade zone in Tangier, with customs exemptions for goods manufactured in the zone for export abroad. There have been no reports of trade-based money laundering schemes or

terrorist financing activities using the Tangier free zone or the zone's offshore banks, which are regulated by an interagency commission chaired by the Ministry of Finance.

While there have been no verified reports of international or domestic terrorist networks using the Moroccan narcotics trade to finance terrorist organizations and operations in Morocco, investigations into the Ansar Al Mahdi and Al Qaeda in the Islamic Maghreb (AQIM) terrorist organizations are ongoing. At least two suspects arrested as part of the Ansar Al Mahdi cell were accused of providing financing to the cell.

Morocco has a relatively effective system for disseminating U.S. Government (USG) and United Nations Security Council Resolution (UNSCR) terrorist freeze lists to the financial sector and law enforcement. Morocco has provided detailed and timely reports requested by the UNSCR 1267 Sanctions Committee and some accounts have been administratively frozen (based on the U.S. list of Specially Designated Global Terrorists, designated pursuant to Executive Order 13224). In 1993, a mutual legal assistance treaty between Morocco and the United States entered into force.

Morocco is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of Financing of Terrorism, and the UN Convention against Transnational Organized Crime. On May 9, 2007, Morocco ratified the UN Convention against Corruption. Morocco is ranked 72 out of 179 countries surveyed in Transparency International's 2007 International Corruption Perception Index. Morocco has ratified or acceded to 11 of the 12 UN and international conventions and treaties related to counterterrorism. Morocco is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF).

In June 2003, Morocco adopted a comprehensive counterterrorism bill. This bill provided the legal basis for lifting bank secrecy to obtain information on suspected terrorists, allowed suspect accounts to be frozen, and permitted the prosecution of terrorist finance-related crimes. The law also provided for the seizure and confiscation of terrorist assets, and called for increased international cooperation with regard to foreign requests for freezing assets of suspected terrorist entities. The counterterrorism law brought Morocco into compliance with UNSCR 1373 requirements for the criminalization of the financing of terrorism. Other AML controls include legislation prohibiting anonymous bank accounts and foreign currency controls that require declarations to be filed when transporting currency across the border.

The Government of Morocco should continue to implement anti-money laundering/counter-terrorist financing (AML/CTF) programs and policies that adhere to world standards, including a viable FIU that receives, analyzes, and disseminates financial intelligence. The informal economy is very significant in Morocco and authorities are likely to face major challenges as the new AML regime is implemented. Police and customs authorities, in particular, should receive training on recognizing money laundering methodologies, including trade-based laundering and informal value transfer systems.

The Netherlands

The Netherlands is a major financial center and an attractive venue for the laundering of funds generated from a variety of illicit activities. Activities involving money laundering are often related to the sale of heroin, cocaine, cannabis, or synthetic and designer drugs (such as ecstasy). As a major financial center, several Dutch financial institutions engage in international business transactions involving large amounts of United States currency. There are, however, no indications that significant amounts of U.S. dollar transactions conducted by financial institutions in the Netherlands stem from illicit activity. Activities involving financial fraud are believed to generate a considerable portion of domestic money laundering. A recent report by the University of Utrecht commissioned by the Ministry of Finance has found that much of the money laundered in the Netherlands originates abroad,

but did not find evidence that it is predominantly owned by major drug cartels and other international criminal organizations. There are no indications of syndicate-type structures in organized crime or money laundering, and there is virtually no black market for smuggled goods in the Netherlands. Although under the Schengen Accord there are no formal controls on national borders within the EU, the Dutch authorities run special operations in its border areas with Germany and Belgium to keep smuggling to a minimum. Reportedly, money laundering amounts to 18.5 billion euros (approximately U.S. $27.14 billion) annually, or five percent of the Dutch GDP. The Netherlands is not an offshore financial center nor are there any free trade zones in the Netherlands.

In 1994, the Government of the Netherlands (GON) criminalized money laundering related to all crimes. In December 2001, the GON enacted legislation specifically criminalizing facilitating, encouraging, or engaging in money laundering. This eases the public prosecutor's burden of proof regarding the criminal origins of proceeds: under the law, the public prosecutor needs only to prove that the proceeds "apparently" originated from a crime. Self-laundering is also covered. In two cases in 2004 and 2005, the Dutch Supreme Court confirmed the broad application of the money laundering provisions by stating that the public prosecutor does not need to prove the exact origin of laundered proceeds for conviction, and that the general criminal origin as well as the knowledge of the perpetrator may be deduced from objective circumstances.

The Netherlands has an "all offenses" regime for predicate offenses of money laundering. The penalty for "deliberate acts" of money laundering is a maximum of four years' imprisonment and a maximum fine of 45,000 euros (approximately U.S. $66,000), while "liable acts" of money laundering (by people who do not know first-hand of the criminal nature of the origin of the money, but should have reason to suspect it) are subject to a maximum imprisonment of one year and a fine no greater than 45,000 euros (approximately U.S. $66,000). Habitual money launderers may be punished with a maximum imprisonment of six years and a maximum fine of 45,000 euros (approximately U.S. $66,000), and those convicted may also have their professional licenses revoked. In addition to criminal prosecution for money laundering offenses, money laundering suspects can also be charged with participation in a criminal organization (Article 140 of the Penal Code), violations of the financial regulatory acts, violations of the Sanctions Act, or noncompliance with the obligation to declare unusual transactions according to the Economic Offenses Act.

The Netherlands has comprehensive anti-money laundering (AML) legislation. The Services Identification Act and the Disclosure Act set forth identification and reporting requirements. All financial institutions in the Netherlands, including banks, bureaux de change, casinos, life insurance companies, securities firms, stock brokers, and credit card companies, are required to report cash transactions over certain thresholds (varying from 2,500 to 15,000 euros or approximately U.S. $3,670 to $21,000), as well as any less substantial transaction that appears unusual (applying a broader standard than "suspicious" transactions) to the Netherlands' financial intelligence unit (FIU-the Netherlands). Reporting requirements have been expanded to include financing companies, commercial dealers of high-value goods, notaries, lawyers, real estate agents/intermediaries, accountants, business economic consultants, independent legal advisers, tax advisors, trust companies and other providers of trust-related services. In 2007, the notary sector supervisor, BFT, reported that seven notaries allegedly violated AML rules but due to client confidentiality, the names of the notary firms were not released, . Reportedly, the agencies received cash payments above the reporting threshold and failed to report, and facilitated quick transfers of ownership for property. BFT investigators found 192 suspicious cases in 2004 and 2005, and a similar number in 2006 and 2007. The BFT has requested amended legislation.

Since 2005, the GON has implemented measures to enhance the effectiveness of its AML regime. A November 2005 National Directive on money laundering crimes mandates a financial investigation in every serious crime case, sets guidelines for determining when to prosecute for money laundering and provides technical explanations of money laundering offenses, case law, and the use of financial

intelligence. Revised indicators determine when an unusual transaction report must be filed. The indicators reflect a partial shift from a rule-based to a risk-based system and are aimed at reducing the administrative costs of reporting unusual transactions without limiting the preventive nature of the reporting system. Amendments to the Services Identification Act and Disclosure Act expand supervision authority and institute punitive damages. The revised legislation, which became effective on May 1, 2006, also incorporates a terrorist-financing indicator in the reporting system.

Financial institutions are required by law to maintain records necessary to reconstruct financial transactions for five years after termination of the relationship. There are no secrecy laws or fiscal regulations that prohibit Dutch banks from disclosing client and owner information to bank supervisors, law enforcement officials, or tax authorities. All institutions under the reporting and identification acts, and their employees, are specifically protected by law from criminal or civil liability related to cooperation with law enforcement or bank supervisory authorities. The Money Transfer and Exchange Offices Act, passed in June 2001, requires money transfer offices, as well as exchange offices, to obtain a permit to operate, and subjects them to supervision by the Central Bank. Every money transfer client must be identified and all transactions totaling more than 2,000 euros (approximately U.S. $2,935) must be reported to the FIU. Sharing of information by Dutch supervisors does not require formal agreements or memoranda of understanding (MOUs).

The FIU for the Netherlands is a hybrid administrative-law enforcement unit that in 2006 combined the original, administrative FIU MOT (Meldpunt Ongebruikelijke Transacties, or in English the Office for the Disclosure of Unusual Transactions) with its police counterpart, the Office of Operational Support of the National Public Prosecutor (BLOM). When MOT, established in 1994, and BLOM merged, the resulting entity was integrated within the National Police (KLPD). The new unit, FIU-the Netherlands, not only provides an administrative function that receives, analyzes, and disseminates the unusual and currency transaction reports filed by banks, financial institutions and other reporting entities, but it also provides a police function that serves as a point of contact for law enforcement. It forwards suspicious transaction reports (STRs) with preliminary investigative information to the Police Investigation Service. Over the last five years, the MOT and the BLOM have responded to international requests for financial and law enforcement information, including those from counterpart FIUs, so this merger has not changed the nature of the Dutch reporting system with respect to international cooperation. FIU-the Netherlands is a member of the Egmont Group.

Obliged entities that fail to file reports with the FIU-the Netherlands can be prosecuted in two ways. One of the four supervisory bodies, depending on the entity, may impose an administrative fine of up to 32,670 euros (approximately U.S. $47,905), depending on the size of the entity. The Dutch Tax Administration supervises commercial dealers; the Bureau Financieel Toezicht (BFT or Office for Financial Oversight) supervises notaries, lawyers, real estate agents, and accountants; de Nederlandsche Bank (Dutch Central Bank) supervises trust companies, casinos, banks, bureaux de change, and insurance companies; and the Authority for Financial Markets supervises clearinghouses, brokers, and securities firms. The public prosecutor may fine nonreporting entities 11,250 euros (approximately $16,495), or charge individuals failing to report with prison terms of up to two years. Under the Services Identification Act, those subject to reporting obligations must identify their clients, including the identity of beneficial owners, either at the time of the transaction or prior to the transaction, before providing financial services.

The FIU receives every unusual transaction report electronically through its secure website. In 2005, the FIU-the Netherlands received 181,623 reports and forwarded 38,481, totaling over 1.1 billion euros (approximately U.S. $1.6 billion), to enforcement agencies such as the police, fiscal police, and public prosecutor. In 2006, the FIU-the Netherlands received 172,865 unusual transaction reports and forwarded 34,531, totaling over 9.2 billion euros (approximately U.S. $13.5 billion) to enforcement agencies as suspicious transactions for further investigation. The average amount reported was 26,870 euros (approximately U.S. $39,400) in 2006, a decrease from the 28,945 euros (approximately U.S.

$42,440) average reported in 2005. Approximately 89 percent of the transactions are in euros, 8 percent are in other European currency (of which 5 percent are in English Pounds) and finally 3 percent of the transactions are in U.S. dollars.

To facilitate the forwarding of STRs, the FIU created an electronic network called Intranet Suspicious Transactions (IST). Fully automatic matches of data from the police databases are included with the unusual transaction reports forwarded to enforcement agencies. On January 1, 2003, the former MOT and BLOM organizations together created a special unit (the MBA unit) to analyze data generated from the IST. Under the new FIU-the Netherlands structure, the MBA continues to analyze IST data and forwards reports to the police. Since the money laundering detection system also covers areas outside the financial sector, the system is used for detecting and tracing terrorist financing activity. The FIU-the Netherlands provides the AML division of Europol with suspicious transaction reports, and Europol applies the same analysis tools as the FIU.

Current legislation requires Customs authorities to report unusual transactions to the FIU-the Netherlands. On June 15, 2007, EU regulation 1889/2005 on Liquid Assets Control introduced a currency declaration requirement for amounts valued over 10,000 euros for travelers entering and leaving Schengen-agreement countries. Travelers crossing Dutch borders must complete a declaration form. The Dutch use specially trained dogs at ports and airports to identify cash smugglers in 2006 finding four million euros (approximately $5.9 million) in passenger luggage at Schiphol airport.

The Netherlands has enacted legislation governing asset forfeiture. The 1992 Asset Seizure and Confiscation Act enables authorities to confiscate assets that are illicitly obtained or otherwise connected to criminal acts. The GON amended the legislation in 2003 to improve and strengthen the options for identifying, freezing, and seizing criminal assets. The police and several special investigation services are responsible for enforcement in this area. These entities have adequate powers and resources to trace and seize assets. All law enforcement investigations into serious crime may integrate asset seizure.

Authorities may seize any tangible assets, such as real estate or other conveyances that were purchased directly with proceeds tracked to illegal activities. Both moveable property and claims are subject to confiscation. Assets can be seized as a value-based confiscation. Legislation defines property for the purpose of confiscation as “any object and any property right” and provides for the seizure of additional assets controlled by a drug trafficker. Proceeds from narcotics asset seizures and forfeitures are deposited in the general fund of the Ministry of Finance.

To facilitate the confiscation of criminal assets, the GON has instituted special court procedures that enable law enforcement to continue financial investigations to prepare confiscation orders after the underlying crimes have been successfully adjudicated. All police and investigative services in the field of organized crime rely on the real time assistance of financial detectives and accountants, as well as on the assistance of the Proceeds of Crime Office (BOOM), a special bureau advising the Office of the Public Prosecutor in international and complex seizure and confiscation cases. To further international cooperation in this area, BOOM played a leading role in the creation of an informal international network of asset recovery specialists aiming to exchange information and share expertise. Known as the Camden Asset Recovery Network (CARIN), this network was established in The Hague in September 2004. .

Statistics provided by the Office of the Public Prosecutor show that the assets seized in 2006 amounted to 17 million euros (approximately U.S. $24.9 million). This compares with 11 million euros in 2005 and 11 million euros in 2004 (approximately U.S. $14.5 million and U.S. $13 million respectively, based on the exchange rates at the time). The United States and the Netherlands have had an asset-sharing agreement in place since 1994. The Netherlands also has an asset-sharing treaty with the United Kingdom, and an agreement with Luxembourg.

In June 2004, the Minister of Justice sent an evaluation study to the Parliament on specific problems authorities encountered with asset forfeiture in large, complex cases. In response to this report, the GON announced several measures to improve the effectiveness of asset seizure enforcement, including steps to increase expertise in the financial and economic field, assign extra public prosecutors to improve the coordination and handling of large, complex cases, and establish a specific asset forfeiture fund. The Office of the Public Prosecutor designed a centralized approach for large confiscation cases and a more flexible approach for handling smaller cases. The improvements took effect in 2006 and have significantly increased BOOM's capacity to handle asset forfeiture cases.

Terrorist financing is a crime in the Netherlands. In August 2004, the Act on Terrorist Crimes, implementing the 2002 EU framework decision on combating terrorism, became effective. The Act makes recruitment for jihad, and conspiracy to commit a terrorist act, criminal offenses. In 2004, the government created a National Counterterrorism Coordinator's Office to streamline and enhance Dutch counterterrorism efforts.

UN resolutions and EU regulations form a direct part of the national legislation on sanctions in the Netherlands. The "Sanction Provision for the Duty to Report on Terrorism," passed in 1977, was amended in June 2002 to implement European Union (EU) Regulation 2580/2001. United Nations Security Council Resolution (UNSCR) 1373 is implemented through Council Regulation 2580/01; listing is through the EU Clearinghouse process. The ministerial decree provides authority to the Netherlands to identify, freeze, and seize terrorist finance assets. The decree also requires financial institutions to report to the FIU all transactions (actually carried out or intended) involving persons, groups, and entities that have been linked, either domestically or internationally, with terrorism. Any terrorist crime automatically qualifies as a predicate offense under the Netherlands "all offenses" regime for predicate offenses of money laundering. Involvement in financial transactions with suspected terrorists and terrorist organizations listed on the United Nations (UN) 1267 Sanctions Committee's consolidated list or designated by the EU has been made a criminal offense. UNSCR 1267/1390 is implemented through Council Regulation 881/02. Sanctions Law 1977 also addresses this requirement parallel to the regulation in the Netherlands. The Dutch have taken steps to freeze the assets of individuals and groups included on the UNSCR 1267 Sanctions Committee's consolidated list.

The Netherlands does not require a collective EU decision to identify and freeze assets suspected of being linked to terrorism nationally. In these cases, the Minister of Foreign Affairs and the Minister of Finance make the decision to execute the asset freeze. Decisions take place within three days after a target is identified. Authorities have used this instrument several times in recent years. In three cases, national action followed the actions taking place on the EU level. In one case, the entity was included on the UN 1267 list and thus included in the list that circulated pursuant to EU regulation 2002/881. In two other cases, the Netherlands successfully nominated the entity/individual for inclusion on the autonomous EU list that is compiled pursuant to Common Position 2001/931.

The 2004 Act on Terrorist Offenses introduced Article 140A of the Criminal Code, which criminalizes participation in a terrorist organization, and defines participation as membership or providing provision of monetary or other material support. Article 140A carries a maximum penalty of fifteen years' imprisonment for participation in, and life imprisonment for leadership of, a terrorist organization. Nine individuals were convicted in March 2006 on charges of membership in a terrorist organization. Legislation expanding the use of special investigative techniques was enacted in February 2007.

Unusual transaction reports by the financial sector act as the first step against the abuse of religious organizations, foundations and charitable institutions for terrorist financing. No individual or legal entity using the financial system (including churches and other religious institutions) is exempt from the client identification requirement. Financial institutions must also inquire about the identity of the

ultimate beneficial owners. The second step, provided by Dutch civil law, requires registration of all active foundations with the Chambers of Commerce. Each foundation's formal statutes (creation of the foundation must be certified by a notary of law) must be submitted to the Chambers. Charitable institutions also register with, and report to, the tax authorities to qualify for favorable tax treatment. Approximately 15,000 organizations (and their managements) are registered in this way. The organizations must file their statutes, showing their purpose and mode of operations, and submit annual reports. Samples are taken for auditing. Finally, many Dutch charities are registered with or monitored by private "watchdog" organizations or self-regulatory bodies, the most important of which is the Central Bureau for Fund Raising. In April 2005, the GON approved a plan to improve Dutch efforts to fight fraud, money laundering, and terrorist financing by replacing the current initial screening of founders of private and public-limited partnerships and foundations with an ongoing screening system. The GON aimed to introduce the new system in 2007.

Certain groups of immigrants use informal banks to send money to their relatives in their countries of origin. However, indicators point to the misuse of these informal banks for criminal purposes, including a small number of informal bankers deliberately engaging in money laundering transactions and cross-border transfers of criminal money. Initial research by the Dutch police and Internal Revenue Service and Economic Control Service (FIOD/ECD) indicates that the number of informal banks and hawaladars in the Netherlands is rising. The Dutch Government plans to implement improved procedures for tracing and prosecuting unlicensed informal or hawala-type activity, with the Dutch Central Bank, FIOD/ECD, the Financial Expertise Center, and the Police playing a coordinating and central role. The Dutch Finance Ministry has participated in a World Bank-initiated international survey on money flows by immigrants to their native countries, with a focus on relations between the Netherlands and Suriname. The Dutch Central Bank has initiated a study into the number of informal banking institutions in the Netherlands. In Amsterdam, a special police unit has been investigating underground bankers. These investigations have resulted in the disruption of three major underground banking schemes.

The Netherlands is in compliance with all FATF Recommendations, with respect to both legislation and enforcement. The Netherlands also complies with the Second EU Money Laundering Directive and plans to implement the Third EU Money Laundering Directive through the adoption of a new act on combating money laundering and terrorist financing that will enter into force in 2008.

The United States enjoys good cooperation with the Netherlands in fighting international crime, including money laundering. In September 2004, the United States and the Netherlands signed bilateral implementing instruments for the U.S.-EU mutual legal assistance and extradition treaties; the agreements have not yet been ratified. One provision of the U.S.-EU legal assistance agreement would facilitate the exchange of information on bank accounts. In 2007, the Dutch Ministry of Justice and the Dutch National Police began working two operational money laundering initiatives with U.S. law enforcement authorities in the Netherlands. This is the first time that such operations have been attempted in the Netherlands.

The FIU supervised the PHARE Project for the European Union. The PHARE Project was the European Commission's Anti-Money Laundering Project for Economic Reconstruction Assistance and provided support to Central and Eastern European countries in the development and/or improvement of AML regulations. When the PHARE project concluded in December 2003, the FIU moved forward with the development of the FIU.NET Project, (an electronic exchange of current information between European FIUs by means of a secure intranet), which the FIU continues to use.

The Netherlands is a member of the Financial Action Task Force and the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The Netherlands was a founding member of the CARIN asset-recovery network, and participates in the Caribbean Financial Action Task Force as a Cooperating and Supporting Nation. As a member of the

Egmont Group, the FIU has established close links with the U.S Treasury's FinCEN as well as with other Egmont members, and is involved in efforts to expand international cooperation. The Netherlands is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime.

The Netherlands should continue its shift to the risk-based approach throughout its regulatory and AML/CTF regime, as well as proceed with enacting its new AML/CTF legislation. The GON should continue with its plans implementing a screening system for private and public-limited partnerships, including attendant requirements for all charities to register with a supervisory state or state-sanctioned body. The Netherlands should obtain statistics and examine the progress that has been achieved since the improvements in the asset forfeiture regime have been implemented. The GON should devote more resources toward getting better data and a better understanding of alternate remittance systems in the Netherlands, and channel more investigative resources toward tracing informal bank systems.

Netherlands Antilles

The Netherlands Antilles is comprised of the islands of Curacao, Bonaire, Dutch Sint Maarten, Saba, and Sint Eustatius. Though a part of the Kingdom of the Netherlands, the Netherlands Antilles has autonomous control over its internal affairs. The Government of the Netherlands Antilles (GONA) is located in Willemstad, the capital of Curacao, which is also the financial center for the five islands. A significant offshore sector and loosely regulated free trade zones, as well as narcotics trafficking and a lack of border control between Sint Maarten (the Dutch side of the island) and St. Martin (the French side), create opportunities for money launderers in the Netherlands Antilles.

The Netherlands Antilles' banking sector consists of seven local general banks, 14 investment institutions, one subsidiary of a foreign general banks, two branches of foreign general banks, 12 credit unions, six specialized credit unions, one savings bank, four savings and credit funds, 15 consolidated international banks, 18 nonconsolidated international banks, and 22 pension funds. The laws and regulations on bank supervision provide that international banks must have a physical presence and maintain records on the island. There are multiple insurance companies, including three subsidiaries of foreign life insurance companies, seven branches of foreign life insurance companies, six subsidiaries of foreign nonlife insurance companies, six branches of foreign insurance companies, and six independent insurance companies. In addition, there are two captive life insurance companies, 13 captive nonlife insurance companies, four professional reinsurance companies, and one other health insurance company.

The Netherlands Antilles has an offshore financial sector with 84 trust service companies providing financial and administrative services to an international clientele, which includes offshore companies, mutual funds, and international finance companies. As of September 2007, there were a total of 14,191 offshore companies registered with the Chamber of Commerce in the Netherlands Antilles, as is required by law. International corporations may be registered using bearer shares. The practice of the financial sector in the Netherlands Antilles is for either the bank or the company service providers to maintain copies of bearer share certificates for international corporations, which include information on the beneficial owner(s). The Netherlands Antilles also permits Internet gaming companies to be licensed on the islands. There are currently four-operator member and nine-nonoperator member licensed Internet gaming companies.

In February 2001, the GONA approved proposed amendments to the free zone law to allow e-commerce activities into these areas (National Ordinance Economic Zone no.18, 2001). It is no longer necessary for goods to be physically present within the zone as was required under the former free zone law. Furthermore, the name "Free Zone" was changed to "Economic Zone" (e-zone). Seven areas

within the Netherlands Antilles qualify as e-zones, five of which are designated for e-commerce. The remaining two e-zones, located at the Curacao airport and harbor, are designated for goods. These zones are minimally regulated; however, administrators and businesses in the zones have indicated an interest in receiving guidance on detecting unusual transactions.

Money laundering is a criminal offense in the Netherlands Antilles under the 1993 National Ordinance on the penalization of money laundering (O.G. 1993, no. 52), as amended by a 2001 National Ordinance (O.G. 2001, no. 77). This legislation establishes that prosecutors do not need to prove that a suspected money launderer also committed an underlying crime to obtain a money laundering conviction. In recent years, the GONA has taken steps to strengthen its anti-money laundering regime by expanding suspicious activity reporting requirements to nonfinancial sectors; introducing indicators for the reporting of unusual transactions for the gaming industry; issuing guidelines to the banking sector on detecting and deterring money laundering; and modifying existing money laundering legislation that penalizes currency and securities transactions by including the use of valuable goods. A GONA interagency anti-money laundering working group cooperates with its Kingdom counterparts.

Both bank and nonbank financial institutions, such as company service providers and insurance companies, are required by law to report suspicious transactions to the financial intelligence unit (FIU), the Meldpunt Ongebruikelijke Transacties (MOT NA). Obligated entities are also required to report all transactions over NAF 250,000 (approximately U.S. $142,000). Banks are required to maintain records for ten years and all other financial intermediaries must maintain records for five years. The GONA is currently amending its legislation to add designated nonfinancial businesses and professions as reporting entities, including lawyers, accountants, notaries, jewelers and real estate agents. It is expected that the legislation will be passed in 2008. Obligated entities are required to report suspected terrorist financing activity to the MOT NA as well, although terrorist financing is not a criminal offense in the Netherlands Antilles.

The MOT NA was established under the Ministry of Finance in 1997. Through October 2006, the MOT NA received 10,788 suspicious transaction reports totaling U.S. $1.3 billion. Of these, 283 were reported to the relevant law enforcement authorities. No statistics are currently available for 2007. The MOT NA currently has a staff of nine, and is engaged in increasing the effectiveness and efficiency of its reporting system. Progress has been reported in automating suspicious activity reporting. Additionally, the MOT NA has issued a manual for casinos on how to file reports and has started to install software in casinos that will allow reports to be submitted electronically. The MOT NA hosted a Kingdom of the Netherlands seminar in October 2007. The Government of the Netherlands plans to provide technical support to the MOT NA to improve their analytical capabilities with regard to terrorist financing.

The Central Bank of the Netherlands Antilles supervises all banking and credit institutions, including banks for local and international business, specialized credit institutions, savings banks, credit unions, credit funds, and pension funds. The Central Bank also supervises insurance companies, insurance brokers, mutual funds and administrators of these funds, and company service providers, all of which must be licensed by the Central Bank. The Central Bank has issued anti-money laundering guidelines for banks, insurance companies, pension funds, money transfer services, financial administrators, and company service providers. The guidelines also specifically include terrorist financing indicators. Entities under supervision must submit an annual statement of compliance. The Central Bank has provided training to different sectors on the guidelines. The Central Bank also established the Financial Integrity Unit to monitor corporate governance and market behavior.

As of May 2002, all persons entering or leaving one of the island territories of the Netherlands Antilles must report of the transportation of NAF 20,000 (approximately U.S. $11,300) or more in cash or bearer instruments to Customs officials. This provision also applies to those entering or leaving who

are demonstrably traveling together and who jointly carry with them money for a value of NAF 20,000 or more. Declaration of currency exceeding the threshold must include origin and destination. Violators may be fined up to NAF 250,000 (approximately U.S. $142,000) and/or face one year in prison.

In 2000, the GONA enacted the National Ordinance on Freezing, Seizing and Forfeiture of Assets Derived from Crime. The law allows the prosecutor to seize the proceeds of any crime proven in court. Civil forfeiture is not permitted.

Terrorist financing is not a separate crime in the Netherlands Antilles, although acts that can be considered to support terrorism are criminalized in Articles 49 and 50 of the Criminal Code. Although terrorist financing is not per se a crime, the GONA enacted legislation in 2002 allowing a judge or prosecutor to freeze assets related to the Taliban and Usama Bin Laden, as well as all persons and companies connected with them. The legislation contains a list of individuals and organizations suspected of terrorism. The Central Bank instructed financial institutions to query their databases for information on the suspects and to immediately freeze any assets found. In October 2002, the Central Bank instructed the financial institutions under its supervision to continue these efforts and to consult the UN website for updates to the list.

Netherlands Antilles' law allows the exchange of information between the MOT NA and foreign FIUs by means of memoranda of understanding and by treaty. The MOT NA's policy is to answer requests within 48 hours of receipt. A tax information exchange agreement (TIEA) between the Netherlands and the United States with regard to the Netherlands Antilles, signed in 2002, entered into force in March 2007. The Mutual Legal Assistance Treaty between the Netherlands and the United States applies to the Netherlands Antilles; however, the treaty is not applicable to requests for assistance relating to fiscal offenses addressed to the Netherlands Antilles. The U.S.-Netherlands Agreement Regarding Mutual Cooperation in the Tracing, Freezing, Seizure and Forfeiture of Proceeds and Instrumentalities of Crime and the Sharing of Forfeited Assets also applies to the Netherlands Antilles.

The MOT NA is a member of the Egmont Group. The Netherlands Antilles is a member of the Caribbean Financial Action Task Force (CFATF), and as part of the Kingdom of the Netherlands, participates in the Financial Action Task Force (FATF). The Netherlands Antilles is also a member of the Offshore Group of Banking Supervisors. The Kingdom of the Netherlands has extended its ratification of the 1988 UN Drug Convention to the Netherlands Antilles. The Kingdom of the Netherlands became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. In accordance with Netherlands Antilles' law, which stipulates that all the legislation must be in place prior to ratification, the GONA is preparing legislation to enable the Netherlands to extend ratification of the Convention to the Netherlands Antilles. Likewise, the Kingdom of the Netherlands has not yet extended ratification of the UN Convention against Transnational Organized Crime or the UN Convention against Corruption to the Netherlands Antilles.

The Government of the Netherlands Antilles has demonstrated a commitment to combating money laundering. However, the GONA should criminalize the financing of terrorism and enact the necessary legislation to implement the UN International Convention for the Suppression of the Financing of Terrorism. The Netherlands Antilles should also continue its focus on increasing regulation and supervision of the offshore sector and free trade zones, as well as pursuing money laundering investigations and prosecutions. The GONA should ensure that anti-money laundering regulations and reporting requirements are extended to designated nonfinancial businesses and professions.

Nicaragua

Nicaragua is not a regional financial center or a major drug producing country. However, it continues to serve as a significant transshipment point for South American cocaine and heroin destined for the

United States and—on a smaller scale—for Europe. There is evidence that the narcotics trade is increasingly linked to arms trafficking. This situation, combined with weak adherence to the rule of law, judicial corruption, the politicization of the public prosecutor's office and the Supreme Court, and insufficient funding for law enforcement institutions, makes Nicaragua's financial system an attractive target for money laundering. Nicaragua's geographical position—with access to both the Atlantic and the Pacific Oceans, porous border crossings to its north and south, and a lightly inhabited and underdeveloped Atlantic Coast area—makes it an area heavily used by transnational organized crime groups. These groups also benefit from Nicaragua's weak legal system and its ineffective fight against financial crimes, money laundering, human trafficking, and the financing of terrorism. Nicaraguan officials have expressed concern that, as neighboring countries have tightened their anti-money laundering laws, established financial intelligence units (FIUs), and taken other enforcement actions, more illicit money has moved into the vulnerable Nicaraguan financial system.

Nicaragua does not permit direct offshore bank operations, but it does permit such operations through nationally chartered entities. Bank and company bearer shares are permitted. Nicaragua has a well-developed indigenous gaming industry, which remains largely unregulated. Two competing casino regulation bills are currently in the National Assembly; the main difference between the bills is whether regulatory authority will fall under the tax authority or if an independent institution will be established to supervise the industry. There are no known offshore or Internet gaming sites in Nicaragua.

A number of foreign institutions own significant shares of the Nicaraguan financial sector. In 2008, GE Consumer Finance, one of the largest financial service firms in the world, will become the owner of Banco de America Central (BAC), which operates in several Central American countries, including Nicaragua. In 2007, HSBC purchased Banistmo, a Panamanian bank, and now operates under that name in Nicaragua. Most large Nicaraguan banks already maintain correspondent relationships with Panamanian institutions.

The entry into force of the Central America/Dominican Republic Free Trade Agreement (CAFTA-DR) in 2006 and the increased pace of regional integration suggest growing involvement of Nicaraguan financial institutions with international partners and clients. A new free trade agreement (FTA) with Taiwan will go into effect in 2008, which should expand Nicaragua's financial relationships with Asia. Nicaragua also just concluded FTA negotiations with Panama and, along with its Central American neighbors, is expected to begin negotiating an FTA with the EU.

As of January 2007, a total of 109 companies operate in 38 designated free trade zones (FTZs) in Nicaragua. As of December 2006, an estimated 80,000 persons were employed by companies operating in FTZs, producing a total of $900 million in export sales. The National Free Trade Zone Commission (CNZF), a state-owned corporation, regulates all FTZs and the companies located in them. The Nicaraguan Customs Agency also monitors all imports and exports of FTZ companies. While there is no indication that these FTZs are being used in trade-based money laundering schemes or by the financiers of terrorism, a June 2007 inspection by U.S. Customs agents uncovered evidence of transshipments of Chinese-made apparel.

On November 13, 2007, Nicaragua's National Assembly passed a new penal code that criminalizes terrorist financing, bulk cash smuggling, and money laundering beyond drug-related offenses. The penal code also expands legal protection for the financial sector, and defines crimes against the banking and financial system. When implemented, the new penal code should bring Nicaragua's anti-money laundering and counter-terrorist financing regime into greater compliance with the international standards of the Financial Action Task Force. However, the penalty for committing money laundering is still relatively low by international standards, with a sentence of five to seven years. The new penal code does not provide for the creation of an FIU.

While the adoption of the new penal code demonstrates the Government of Nicaragua's (GON) commitment to fight the financing of terrorism, money laundering, and other financial crimes, limited resources, corruption (including in the judiciary), and the lack of political will in some sectors continue to complicate efforts to counteract these criminal activities. Nicaragua has recently made improvements to its oversight and regulatory control of its financial system. Although the current Prosecutor General once advocated a narrow interpretation of money laundering law that only would penalize the laundering of proceeds from narcotics trafficking and not from other illegal activities, he now supports the formation of an FIU and by extension the prosecution of a wider range of money laundering-related offenses. However, the National Prosecutor's Office has still failed to prosecute a single money laundering case. This enforcement problem is exacerbated by the fact that the country does not have an operational FIU. The National Prosecutor's Office has prosecuted at least four cases of cash smuggling, although these crimes are currently considered only customs violations.

Law 285 of 1999 requires all financial institutions (including stock exchanges and insurance companies) under the supervision of the Superintendence of Banks and Other Financial Institutions (SIBOIF) to report cash deposits over $10,000 and suspicious transactions to the SIBOIF and to keep records for five years. The SIBIOF then forwards the reports to the Commission of Financial Analysis (CAF). All persons entering or leaving Nicaragua are also required to declare the transportation of currency in excess of U.S. $10,000 or its equivalent in foreign currency. All financial institutions not supervised by SIBIOF are required to report suspicious transactions directly to the CAF. Bank officials are held responsible for all of their institution's actions, including failure to report money laundering, and sanctions may be imposed on financial institutions and professionals of the financial sector, including internal auditors, who do not develop anti-money laundering programs or do not report to the appropriate authorities suspicious and unusual transactions that may be linked to money laundering, as required by the anti-money laundering law.

The SIBOIF is considered to be an independent and reputable financial institution regulator. The position of the Superintendent does not enjoy legal immunity, exposing the Superintendent to lawsuits from regulated institutions. Officers in financial institutions charged with reporting suspicious transactions to the SIBOIF are also unprotected legally with regard to their cooperation. Given the corruption in the judicial system, this exposure can limit the willingness of SIBIOF to make "unpopular" decisions; however, the institution's financial experts have reached out to the Nicaraguan National Police (NNP) to work with them. The SIBIOF has regularly fined banks for not reporting suspicious transactions. The willingness of the SIBIOF and NNP to investigate financial crimes, and a substantial level of cooperation between the Attorney General's Office and the NNP on financial crimes and money laundering issues, has resulted in a greater adherence by banks to the reporting requirements contained in Law 285.

On paper, the CAF is comprised of representatives from various elements of law enforcement and banking regulators and is responsible for detecting money laundering trends, coordinating with other agencies and reporting its findings to Nicaragua's National Anti-Drug Council. The CAF does not analyze the information received, and is not considered to be a professional or independent unit. It is ineffective due to an insufficient budget, the politicization of its leadership, and a lack of fully dedicated, trained personnel, equipment and strategic goals. All of its members have primary responsibilities in their parent institutions, which take precedence over CAF duties. The CAF is headed by the National Prosecutor, who receives the reports from banks and decides whether to refer them to the NNP for further investigation.

The NNP's Economics Crimes Unit and the Office of the National Prosecutor are in charge of investigating financial crimes, including money laundering and terrorist financing. The Office of the National Prosecutor is in the process of creating its Economic Crimes Unit to work in tandem with the NNP. The United States has successfully supported the creation of a vetted unit within the NNP. The

unit has been conducting investigations into money laundering and drug related crimes since March 2007 and is expected to work closely with the Attorney General's office.

In October 2007, following publicity that highlighted the consequences of Nicaragua's being one of the few countries in Latin America without an FIU, the National Assembly renewed debate on a 2004 bill creating an independent FIU. The 2004 bill creates a central, independent FIU that would replace and enhance the functions of the CAF and establish more stringent reporting requirements. In August 2007, the SIBIOF suggested amendments to the bill before the National Assembly that would bring the proposed FIU into compliance with all Egmont Group of FIUs requirements.

Under the new penal code adopted by the National Assembly in November 2007, terrorism and its financing are now crimes in Nicaragua. Through five SIBIOF administrative decrees, the GON also has the authority to identify, freeze, and seize terrorist-related assets, but has not as yet identified any such active cases. Reportedly, there are no hawala or other similar alternative remittance systems operating in Nicaragua, and the GON has not detected any use of gold, precious metals or charitable organizations to disguise transactions related to terrorist financing. However, there are informal "cash and carry" networks for delivering remittances from abroad.

There are over 300 micro-finance institutions (MFI) in Nicaragua, serving over 300,000 clients and handling over U.S. $400 million. MFIs in Nicaragua dominate the informal economy and manage a significant portion of the remittances. Over half of this market is handled by five institutions that have now converted to become formal banks. One institution, Banco Pro-Credit, is a branch of a German MFI institution that also has branches in Eastern Europe and Africa. The MFI sector has grown steadily at about 25 percent per year since 1999. While the five MFIs that are now formal banks are regulated by the SIBIOF, all the others are currently unregulated. These institutions are, however, still subject to the reporting requirements in Law 285 and to financial crimes listed in the current Penal Code. Any crimes committed fall under the jurisdiction of the Economic Crimes unit of the National Police and the National Prosecutor's Office.

Nicaragua is a party to the 1988 United Nations Drug Convention, the UN International Convention on the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GON has also ratified the Inter-American Convention on Mutual Legal Assistance in Criminal Matters and the Inter-American Convention against Terrorism. Nicaragua is a member of the Money Laundering Experts Working Group of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD), and the Caribbean Financial Action Task Force (CFATF). Due to Nicaragua's failure to establish a functional FIU, it is the only country in Central America and one of the only countries in the Americas that does not have an FIU and is not a member of the Egmont Group of FIUs. Due to corruption in the Nicaraguan judiciary, the United States has cut off direct assistance to the Nicaraguan Supreme Court.

The Government of Nicaragua has made progress in its efforts to combat financial crime by expanding the predicate crimes for money laundering beyond narcotics trafficking and criminalizing terrorist financing. However, the GON also needs to allocate the necessary resources to develop an effective financial intelligence unit, and combat corruption. Nicaragua should develop a more effective method of obtaining information and cooperation from foreign law enforcement agencies and banks, take steps to immobilize its bearer shares and adequately regulate its gambling industry. These actions, coupled with increased enforcement, would significantly strengthen the country's financial system against money laundering and terrorist financing, and would bring Nicaragua closer to compliance with relevant international anti-money laundering and counter-terrorist financing standards and controls.

Nigeria

Although the Federal Republic of Nigeria is not an offshore financial center, Nigeria's large economy is a hub for the trafficking of persons and narcotics. Nigeria is a major drug-transit country and is a center of criminal financial activity, reportedly for the entire continent. Individuals and criminal organizations have taken advantage of the country's location, weak laws, systemic corruption, lack of enforcement, and poor socioeconomic conditions to strengthen their ability to perpetrate financial crimes at home and abroad. Nigerian criminal organizations are adept at devising new ways of subverting international and domestic law enforcement efforts and evading detection. Their success in avoiding detection and prosecution has led to an increase in many types of financial crimes, including bank fraud, real estate fraud, and identity theft. In addition, advance fee fraud, also referred to internationally as "419" fraud, in reference to the fraud section in Nigeria's criminal code, is a lucrative financial crime that generates hundreds of millions of illicit dollars annually for criminals. Despite years of government effort to counter rampant crime and corruption, Nigeria continues to be plagued by crime. The establishment of the Economic and Financial Crimes Commission (EFCC) along with the Independent Corrupt Practices Commission (ICPC) and the improvements in training qualified prosecutors for Nigerian courts yielded some successes in 2006 and 2007.

In June 2001, the Financial Action Task Force (FATF) placed Nigeria on its list of noncooperative countries and territories (NCCT). In December 2002, Nigeria enacted two pieces of legislation to remedy the deficiencies. It passed an amendment to the 1995 Money Laundering Act extending the scope of the law to cover the proceeds of all crimes. The Government of Nigeria (GON) also passed an amendment to the 1991 Banking and Other Financial Institutions (BOFI) Act expanding coverage of the law to stock brokerage firms and foreign currency exchange facilities, giving the Central Bank of Nigeria (CBN) greater power to deny bank licenses, and allowing the CBN to freeze suspicious accounts. The third piece of legislation, the 2004 Economic and Financial Crimes Commission (Establishment) Act, established the Economic and Financial Crimes Commission (EFCC), the body that investigates and prosecutes money laundering and other financial crimes, and coordinates information sharing. The Economic and Financial Crimes Commission Act also criminalizes the financing of terrorism and participation in terrorism. Violation of the Act carries a penalty of up to life imprisonment. In May 2006, the FATF visited Nigeria to conduct an evaluation of the revisions made to the government's AML regime. FATF recognized that the GON had remedied the major deficiencies in its anti-money laundering (AML) regime and removed Nigeria from the NCCT list.

Since its inception in April 2004, the EFCC has had the mandate to investigate and prosecute financial crime. It has recovered or seized assets from people guilty of fraud both inside and outside of Nigeria, including a syndicate that included highly placed government officials who were defrauding the Federal Inland Revenue Service (FIRS). Several influential individuals have been arrested and are currently awaiting trial. EFCC members also embarked upon a campaign to identify and prosecute former officials. Some EFCC members have been killed for their efforts to expose and enforce the laws against corruption and financial crime.

The National Assembly passed the Money Laundering (Prohibition) Act (2004), which applies to the proceeds of all financial crimes. Nigeria also employs the 1995 Foreign Exchange (Monetary and Miscellaneous Provisions) Act. The legislation gives the CBN greater power to deny bank licenses and freeze suspicious accounts. This legislation also strengthens financial institutions by requiring more stringent identification of accounts, removing a threshold for suspicious transactions, and lengthening the period for retention of records. Money laundering controls apply to banks and other financial institutions, including stock brokerages and currency exchange house, as well as designated nonfinancial businesses and professions (DNFBPs). These institutions include dealers in jewelry, cars and luxury goods, chartered accountants, audit firms, tax consultants, clearing and settlement companies, legal practitioners, hotels, casinos, supermarkets and other businesses that the Federal Ministry of Commerce designates as obliged. The EFCC Act provides safe-harbor provisions to

obliged entities. Nigeria has no secrecy laws that prevent the disclosure of client and ownership information by domestic financial services companies to bank regulatory and law enforcement authorities.

The Special Control Unit Against Money Laundering (SCUML), is a special unit in the Ministry of Commerce which monitors, supervises, and regulates the activities of all DNFBPs. Oversight, however, has reportedly not been very rigorous or effective. Amendments to the 2004 EFCC Act gave the EFCC the authority to investigate and prosecute money laundering, enlarged the number of EFCC board members, enabled the EFCC police members to bear arms, and banned interim court appeals that hinder the trial court process.

The Nigerian Financial Intelligence Unit (NFIU), established in 2005, derives its powers from the Money Laundering (Prohibition) Act of 2004 and the Economic and Financial Crimes Commission Act of 2004. Housed within the EFCC, it is the central agency for the collection, analysis and dissemination of information on money laundering and terrorist financing. The NFIU is a significant component of the EFCC, complementing the EFCC's directorate of investigations. It does not carry out its own investigations. Legal provisions give the NFIU power to receive suspicious transaction reports (STRs) submitted by financial institutions and designated nonfinancial businesses and professions. The NFIU also receives reports involving the transfer to or from a foreign country of funds or securities exceeding U.S. $10,000 in value. All financial institutions and designated nonfinancial institutions are required by law to furnish the NFIU with details of these financial transactions.

The NFIU fulfills a crucial role in receiving and analyzing STRs. As a result of the NFIU's activities, banks have improved both their timeliness and quality in filing STRs reported to the NFIU. The NFIU has access to records and databanks of all government and financial institutions, and it has entered into memoranda of understandings (MOUs) on information sharing with several other FIUs. In 2006, the NFIU received 3,772,843 currency transaction reports (CTRs). Out of the 47 cases the NFIU developed, 12 investigations are ongoing, and the NFIU disseminated 18 and placed 10 under monitoring. The NFIU closed seven in-house cases. Because the disseminated cases are still under investigation, no formal feedback came from stakeholders in either 2006 or 2007. There were 73 money laundering convictions from January 2005 through October 2006. The trial court process has improved after several experienced judges received assignations specifically to handle EFCC cases; encouraged, EFCC officials have brought more cases to court. Additional information for 2007 is not available.

Due to the EFCC's activities, the enactment of new laws, and a public enlightenment campaign, crimes such as bank fraud and counterfeiting have been reported and prosecuted, sometimes for the first time. The EFCC is the agency with the most capacity to effectively investigate and prosecute financial crimes, including money laundering and terrorist financing. The EFCC coordinates agencies' efforts in pursuing financial crime investigations. In addition to the EFCC, the National Drug Law Enforcement Agency (NDLEA), the Independent Corrupt Practices Commission (ICPC), and the Criminal Investigation Department of the Nigeria Police Force (NPF/CID) are empowered to investigate financial crimes. Reportedly, the Nigerian Police Force is incapable of handling financial crimes because of alleged corruption and poor institutional capacity.

In 2007, the EFCC marked significant successes in combating financial crime. Through EFCC efforts, a former inspector general of police was arrested and prosecuted for financial crimes valued at over U.S. $13 million. The GON seized his assets and froze his bank accounts. Currently serving a prison sentence, he still faces 92 charges of money laundering and official corruption. Five former state governors are under investigation for money laundering. The EFCC is working with the FBI on a case involving a group of money brokers laundering money through banks in the United States. In 2006, the EFCC received a surge of petitions and leads provided by whistleblowers. Reportedly, many of

these alleged abuses of office involved politically exposed persons (PEPs) and/or their collaborators. As the period coincided with preparations for the general elections in 2007, some of the investigations were politically charged. The Legal and Prosecution Unit, responsible for the prosecution of all cases, is examining 437 of these cases for possible prosecution.

The Unit prosecuted several high profile cases involving powerful and well connected persons and their associates. The EFCC filed 588 cases between 2006 and mid-2007. In 2007, the Legal Unit had obtained 53 convictions by mid-year. Investigations led to the recovery of approximately 30 billion naira (approximately U.S. $259 million). Suspects returned several other billions of naira when it became apparent that the Commission was about to expose the abuses. Some governors were arrested for laundering their state government funds. The Executive Chairman, appearing before the Senate to present a report of the Commission's activities, revealed allegations of corrupt practices and abuse of office reportedly associated with 31 out of the 36 then serving Governors. Some of the Governors had constitutional immunity that expired in May 2007. They are now standing trial in various courts for various offenses including money laundering.

While the NDLEA has the authority to handle narcotics-related cases, it does not have adequate resources to trace, seize, and freeze assets. Cases of this nature are usually referred to the EFCC. Depending on the nature of the case, the tracing, seizing, and freezing of assets may be executed by the EFCC, NDLEA, NPF, or the ICPC. The proceeds from seizures and forfeitures pass to the federal government, and the GON uses a portion of the recovered sums to provide restitution to the victims of the criminal acts. The banking community is cooperating with law enforcement to trace funds and seize or freeze bank accounts. Since its establishment the EFCC has reportedly seized assets worth $5 billion.

Section 20 of the 2004 EFCC Act provides for the forfeiture of assets and properties to the federal government after a money laundering conviction. Foreign assets are also subject to forfeiture. The properties subject to forfeiture are set forth in EFCC Act Sections 24-26, and include any real or personal property representing the gross receipts a person obtains directly as a result of the violation of the act, or traceable to such receipts. They also include any property representing the proceeds of an offense under the laws of a foreign country within which the offense or activity would be punishable for more than one year. All means of conveyance, including aircraft, vehicles, or vessels used or intended to be used to transport or facilitate the transportation, sale, receipt, possession or concealment of the economic or financial crimes is likewise subject to forfeiture. Forfeiture is possible only as part of a criminal prosecution. There is no comparable law providing for civil forfeiture independent of a criminal prosecution, but the EFCC has established a committee addressing this deficiency by drafting legislation.

The EFCC has the authority to prevent the use of charitable and nonprofit entities as money laundering vehicles, although it has not reported any cases involving these entities.

Nigerian criminals initially made the advance fee fraud scheme infamous. Today, nationals of many African countries and from a variety of countries around the world also perpetrate advance fee fraud. While there are many variations, the main goal of 419 frauds is to deceive victims into the payment of a fee by persuading them that they will receive a very large benefit in return, or by persuading them to pay fees to "rescue" or help a newly-made "friend" in some sort of alleged distress. A majority of these schemes end after the victims have suffered monetary losses, but some have also involved kidnapping, and/or murder. Perpetrators use the Internet to target businesses and individuals around the world.

The Government of Nigeria continued throughout 2007 with its efforts to eradicate 419 crimes. GON efforts previously led to the successful prosecution and conviction of a number of them, but the problem is far from over. Following the promulgation of the Advance Fee Fraud Act 2006 the EFCC held an interactive session with stakeholders. The EFCC also briefed cyber cafe operators, business

centers, Internet service providers, telecommunication companies and banks on their responsibilities under the new law. One of their requirements is to register their businesses with the EFCC. To keep pace with the sophistication with which the fraudsters operate, the EFCC deployed interception technology to enhance the investigation of crimes, particularly those committed through cyberspace. The Advance Fee Fraud Unit burst several employment, credit card, and e-payment scams, shut down several domains and cloned websites, raided residential houses, seized computers, and blocked fraudulent e-mail addresses, telephone lines and faxes associated with cybercrimes. Despite the progress the EFCC has made, there have been few recorded successes as a result of the EFCC's cybercrime initiatives.

The EFCC's success in investigating and prosecuting financial crime, especially high-level corruption, has brought it both the support of the international community and the ire of corrupt officials. In December 2007, the Government of Nigeria reassigned the EFCC Chairman, the country's highest ranking and most publicly visible anti-corruption official, Nuhu Ribadu, to a year-long training course. This reassignment coincides with the high-profile trials of several officials, including seven former governors. Ribadu has served as the face of Nigerian AML/CTF efforts, and his removal could undermine the perception of the GON's commitment to fighting corruption. The reassignment of Ribadu may also impact the NFIU's autonomy and its ability to act independently.

Nigeria criminalized the financing of terrorism under the Economic and Financial Crimes Commission (Establishment) Act of 2004. The EFCC has authority under the act to identify, freeze, seize, and forfeit terrorist finance-related assets. Nigerian financial institutions periodically receive the UNSCR 1267 Sanctions Committee's consolidated list, but have not yet detected a case of terrorist financing within the banking system.

Nigeria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Nigeria has also ratified the African Union Convention on the Prevention and Combating of Terrorism and the African Union Convention on Preventing and Combating Corruption. Nigeria ranks 147 out of 180 countries in Transparency International's 2007 Corruption Perceptions Index.

The United States and Nigeria have a Mutual Legal Assistance Treaty, which entered into force in January 2003. Nigeria has signed memoranda of understanding with Russia, Iran, India, Pakistan and Uganda to facilitate cooperation in the fight against narcotics trafficking and money laundering. Nigeria has also signed bilateral agreements for exchange of information on money laundering with South Africa, the United Kingdom, and all Commonwealth and Economic Community of West African States countries. The EFCC worked with foreign partners to raid notorious cyber cafes to curtail the activities of the 419 fraudsters. The EFCC collaborated with the United States Postal Service and the UK Serious and Organized Crime Agency (SOCA) to intercept over 15,000 counterfeit checks. A collaboration scheme between the EFCC, the United States, the UK and the Dutch was constituted to more effectively address the problem of international fraud, including identity theft and e-marketing fraud. Nigeria is a member of the Intergovernmental Task Force against Money Laundering in West Africa (GIABA), a FATF-style regional body. During 2007, Nigeria held the Directorship General of GIABA. The NFIU is a member of the Egmont Group.

The Government of Nigeria continued to pursue money laundering both within and outside the country in 2007. Nigeria should continue to pursue its anti-corruption program and support both the ICPC and EFCC in their mandates to investigate and prosecute corrupt government officials and individuals. Nigeria should take steps to ensure the autonomy and independence of those entities. GON should strengthen the authority of the SCUML to supervise designated nonfinancial businesses and professions by moving the Special Control Unit out from under the Ministry of Commerce. The GON should continue to engage with the FATF and other relevant international organizations to identify and

eliminate remaining anti-money laundering deficiencies. Nigeria should ensure that the Police Force has the capacity to function as an investigative partner in financial crime cases, as well as work to eradicate any corruption that might exist within that and other law enforcement bodies. Nigeria should continue to support the EFCC's efforts, including drafting a law for civil forfeiture provisions to the AML/CTF framework, and pursuing those who commit financial crime, regardless of political status. Nigeria should continue towards implementation of a comprehensive AML regime that promotes respect the rule of law; willingly shares information with foreign regulatory and law enforcement agencies; is capable of thwarting money laundering and terrorist financing; and maintains compliance with all relevant international standards.

Pakistan

Pakistan is not considered a regional or offshore financial center; however, financial crimes related to narcotics trafficking, terrorism, smuggling, tax evasion, corruption and fraud are significant problems. Pakistan is a major drug-transit country. The abuse of the charitable sector, smuggling, trade-based money laundering, hawala, and physical cross-border cash transfers are the common methods used to launder money and finance terrorism in Pakistan. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets.

Pakistan does not have firm control of its borders with Afghanistan, Iran and China, facilitating the flow of smuggled goods to the Federally Administered Tribal Areas (FATA) and Baluchistan. Some goods such as foodstuffs, electronics, building materials, and other products transiting Pakistan duty-free under the Afghan Transit Trade Agreement are sold illegally in Pakistan. Counterfeit goods generate substantial illicit proceeds that are laundered. Private unregulated charities are also a major source of illicit funds for international terrorist networks. Madrassas have been used as training grounds for terrorists and for terrorist funding. The lack of control of madrassas, similar to the lack of control of Islamic charities, allows terrorist and jihadist organizations to receive financial support under the guise of support of Islamic education.

Money laundering and terrorist financing are often accomplished in Pakistan via the alternative remittance system called hundi or hawala. This system is also widely used by the Pakistani people for informal banking purposes, although controls have been significantly tightened since 2002. In June 2004, the State Bank of Pakistan required all hawaladars to register as authorized foreign exchange dealers and to meet minimum capital requirements. Despite the State Bank of Pakistan's efforts, unlicensed hawaladars still operate illegally in parts of the country (particularly Peshawar and Karachi), and authorities have taken little action to identify and enforce the regulations prohibiting nonregistered hawaladars. Most illicit funds are transacted through these unlicensed operators. Fraudulent invoicing is typical in hundi/hawala counter valuation schemes. However, legitimate remittances from the roughly five million Pakistani expatriates residing abroad, sent via the hawala system prior to 2001, now flow mostly through the formal banking sector and have increased significantly to U.S. $5.5 billion in 2006-2007.

Pakistan has established a number of Export Processing Zones (EPZs) in all four of the country's provinces. Although no evidence has emerged of EPZs being used in money laundering, inaccurate invoicing is common in the region and could be used by entities operating out of these zones. In 2007, the Directorate General of Customs Intelligence (DGCI) investigated a well-known Pakistani business group involved with trade-based money laundering. The business over-invoiced the value and quantity of the exports of garments and textiles to Dubai and Saudi Arabia. The chairman of the business group and his partners held 49 percent shares in the Dubai-based company that imported many of the goods. The investigation also revealed that the business group used hawala to transfer large amounts of money and value through a prominent foreign exchange company based in Karachi. From 2001-2007, the value of the trade consignments totaled U.S. $330 million.

Pakistan has adopted measures to strengthen its financial regulations and enhance the reporting requirements for the banking sector to reduce its susceptibility to money laundering and terrorist financing. For example, financial institutions are required to follow "know your customer" provisions and must report within three days any funds or transactions they believe are proceeds of criminal activity.

Pakistan became a member of the Asia/Pacific Group on Money Laundering (APG) in 2000, therefore accepting the APG requirement that members develop, pass and implement anti-money laundering and counter-terrorist financing legislation and other measures based on accepted international standards. A high-level APG delegation visited Pakistan in early July 2007 to discuss Pakistan's long-delayed passage of comprehensive anti-money legislation. At its July plenary, APG members agreed that unless Pakistan enacts and proclaims into force consolidated AML legislation or issues a Presidential Ordinance prior to December 31, 2007, Pakistan's membership could be suspended.

On September 8, President Musharraf signed an ordinance to implement the long-awaited AML bill through a presidential ordinance. While creating this ordinance averted suspension of membership in the APG, Pakistan still has work ahead to meet international standards, especially the core FATF Recommendations related to the criminalization of money laundering and suspicious transaction reporting.

Some of the weaknesses identified in the new AML Ordinance include the following: Not all of the FATF designated categories of offenses (e.g., smuggling, racketeering, trafficking in persons, sexual exploitation, arms trafficking, and environmental crime) are covered as predicate offenses. The intent and knowledge requirement required to prove the offense of money laundering is not consistent with the standards set out in the Vienna and Palermo Conventions. Only the concealment of criminal proceeds is an offense, not the transfer of legitimate money to promote criminal activity. The definition of what constitutes a suspicious transaction is not adequate as it does not cover cases where an individual "suspects" or "has reason to suspect" that funds are the proceeds of criminal activity. The Ordinance also does not contain any specific requirement to report transactions in relation to terrorist financing. The forfeiture procedures set forth in the law are cumbersome and will inhibit the successful seizure and confiscation of property involved in offenses. Lastly, the reporting structure of the Financial Monitoring Unit may affect its independence and effectiveness.

The AML ordinance formally establishes a Financial Monitoring Unit (FMU) to monitor suspicious transactions. However, it is subject to the supervision and control of the General Committee, comprised of several Government of Pakistan (GOP) cabinet secretaries, thus limiting its independence. Because Pakistan has lacked a central repository for the reporting of suspicious transactions and the lack of protection from liability for reporting, very few suspicious transactions have been reported or utilized. From July 2006 through June 2007, 22 suspicious transactions were reported to the State Bank of Pakistan by various banks and five referred to law enforcement agencies for investigation. Currently, the FMU has yet to be fully staffed and investigators have not been adequately trained.

Several law enforcement agencies are responsible for enforcing financial crimes laws. The National Accountability Bureau (NAB), the Anti-Narcotics Force (ANF), the Federal Investigative Agency (FIA), and the Directorate of Customs Intelligence and Investigations (CII) all oversee Pakistan's financial enforcement efforts. In addition to the 2007 Anti-Money Laundering Ordinance, major laws in these areas include: The Anti-Terrorism Act of 1997, which defines the crime of terrorist finance and establishes jurisdiction and punishments; the National Accountability Ordinance of 1999, which requires financial institutions to report corruption related suspicious transactions to the NAB and establishes accountability courts; and the Control of Narcotics Substances Act of 1997 which criminalizes acts of money laundering associated with drug offenses and requires the reporting of narcotics related suspicious transactions. The NAB, FIA, ANF and customs have the ability to seize

assets whereas the State Bank of Pakistan has the ability to freeze assets. The ANF shares information about seized narcotics assets and the number of arrests with the USG.

Pakistan has also adopted measures to strengthen its financial regulations and enhance the reporting requirements for the financial sector to reduce its susceptibility to money laundering and terrorist financing. The State Bank of Pakistan and the Securities and Exchange Commission of Pakistan (SECP) are the country's primary financial regulators. They have established AML units to enhance financial sector oversight. However, these units often lack defined jurisdiction and adequate resources to effectively supervise the financial sector on AML/CTF controls. The State Bank of Pakistan has introduced regulations on AML that are generally consistent with the FATF recommendations in the areas of "know your customer" and enhanced due diligence procedures, record retention, the prohibition of shell banks, and the reporting of suspicious transactions. The Securities and Exchange Commission of Pakistan, which has regulatory oversight for nonbank financial institutions, has also applied "know your customer" regulations to stock exchanges, trusts, and other nonbank financial institutions.

Pakistan has specifically criminalized various forms of terrorist financing under the Anti-Terrorism Act (ATA) of 1997. Sections 11H-K provide that a person commits an offence if he is involved in fund raising, uses and possesses property, or is involved in a funding arrangement intending that such money or other property should be used, or has reasonable cause to suspect that they may be used, for the purpose of terrorism. Pakistan has the ability to freeze bank accounts and property held by terrorist individuals and entities. Pakistan has issued freezing orders for terrorists' funds and property in accordance with UN Security Council Resolutions 1267 and 1373. The State Bank of Pakistan circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. The ATA of 1997 also allows the government to proscribe a fund, entity or individual on the grounds that it is involved with terrorism. This done, the government may order the freezing of its accounts. Section 11B of the ATA specifies that an organization is proscribed or listed if the GOP has reason to believe that it is involved with terrorism. In 1997, 16 names were listed in annex to the ATA; none have been added since. As of 2006, bank accounts of 43 individuals and entities had been frozen under various UNSCRs. However, there have been some deficiencies concerning the timeliness and thoroughness of the asset freezing.

A Charities Registration Act has been under consideration by the Ministry of Welfare for some time. Currently, the Economic Affairs Division of the Ministry of Finance is reviewing the draft text and will then forward the bill to the Ministry of Law for review. The bill will then require approval by the cabinet and National Assembly, unless issued as a Presidential Ordinance by the President. Under this bill, charities would have to prove the identity of their directors and open their financial statements to government scrutiny. Currently, charities can register under one of a dozen different acts, some dating back to the middle of the nineteenth century. The Ministry of Social Welfare hopes that when the new legislation is enacted, it will be better able to monitor suspicious charities and ensure that they have no links to designated terrorists or terrorist organizations.

Current efforts to crack down on the flow of illicit funds via charitable organizations are limited to closure of the charity. There is little follow-up on suspect individuals associated with charities in question, thus allowing them to operate freely under alternate names. The court system has also failed to affirm Pakistan's international obligations and maintain closure of UN-proscribed charitable organization. In one such case, a provincial court in Karachi permitted a charity to continue operating in the face of a closure order, provided the charity in question only engaged in humanitarian operations. The GOP failed to aggressively appeal this court decision.

Reportedly, bulk cash couriers are the major source of funding for terrorist activities. According to the Pakistan Central Board of Revenue, cash smuggling is an offense punishable by up to five years in prison. The State Bank of Pakistan legally allows individuals to carry up to U.S. $10,000 in dollars or

the foreign currency equivalent. In tracking the cross border movement of currency Pakistan currently has reporting requirements only for the exportation of currency not the importation of currency. Although there is no requirement for the inbound reporting of currency, Pakistan is in compliance with FATF's Special Recommendation IX as they have the ability to ask anyone entering Pakistan if they are bringing in any currency. There are joint counters at international airports staffed by the State Bank of Pakistan and Customs to monitor the transportation of foreign currency. As a result of cash courier training received by Pakistan in 2006, their efforts to stop and seize the illicit cross-border movement of cash have increased. For example, during 2007 authorities made a number of significant cash seizures at the international airports in Karachi, Lahore and Peshawar as well as land border crossings.

Pakistan is party to the 1988 UN Drug Convention and the UN Convention against Corruption and has signed, but not ratified, the UN Convention against Transnational Crime. Pakistan is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism. Pakistan is ranked 138 out of 180 countries monitored in Transparency International's 2007 Corruption Perception Index.

Although the Government of Pakistan has adopted a long-awaited AML ordinance by presidential decree after years of delay and stall tactics, the GOP needs to amend the current AML Ordinance or pass additional legislation to remedy the number of deficiencies which exist, ensure that the legal provisions are made permanent, and make it fully compliant with international standards. The Presidential Ordinance was valid for only four months and was due to expire in early January 2008. At expiry, the AML Ordinance must be "re-enacted" or ratified by the National Assembly. Pakistan's Financial Monitoring Unit (FMU) needs to be further staffed and strengthened and should be given operational autonomy rather than subject to the supervision and control of the General Committee, comprised of political ministers. The GOP should also issue implementing regulations to consolidate and de-conflict the reporting obligations of suspicious transactions contained in various laws and regulations. Since few suspicious transaction reports are filed, Pakistan should not become dependent on these reports to initiate investigations but rather law enforcement authorities should be proactive in pursuing money laundering in their field investigations. In light of the role that private charities have played in terrorist financing, Pakistan must work quickly to conduct outreach, supervise and monitor charitable organizations and activities, and close those that finance terrorism. In accordance with FATF Special Recommendation IX, Pakistan should implement and enforce cross-border currency reporting requirements and focus greater efforts in identifying and targeting illicit cash couriers. Pakistan should also become a party to the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of Terrorist Financing.

Palau

Palau is an archipelago of more than 300 islands in the Western Pacific with a population of 20,900 (approximately 5,000 of which are foreign guest workers) and per capita GDP of about U.S. $7,000 (a large percentage of which comes from international financial assistance).

Upon its independence in 1994, the Republic of Palau entered the Compact of Free Association with the United States. The U.S. dollar is the legal tender used by the country, though it is not the official currency of Palau. Palau is not a major financial center. Nor does it offer offshore financial services. There are no offshore banks, securities brokers/dealers or casinos in Palau. Palauan authorities that within the last year at least one trust company has been registered, though the scope and size of its business is unknown. Palauan authorities believe that drug trafficking, human trafficking, and prostitution are the primary sources of illegal proceeds that are laundered.

In January 2005, Palau prosecuted its first ever case under the Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 against a foreign national engaged in a large prostitution operation. The defendant was convicted on all three counts as well as a variety of other counts. Subsequently, Palau has prosecuted three more money laundering cases obtaining convictions in two of the cases. Two of

the cases involved domestic proceeds of crime, while one of the cases involved criminal conduct both within and outside of Palau.

Amid reports in late 1999 and early 2000 that offshore banks in Palau had carried out large-scale money laundering activities, a few international banks banned financial transactions with Palau. In response, Palau established a Banking Law Review Task Force that recommended financial control legislation to the Olbill Era Kelulau (OEK), the national bicameral legislature, in 2001. Following that, Palau took several steps toward addressing financial security through banking regulation and supervision and putting in place a legal framework for an anti-money laundering regime. Several pieces of legislation were enacted in June 2001.

The Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 criminalized money laundering and created a financial intelligence unit. Two years after the introduction of proposed amendments, an amended MLPCA was signed into law on December 19, 2007.

The original act did not establish requirements for the recording of cash and bearer securities transactions of U.S. $10,000 and above, and only required the reportage of suspicious transactions in excess of U.S. $10,000. The MLPCA did mandate that records be kept for five years from the date of the transaction. All such transactions (domestic and international) are required to go through a credit or financial institution licensed under the laws of the Republic of Palau. Credit and financial institutions are required to verify customers' identity and address. In addition, these institutions are required to check for information by "any legal and reasonable means" to obtain the true identity of the principal/party upon whose behalf the customer is acting. If identification cannot be confirmed, the transaction must cease immediately.

The amended MLPCA, in addition to generally tightening up the original law, now sets higher standards for record keeping, requires the recording of cash and bearer securities transactions in excess of U.S. $10,000, removes the dollar threshold on suspicious transactions and requires "alternative remittance systems" to be licensed and maintain records of all transactions in excess of U.S. $1,000. The amendment also requires currency transactions over U.S. $5,000 to be effected by wire transfer and also authorizes the Financial Institutions Commission (FIC) to conduct random compliance audits on credit or financial institutions. Palau also monitors cross border transportation of currency through a declaration form requiring travelers to declare U.S. $10,000 or more.

The MLPCA defined offenses of money laundering as: 1) conversion or transfer of property for the purpose of concealing its illegal origin; 2) concealing or disguising the illegal nature, source, location, disposition, or ownership of property; and 3) acquisition, possession, or control of property by any person who knows that the property constitutes the proceeds of crime as defined in the law. The law provides for penalties of a fine not less than U.S. $5,000, nor more than double the amount the convicted individual laundered or attempted to launder, whichever is greater, or imprisonment of not more than 10 years, or both. Corporate entities or their agents are subject to a fine double that specified for individuals. The law protects individuals who report suspicious transactions.

The Financial Institutions Act of 2001 established the Financial Institutions Commission (FIC), an independent regulatory agency, which is responsible for licensing, supervising and regulating financial institutions, defined as banks and security brokers and dealers in Palau. An amendment intended to strengthen the supervisory powers of the FIC and promote greater financial stability within Palau's banking sector passed its first reading in the Senate in January 2005. The Senate Committee on Ways and Means and Financial Matters did not report out the bill until December 2006 when it merely referred it back to the Committee for further study. This amendment still has not become law. The insurance industry is not currently regulated by the FIC. Most insurance companies in Palau are companies registered in the U.S. or the U.S. Territory of Guam.

The Free Trade Zone Act of 2003 created the Ngardmau Free Trade Zone (NFTZ). A public corporation, Ngardmau Free Trade Zone Authority, was established to oversee the development of the NFTZ. The Authority also issues licenses for businesses to operate within the free trade zone. Businesses licensed to operate within the free trade zone will not be subject to the requirements of the Foreign Investment Act and will be exempt from certain import and export taxes. No development has taken place within the area designated for the free trade zone and the NFTZ directors continue to search for developers and investors.

Currently there are seven licensed banks in Palau, the majority ownership of which is primarily foreign. The three largest retail banks—Bank of Hawaii, Bank of Guam and BankPacific are all branches of American banks. In addition there are three banks chartered in Palau (Asia Pacific Commercial Bank, First Fidelity Bank and Palau Construction Bank) and one chartered in Taiwan (First Commercial Bank.)

On November 7, 2006, the FIC closed the second largest and the only locally owned bank, Pacific Savings Bank (PSB), for illiquidity and insolvency. The Receiver and a Special Prosecutor hired specifically for the purpose of developing cases related to the failure of PSB have filed a number of civil and criminal actions against former bank managers and insiders. An additional five to ten cases are currently being prepared. Investigations and litigation, though hampered by lack of resources, continue.

With the legal framework now being made more robust, the weakest link in Palau's money laundering prevention regime is the paucity of human and fiscal resources. The operations of the government's Financial Intelligence Unit (FIU) are severely restricted by a lack of dedicated human resources and no dedicated budget. The FIU works under the Office of the Attorney General and is responsible for receiving, analyzing, and processing suspicious transaction reports, and disseminating the reports as necessary. In addition, the FIU is responsible for tracing, seizing, and freezing assets.

Another impediment to enforcement is the lack of implementing regulations to ensure compliance with the amended MLPCA. With the passage of the 2007 amendment, however, these can now be developed.

The will of the Executive branch to comply with international standards was clearly demonstrated by President Remengesau in 2003, when he vetoed a bill that would have extended the deadline for bank compliance and would have reduced the minimum capital for a bank from $500,000 to $250,000. Additionally, the President established the Anti-Money Laundering Working Group that is comprised of the Office of the President, the FIC, the Office of the Attorney General, Customs, the FIU, Immigration and the Bureau of Public Safety.

Palau has enacted several legislative mechanisms to foster international cooperation. The Mutual Assistance in Criminal Matters Act (MACA), passed in June 2001, enables authorities to cooperate with other jurisdictions in criminal enforcement actions related to money laundering and to share seized assets. The Foreign Evidence Act of 2001 provides for the admissibility in civil and criminal proceedings of certain types of evidence obtained from a foreign state pursuant to a request by the Attorney General under the MACA. Under the Compact of Free Association with the United States, a full range of law enforcement cooperation is authorized and in 2004 Palau was able to assist the Department of Justice in a money laundering investigation by securing evidence critical to the case and freezing the suspected funds. Palau has also entered into an MOU with Taiwan and the Philippines for mutual sharing of information and interagency cooperation in relation to financial crimes and money laundering.

In 2004 The President also sent the Cash Courier Act, drafted by the Palau Anti-Money Laundering Working Group, to the legislature. The bill passed the Senate in March 2006 and went to the House of Delegates, where it passed its first reading in the same month and was referred to the House

Committee on Ways and Means and Financial Matters where, like the bill intended to strengthen the FIC, it remains.

The Counter-Terrorism Act of 2007 includes provisions for the freezing of assets of entities and persons designated by the United Nations as terrorists or terrorist organizations, provisions for the regulation of nonprofit entities to prevent abuses by criminal organizations and terrorists, and provisions for criminalizing the financing of terrorism. The Counter-Terrorism Act specifically addresses Palau's obligation under UN Security Council Resolution 1373. Palau is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Under the Act, acts of terrorism that cause loss of life are punishable by a prison term of 20 years to life and a maximum fine of U.S. $1,000,000. All other acts of terrorism are punishable by a prison term of 10 years to life and a maximum fine of U.S. $1,000,000.

Donations over U.S. $5,000 to any nonprofit organization are to be recorded. The organization must maintain the record for 3 years and must provide it to the FIU upon request. Donations over U.S. $10,000 are to be reported to the Office of the Attorney General and FIU. Any suspicious donations are also to be reported to the Office of the Attorney General and FIU. Penalties for violations are: 1) a fine not to exceed U.S. $10,000; 2) a temporary ban on operations for up to 2 years; or 3) the dissolution of the organization.

The Government of Palau (GOP) has taken several steps toward enacting a legal framework by which to combat money laundering. The GOP should circulate the UNSCR 1267 Sanctions Committee Consolidated list of terrorist entities. The GOP should provide more resources to its FIU, and provide more assistance to and proactively support the work of the Pacific Savings Bank Special Prosecutor. The GOP should enact the Cash Courier Act and carefully monitor its border points of entry and exit to protect against the smuggling of bulk cash, narcotics and other contraband. The GOP should also implement all aspects of the legal reforms already in place.

Panama

Panama is a major drug-transit country, and is particularly vulnerable to money laundering because of its proximity to Colombia and other drug-producing countries. Colombian nationals are able to enter Panama without visas, facilitating the investment of drug money into Panama's economy. Panama is also an important regional financial center. Panama's economy is 77 percent service-based, 15 percent industry and 8 percent agriculture. The maritime sector, construction, tourism, and banking are among Panama's most important and fastest growing sectors. Panama has had one of the fastest growing economies in the Western Hemisphere over the last 15 years, and is estimated to have the fastest growing economy in the region during 2007, with GDP growth approaching 10 percent. The funds generated from illegal activity are susceptible of being laundered through a wide variety of methods in Panama, including the banking system, casinos, bulk cash shipments, pre-paid telephone cards, debit cards, ATM machines, insurance companies, and real estate projects and agents.

Panama's sophisticated international banking sector, Colon Free Zone (CFZ), U.S. dollar-based economy, and legalized gambling sector are utilized to facilitate potential money laundering. The CFZ is the world's second largest free zone after Hong Kong, and serves as an originating or transshipment point for some goods purchased with narcotics proceeds (mainly dollars obtained in the United States) through the Colombian Black Market Peso Exchange. The CFZ has over 2,600 business, 25 bank branches, and employs approximately 25,000 personnel. The CFZ is estimated to have imported and re-exported over U.S. $15 billion in goods during 2007. The ports of Panama handle over 4 million twenty-foot equivalent units (TEUs) of container traffic per year. The CFZ has limited resources to conduct supervisory programs and monitor for illegal activities, with a legal staff of approximately five people who, among other things, oversee efforts to detect money laundering, transshipment, goods smuggling, counterfeit products and intellectual property rights violations.

Panama is one of the world's largest offshore financial centers. Panama's offshore financial sector includes international business companies, offshore banks, captive insurance companies and fiduciary companies. Approximately 34,800 new offshore corporations were registered in Panama in 2007, as of October 2007. As of June 2007, Panamas had 85 commercial banks: 2 official banks, 14 local banks of general license, 26 foreign banks of general license, 34 banks of international license, and nine representative offices. Shell companies are permitted and have been used by a wide range of criminal groups around the world. Bearer shares are permitted for corporations and nominee directors and trustees as are allowed by law. The Government of Panama (GOP) regulates casinos, but does not regulate Internet gaming sites.

Law No. 42 of 2000 requires Panamanian trust companies to identify to the Superintendence of Banks the real and ultimate beneficial owners of trusts. Executive Decree 213 of 2000, amending Executive Order 16 of 1984, provides for the dissemination of information related to trusts to appropriate administrative and judicial authorities. Both the onshore and offshore financial entities are subject to similar regulation by the Superintendence of Banks. The onshore and offshore registration of corporations is also handled by the Public Registry. There are no differing regulations governing onshore and offshore corporations. The application process for a banking license in favor of a bank to be constituted in Panama and a banking license in favor of a foreign bank are substantially the same.

Panama's construction sector, which is growing at double-digit rates, is also susceptible to money laundering activities. In Panama City alone, there is either in process or approved the construction of over 150 buildings of twenty stories or greater. It is estimated that approximately 20,000 high-end condominium units will enter the Panamanian real estate market within the next five years. The bulk of these units are for purchase by foreigners. The developer of one residential project (Resort Paraiso Las Perlas on Isla Chapera in the Gulf of Panama), Jose Nelson Urrego Cardenas, was arrested in 2007 on drug money laundering charges.

Money laundering is a criminal offense in Panama under Law No. 41 of October 2000. Law 41 amends the Penal Code by expanding the predicate offenses for money laundering beyond narcotics trafficking to include criminal fraud, arms trafficking, trafficking in humans, kidnapping, extortion, embezzlement, corruption of public officials, terrorism and international theft or trafficking of motor vehicles. Law No. 1 of 2004 also adds crimes against intellectual property as a predicate offense for money laundering. In May 2007, Law No. 14 was adopted, establishing terrorist financing as a predicate offense for money laundering. Law 41 establishes a 5 to 12 year prison sentence, plus possible fines. Law No. 45 of 2003 also establishes criminal penalties of up to ten years in prison and fines of up to one million dollars for financial crimes that undermine public trust in the banking system, the financial services sector, or the stock market. This law criminalizes a wide range of activities related to financial intermediation, including the following: illicit transfers of monies, accounting fraud, insider trading, and the submission of fraudulent data to supervisory authorities.

Law No. 42 of 2000 requires financial institutions (banks, trust companies, money exchangers, credit unions, savings and loans associations, stock exchanges and brokerage firms, and investment administrators) to report currency transactions in excess of U.S. $10,000 and suspicious financial transactions to Panama's financial intelligence unit, the Unidad de Análisis Financiero (UAF). Law 42 also mandates casinos, CFZ businesses, the national lottery, real estate agencies and developers, and insurance and reinsurance companies report to the UAF currency transactions that exceed U.S. $10,000. Furthermore, Law 42 requires Panamanian trust companies to identify to the Superintendent of Banks the beneficial owners of trusts. Additionally, Law 16 of 2005, which regulates the activities of pawnshops, requires such enterprises to report suspicious transactions to the UAF. Financial institutions are prohibited from informing their client or third parties that they have transmitted any information regarding such transactions to the UAF. Law 42 protects reporting entities from civil and criminal suits with respect to providing the information required by the law and otherwise cooperating with law enforcement entities.

The Superintendent of Banks is responsible for supervising both onshore and offshore financial institutions with regard to their anti-money laundering and counter-terrorist financing (AML/CTF) requirements. In 2000, Panama's Superintendence of Banks issued Agreement No. 9 of 2000 that defines requirements that banks must follow for identification of customers, exercise of due diligence, and retention of transaction records and increased the number of finance company inspections. In 2005, the Superintendence of Banks modified that Agreement, to include fiduciary companies within the prevention measures and to bring the banking center into line with international standards and Financial Action Task Force (FATF) recommendations. Financial institutions must have sufficient information to adequately identify their customers. They must examine every cash (or cash equivalent) transaction in excess of $10,000 or a series of transactions that in the aggregate exceed U.S. $10,000 in any given week. Additionally, they must examine with special attention, any transaction, regardless of amount, which could be related to money laundering activity. Financial institutions must also establish procedures and mechanisms for internal controls to prevent money laundering related activities. Financial institutions must also insure that their employees are aware of these laws and regulations.

A number of other supervisory bodies have regulatory responsibility for AML/CTF compliance purposes. The Ministry of Commerce and Industry is responsible for supervising money remittance houses, financing companies, real estate promoters and agents, pawnshops, and companies located in enterprise processing zones. The Panamanian Autonomous Cooperative Institute supervises savings and loan cooperatives, and has established a specialized unit for the supervision of loans and credit cooperatives regarding compliance with Law 42. The National Securities Commission supervises securities firms, stockbrokers, stock exchanges and investment managers, and carries out various training sessions and workshops for its personnel and related entities. The Gaming Commission supervises casinos and other establishments dedicated to betting and games of chance. The Colon Free Zone Authority supervises the companies and activity within the CFZ, and has issued a procedures manual for all CFZ businesses, outlining their responsibilities regarding the prevention of money laundering and the requirements of Law 42. The Superintendence of Insurance supervises insurance companies, reinsurance companies, and insurance brokers.

Executive Decree No. 136 of 1995 establishes the UAF. The UAF falls under the jurisdiction of the GOP's Council for Security and National Defense within the Ministry of the Presidency. The UAF currently has approximately 25 employees. During 2007, the UAF reinforced the analysis department by hiring two new accountants, a financial analyst, and a lawyer. Also, the statistics and typology departments have newly trained personnel. Despite these additions, the UAF is overworked and understaffed, lacks adequate resources, and suffered the loss of experienced personnel in 2007.

The UAF works with other GOP agencies to identify new methods of money laundering and terrorist financing, and participates in the training of financial and nonfinancial sector employees in detecting and preventing money laundering and terrorist financing. During the first six months of 2007, the UAF trained 1,476 individuals, 59 percent of which were banking employees, 29 percent of which were government employees, and 12 percent of which were financial service employees.

The UAF has access to the records or databases of other government entities that have public websites or public investigative offices. The UAF has online access with other GOP entities to access information from the public registry, traffic department, electoral tribunal, as well as information on immigration movements and travelers' declarations of the cross-border transportation of currency. The UAF may also request additional information from financial institutions in writing.

Once the UAF has reviewed all cash transaction reports (CTRs) or suspicious transaction reports (STRs) and gathered any other relevant information from reporting institutions and other government agencies, the UAF provides information related to possible money laundering or terrorist financing to the Office of the Attorney General for investigation. Money laundering cases involving narcotics are

handled by the Drug Prosecutor's Office within the Office of the Attorney General. The Judicial Technical Police (Sección de Investigaciones Financieras, or SIF, similar in function to the Federal Bureau of Investigation) provides expert assistance to the prosecutors. The UAF routinely transfers cases to the financial investigations unit of the SIF for investigation.

As of November, the UAF received 1,012 STRs in 2007, of which 170 were sent to the Attorney General's Office for further action. During all of 2006, the UAF investigated 935 suspicious transaction reports (843 from banks), of which 158 were sent to the Attorney General's Office. During the second quarter of 2007, the UAF received 63,752 CTRs, a 3.8 percent increase from the same period in 2006. The total amount reported via CTRs during the first six months of 2007 was $2.7 billion, a 46.9 percent increase from the same period in 2006. Approximately 91 percent of the reports came from banks, and 4.5 percent from exchange houses. The UAF attributes the increase in CTRs to the growth in the Panamanian economy. As of October, the Drug Prosecutor's Office reported 43 drug-related money laundering arrests in 2007.

Under Panamanian customs regulations, any individual bringing cash in excess of $10,000 into Panama must declare such monies at the point of entry. If such monies are not declared, they are confiscated and are presumed to relate to money laundering. Some GOP officials have expressed concern at the millions of dollars in cash they have seen brought into Panama from Colombia. The actual movement/transfer of this cash is legal insofar that it was declared to both Colombian and Panamanian customs. However, the GOP maintains that it cannot vouch for the legitimate origins of said cash. All instances of cash smuggling are required to be reported into a database maintained by Panamanian customs.

On August 10, 2007, Law 38 entered into force. Law 38 provides for the seizure of assets derived from criminal activity. Upon an arrest, assets are frozen and seized. The assets are released upon a judge's order to the defendant in the event of a dismissal of charges or acquittal. In the event of a conviction, assets derived from money laundering activity related to narcotics trafficking are delivered to the National Commission for the Study and Prevention of Narcotics Related Crimes (CONAPRED) for administration and distribution among various GOP agencies. Seized perishable assets may be sold and the proceeds deposited in a custodial account with the National Bank. Responsibility for tracing, seizing and freezing assets lies principally with the Drug Prosecutor's Office of the Attorney General's Office. The GOP has not enacted legislation allowing for civil forfeiture or the sharing of seized assets with other governments.

Law 50 of 2003 criminalizes the financing of terrorism. Under Law 14 of May 2007, terrorist financing and terrorist acts, among other offenses, are now predicate offenses for money laundering. Panama circulates to its financial institutions the list of individuals and entities included on the United Nations Security Council Resolution 1267 Sanctions Committee list. The Ministry of Foreign Relations sends the UAF and the Superintendence of Banks a copy of a diplomatic note or letter with the names of terrorist organizations or financiers designated by the U.S. Government or the UN. The UAF in turn sends it to the appropriate regulators, who in turn send it to the regulated entities. The GOP does not have an independent national system or mechanism for freezing terrorist assets.

Executive Decree 524 of 2005, as amended by Executive Decree 627 of 2006, establishes procedures to regulate, supervise, and control nongovernmental organizations and charities, including regulatory procedures to combat terrorism and prevent terrorist financing. Press reports, however, have questioned the degree to which the nongovernmental organizations are complying with their reporting and registration requirements.

Decree No. 22 of June 2003, gave the Presidential High Level Commission against Narcotics Related Money Laundering responsibility for combating terrorist financing. The Panama Public Force (PPF) and the judicial system have limited resources to deter terrorists, due to insufficient personnel and lack of expertise in handling complex international investigations. The GOP has a border security

cooperation agreement with Colombia, and has also increased funds to the PPF to help secure the frontier. The GOP also created within the Ministry of Foreign Affairs the Department of Analysis and Study of Terrorist Activities. This department is tasked with working with the United Nations and the Organization of American States to investigate transnational issues, including money laundering. Panama has an implementation plan for compliance with the FATF Forty Recommendations on Money Laundering and its Nine Special Recommendations on Terrorist Financing.

Panama and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. The GOP has also assisted numerous countries needing help in strengthening their anti-money laundering programs, including Guatemala, Costa Rica, Russia, Honduras, and Nicaragua. Executive Decree No. 163 authorizes the UAF to share information with FIUs of other countries, subject to entering into a memorandum of understanding or other information exchange agreement. The UAF has signed more than 43 memoranda of understanding with foreign FIUs, including the Financial Crimes Enforcement Network (FinCEN), the U.S. FIU.

Panama is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD), and the Caribbean Financial Action Task Force. Panama is also a member of the Offshore Group of Banking Supervisors, and the UAF is a member of the Egmont Group. Panama is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the Inter-American Convention against Terrorism.

The Government of Panama has a comprehensive legal framework to detect, prevent, and combat money laundering and terrorist financing, and cooperates with the United States and other countries with criminal investigations of drug trafficking, money laundering, and financial crimes. Panama nonetheless remains vulnerable to money laundering owing to its lack of adequate enforcement, personnel and resources, the sheer volume of economic transactions, its location as a major drug transit country, and corruption. The GOP should consider adopting legislation that allows for civil forfeiture and the freezing of terrorist assets, and enhance law enforcement efforts to address such vulnerabilities as smuggling, abuse of the real estate sector, trade-based money laundering, and the proliferation of nontransparent offshore companies. The GOP should also ensure that the UAF and other law enforcement and regulatory entities have sufficient personnel and resources.

Paraguay

Paraguay is a principal money laundering center involving the banking and nonbanking financial sectors. The multi-billion dollar contraband trade that occurs on the borders shared with Argentina and Brazil, the Tri-Border Area, facilitates much of the money laundering in Paraguay. Paraguay is a major drug-transit country. The Government of Paraguay (GOP) suspects proceeds from narcotics trafficking are often laundered, but it is difficult to determine the percentage of the total amount of laundered funds generated from narcotics sales. Weak controls in the financial sector, open borders, and minimal enforcement activity for financial crimes allow money launderers and terrorist financiers to take advantage of Paraguay's financial system.

Ciudad del Este (CDE), on Paraguay's border with Brazil and Argentina, represents the heart of Paraguay's informal economy. The area is well known for arms and narcotics trafficking and violations of intellectual property rights. The illicit proceeds from these crimes are an additional source of laundered funds. A wide variety of counterfeit goods, including cigarettes, CDs, DVDs, computer software, and games, are imported from Asia and transported across the border into Brazil, with a smaller amount remaining in Paraguay for sale in the local economy. Some senior government officials, including members of Congress, have been accused of involvement in the smuggling of contraband or pirated goods. To date, there have been few criminal investigations, much less prosecutions, of senior GOP officials involved in smuggling contraband or pirated goods.

Paraguay is particularly vulnerable to money laundering, as little personal background information is required to open a bank account or to conduct financial transactions. Paraguay is an attractive financial center for neighboring countries, particularly Brazil. Foreign banks are registered in Paraguay and nonresidents are allowed to hold bank accounts, but current regulations forbid banks from advertising or seeking deposits from outside the country. Offshore banking in Paraguay is illegal. While casinos exist, offshore casinos do not, and Internet gambling is marginal, largely due to limited Internet connectivity throughout the country. Shell companies and trust funds structures are legal but are seldom used and uncommon in the financial system. At present, the financial sector seems to lack the depth and sophistication to use these structures. The nonbank financial sector operates in a weak regulatory environment with limited supervision. Credit unions or "cooperatives" are one of the main nonbank agents in the economy, rapidly growing in membership and representing over 20 percent of deposits and 33 percent of loans in the financial system. The organization responsible for regulating and supervising credit unions, the National Institute of Cooperatives (INCOOP), is an independent body that provides regulatory and supervisory guidelines, but lacks the capacity to enforce compliance. Exchange houses are another nonbank sector where enforcement of compliance requirements remains limited.

On December 20, 2007, Paraguay's Congress approved a new penal code that includes enhanced legislation on money laundering. In January 2008, the President of Paraguay signed the law and it entered into force. Under the new penal code, money laundering is an autonomous crime, punishable by a prison term of up to five years. The new code establishes predicate offenses for money laundering, but does not require a conviction for the predicate offense before initiating money laundering charges. The law also allows the state to charge financial sector officials who negligently permit money laundering to occur. Under Paraguayan law, the implementation of the new penal code will be delayed for one year to allow for the training of judges and prosecutors.

Another bill amending Paraguay's criminal procedure code is expected in early 2008, and terrorist finance legislation is also expected as a separate bill in 2008, after efforts to include it in the proposed penal code reforms failed in 2007. The proposed amendments to the criminal procedure code would move Paraguay towards a more accusatory system. The reforms would allow criminal investigations to occur without advance notice of the investigation to the subject or the defense attorney, it would lengthen statutes of limitation, and it would allow for confrontation and cross examination of witnesses.

There are other challenges, however, that the proposed money laundering legislation will not address, including limited resources and training. Paraguay added three financial crimes prosecutors in 2007, bringing the total number to 11, but prosecutors still face resource constraints that limit their ability to investigate and prosecute money laundering and financial crimes. New criteria were issued in 2005 for the selection of judges, prosecutors and public defenders; however, the process remains one that is largely based on politics, nepotism and influence peddling, affording the ruling party an opportunity to manipulate the judicial system to its advantage. Now that the new anti-money laundering legislation has been passed as part of the new penal code, training for judges and prosecutors is key to Paraguay's future prosecutorial successes.

There are no effective controls or laws that regulate the amount of currency that can be brought into or out of Paraguay. Cross-border reporting requirements are limited to those forms issued by airlines at the time of entry into Paraguay. Persons transporting U.S. $10,000 into or out of Paraguay are required to file a customs report, but these reports are not collected or checked. Customs operations at the airports or land ports of entry provide no control of cross-border cash movements. The nonbank financial sector (particularly exchange houses) is used to move illegal proceeds both from within and outside of Paraguay into the U.S. banking system. Paraguay exercises a dual monetary system in which most high-priced goods are paid for in U.S. dollars. Large sums of dollars generated from normal commercial activity and suspected illicit commercial activity are transported physically from

Paraguay through Uruguay to banking centers in the United States. The GOP is only beginning to recognize and address the problem of the international transportation of currency and monetary instruments derived from illegal sources.

Bank secrecy laws in Paraguay do not prevent banks and financial institutions from disclosing information to bank supervisors and law enforcement entities. Bankers and others are protected under the anti-money laundering law with respect to their cooperation with law enforcement agencies. Banks, finance companies, insurance companies, exchange houses, stock exchanges and securities dealers, investment companies, trust companies, mutual and pension funds administrators, credit and consumer cooperatives, gaming entities, real estate brokers, nongovernmental organizations, pawn shops, and dealers in precious stones, metals, art, and antiques are required to know and record the identity of customers engaging in significant currency transactions. These entities must also report suspicious activities to Paraguay's financial intelligence unit (FIU), the Unidad de Análisis Financiera (UAF) within the Secretariat to Combat Money Laundering (SEPRELAD) of the Ministry of Industry and Commerce (MIC). The Superintendence of Banks enforces these reporting obligations for banks, but they are not enforced for other financial institutions. In November 2007, the MIC issued new regulations that define reporting requirements and sanctions for noncompliance for the insurance industry and credit unions.

In recent years, the GOP has made significant efforts to strengthen SEPRELAD, but weak leadership and suspicious activity caused SEPRELAD to falter in the first half of 2007, resulting in a halt in information sharing and the departure of several analysts. The GOP dismissed SEPRELAD's director and appointed a new director, former Central Bank president Gabriel Gonzalez, in August 2007. SEPRELAD received over 3,600 suspicious activity reports (SARs) in 2007, but its former director left a backlog of over 3,000 SARs not entered into its system. Director Gonzalez has now updated the system by entering the entire backlog of SARs. He has hired new analysts, who have been vetted and are being trained. SEPRELAD has drafted a bill, not yet pending before Congress, which would make it an independent secretariat reporting directly to the president. SEPRELAD is also hampered by a lack of effective inter-agency cooperation, as there is no formal mechanism for sharing sensitive information. Director Gonzalez is working on creating information sharing mechanisms within the Paraguayan government law enforcement agencies.

SEPRELAD is seeking to strengthen its relationship with other financial intelligence units and has signed agreements for information exchange with regional FIUs. However, its relationship with international and regional anti-money laundering groups, including the Egmont Group and the Financial Action Task Force for South America (GAFISUD), is tenuous. As a result of the GOP's failure to pay any of its dues dating back to 2002 (totaling approximately U.S. $76,000), GAFISUD placed sanctions on Paraguay in July and suspended its membership on December 1. However, the GOP made a partial payment of its dues after the December 1 deadline, and GAFISUD agreed to reinstate its membership on the condition that the remainder of its arrears will be paid by July 2008. Likewise, while SEPRELAD has been a member of the Egmont Group since 1998, it may be suspended from the Egmont Group in May 2008 if the GOP fails to approve terrorist financing legislation.

Paraguay has taken some measures to tackle illicit commerce and trade in the informal economy and to develop strategies to implement a formal, diversified economy. Transparency International Corruption Perceptions Index ranks Paraguay at number 138 of the 180 countries ranked. The GOP has signed an agreement with the Millennium Challenge Corporation for a $34.9 million Threshold Program to address corruption problems of impunity and informality, both of which hamper law enforcement efforts and contribute to money laundering. Paraguay's Threshold Program also supports the continued development of the "maquila" sector, which comprises businesses operating for export (of either goods or services) that enjoy special tax advantages. The MIC's Specialized Technical Unit (UTE), working in close coordination with the Attorney General's Trademarks and Intellectual

Property Unit, seized U.S. $51 million worth of pirated goods during the first ten months of 2007. The Attorney General's Trademarks and Intellectual Property Unit initiated criminal proceedings in 110 cases, but most offenders paid a fine instead of serving jail time. In cooperation with the U.S. Department of Homeland Security's Agency of Immigration and Customs Enforcement (ICE), the GOP established a Trade Transparency Unit (TTU) that examines discrepancies in trade data that could be indicative of customs or tax fraud, trade-based money laundering, or the financing of terrorism. ICE estimates that U.S. $20 million left Paraguay for the U.S. on a daily basis in 2006, but less than U.S. $1 million was reported coming in.

Under its current laws, the GOP has limited authority to seize or forfeit assets of suspected money launderers. In most cases, assets that the GOP is permitted to seize or forfeit are limited to transport vehicles, such as planes and cars, and normally do not include bank accounts. However, authorities may not auction off these assets until a defendant is convicted. At best, the GOP can establish a "preventative seizure" (which has the same effect as freezing) against assets of persons under investigation for a crime in which the state risks loss of revenue from furtherance of a criminal act, such as tax evasion. However, in those cases the limit of the seizure is set as the amount of the suspect's liability to the government. In the past few years, the anti-narcotics agency, SENAD, has been permitted on a temporary basis to use assets seized in pending cases, but SENAD cannot fully use such assets because the law does not permit the assets to be maintained or repaired. New asset forfeiture legislation is required to make improvements in this regard.

The GOP has no authority to freeze, seize, or forfeit assets related to the financing of terrorism, which is not a criminal offense under Paraguayan law. However, the Ministry of Foreign Affairs often provides the Central Bank and other government entities with the names of suspected terrorists on the UNSCR 1267 Sanctions Committee list. To date, the GOP has not identified, seized, or forfeited any assets linked to these groups or individuals. The current law also does not provide any measures for thwarting the misuse of charitable or nonprofit entities that can be used as conduits for the financing of terrorism.

The GOP has been slow to recognize terrorist financing within its borders. In December 2006, the U.S. Department of Treasury designated nine individuals and two companies operating in the Tri-Border Area as entities that provide financial and logistical support to Hezbollah. The nine individuals have all provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was designated by the U.S. Treasury in June 2004 for his support to Hizballah leadership. Two companies, Galeria Page and Casa Hamze, are located in Ciudad del Este and are used to generate or move terrorist funds. The GOP publicly disagreed with the designations, stating that the U.S. has not provided any new information that would prove terrorist financing activity occurs in the Tri-Border Area.

In spite of limitations in prosecuting suspected terrorist financiers such as Assad Ahmad Barakat and Kassem Hijazi, who were charged with tax evasion rather than terrorist financing or money laundering, the GOP is making improvements in its ability to successfully investigate and prosecute some money laundering cases. Leoncio Mareco was sentenced to 20 years in prison on August 14, 2007, for drug trafficking and money laundering. His wife, Zulma Rios de Mareco, was sentenced to 10 years in prison for money laundering. According to GOP authorities, the General Attorney's office has eight other active cases pending. These cases reinforce the fact that convictions are possible, although difficult, under the current legal framework.

The GOP is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the Inter-American Convention on Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. Paraguay participates in the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group, and is a member of the "3

Plus 1" Security Group between the United States and the Tri-Border Area countries. The GOP is a member of GAFISUD, and SEPRELAD is a member of the Egmont Group.

The Government of Paraguay took a number of positive steps in 2007 to combat money laundering, particularly with the passage of the new penal code and the GOP's money laundering convictions. However, it should continue to pursue other initiatives to increase its effectiveness in combating money laundering and terrorist financing. Most important is enactment of legislation that meets international standards and enables law enforcement authorities to more effectively investigate and prosecute money laundering and terrorist financing cases. The GOP should take steps to ensure that the penal and procedural code reforms are approved and implemented, allowing for a more effective anti-money laundering regime. Paraguay does not have a counterterrorism law or a law criminalizing terrorist financing, and the GOP should take steps as quickly as possible to ensure that comprehensive counterterrorism and counter-terrorist financing legislation is introduced again and adopted. Paraguay also should continue its efforts to combat corruption and increase information sharing among concerned agencies .It should also take the necessary steps to ensure that its Trade Transparency Unit is comprised of vetted employees from all relevant agencies, including SEPRELAD. Further reforms in the selection of judges, prosecutors and public defenders are needed, as well as reforms to the customs agency to allow for increased inspections and interdictions at ports of entry and to develop strategies targeting the physical movement of bulk cash. The GOP should also ensure that its GAFISUD dues are paid, preventing suspension of its membership. It is essential that SEPRELAD continues to receive the financial and human resources necessary to operate as an effective, fully functioning financial intelligence unit capable of combating money laundering, terrorist financing, and other financial crimes.

Peru

Peru is not a major regional financial center, nor is it an offshore financial center. Peru is a major drug producing and drug-transit country. Narcotics-related and other money laundering does occur, and the Government of Peru (GOP) has taken several steps to improve its money laundering legislation and enforcement abilities in recent years. Nevertheless, more reliable and adequate mechanisms are necessary to better assess the scale and methodology of money laundering in Peru. Peru is the world's second largest producer of cocaine. Although no reliable figures exist regarding the exact size of the narcotics market in Peru, estimates indicate that the cocaine trade generates in a range of one to two billion dollars annually, or up to 2.5 percent of Peru's GDP. As a result, money laundering is believed to occur on a significant scale to integrate these illegal proceeds into the Peruvian economy.

Money laundering has historically been facilitated by a number of factors, primarily Peru's cash-based economy. Peru's economy is heavily dependent upon the U.S. dollar. Approximately 60 percent of the economy is informal and approximately 65 percent is dollarized, allowing traffickers to handle large bulk shipments of U.S. currency with minimal complications. Currently no restrictions exist on the amount of foreign currency an individual can exchange or hold in a personal account, and until recently, there were no controls on bulk cash shipments coming into Peru. There have not been any official studies to establish an approximate percentage of the relationship between money laundering and drug trafficking. However, reports sent from Peru's financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), to the Public Ministry (Attorney General's office) indicate that approximately 45 percent of the money laundering cases have connections to criminal activity stemming from the drug trade.

Corruption remains an issue of serious concern in Peru. It is estimated that 15 percent of the public budget is lost due to corruption. A number of former government officials, most from the Fujimori administration, are under investigation for corruption-related crimes, including money laundering. These officials have been accused of transferring tens of millions of dollars in proceeds from illicit

activities (e.g., bribes, kickbacks, or protection money) into offshore accounts in the Cayman Islands, the United States, and/or Switzerland. The Peruvian Attorney General, a Special Prosecutor, the office of the Superintendent of Banks and Insurance, and the Peruvian Congress have conducted numerous investigations, some of which are ongoing, involving dozens of former GOP officials.

Law 27.765 of 2002 criminalizes money laundering in Peru. Prior to its passage, money laundering was only a crime when directly linked to narcotics trafficking, "narcoterrorism," and nine specific predicate offenses that did not include corruption, bribery, or fraud. Law 27.765 expands the predicate offenses for money laundering to include the laundering of assets related to all serious crimes, such as narcotics trafficking, terrorism, corruption, trafficking of persons, and kidnapping. However, there remains confusion on the part of some GOP officials and prosecutors as to whether money laundering must still be linked to the earlier list of predicate offenses. The law's brevity and lack of implementing regulations are also likely to limit its effectiveness in obtaining convictions. However, reportedly, money laundering is an autonomous offense. There does not have to be a conviction relating to the predicate offense. Rather it must only be established that the predicate offense occurred and that the proceeds of crime from that offense were laundered.

Law 27.765 also revises the penalties for money laundering in Peru. Instead of a life sentence for the crime of laundering money, Law 27.765 sets prison terms of up to 15 years for convicted launderers, with a minimum sentence of 25 years for cases linked to narcotics trafficking, terrorism, and laundering through banks or financial institutions. In addition, revisions to the Penal Code criminalize "willful blindness," the failure to report money laundering conducted through one's financial institution when one has knowledge of the money's illegal source, and imposes a three to six year sentence for failure to file suspicious transaction reports.

The UIF began operations in June 2003 and today has approximately 48 personnel. In June 2007, the UIF was incorporated into the Office of the Superintendent of Banks and Insurance and a new director was appointed. As Peru's financial intelligence unit, the UIF is the government entity responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs) filed by obligated entities. The entities obligated to report suspicious transactions to the UIF within 30 days include banks, financial institutions, insurance companies, stock funds and brokers, the stock and commodities exchanges, credit and debit card companies, money exchange houses, mail and courier services, travel and tourism agencies, hotels and restaurants, notaries, the customs agency, casinos, auto dealers, construction or real estate firms, notary publics, and dealers in precious stones and metals. The UIF cannot receive STRs electronically; obligated entities must hand-deliver STRs to the UIF. The UIF received 1,179 STRs in 2006, and 1,007 from January through September 2007.

Obligated entities must also maintain reports on large cash transactions. Individual cash transactions exceeding U.S. $10,000 or transactions totaling U.S. $50,000 in one month must be maintained in internal databases for a minimum of five years and made available to the UIF upon request. Nonfinancial institutions, such as exchange houses, casinos, lotteries or others, must report individual transactions over U.S. $2,500 or monthly transactions over U.S. $10,000. Individuals or entities transporting more than U.S. $10,000 in currency or monetary instruments into or out of Peru must file reports with the customs agency, and the UIF may have access to those reports upon request. Any cash transactions that appear suspicious must be reported to the UIF. These reporting requirements are not being strictly enforced by the responsible GOP entities. However, the UIF is able to sanction persons and entities for failure to report suspicious transactions, large cash transactions, or the transportation of currency or monetary instruments.

The UIF does not automatically receive cash transactions reports (CTRs) or reports on the international transportation of currency or monetary instruments. CTRs are maintained in internal registries within the obligated entities, and reports on the international transportation of currency or monetary instruments are maintained by the customs agency. If the UIF receives an STR and

determines that the STR warrants further analysis, it contacts the covered entity that filed the report for additional background information-including any CTRs that may have been filed-and/or the customs agency to determine if the subject of the STR had reported the transportation of currency or monetary instruments. Some requests for reports of transactions over U.S. $10,000—such as those that are deposits into savings accounts—are protected under the constitution by bank secrecy provisions and require an order from the Public Ministry or SUNAT, the tax authority. A period of 15-30 days is required to lift the bank secrecy restrictions. All other types of cash transaction reports, however, may be requested directly from the reporting institution.

Law 28.306 of 2004 mandates that obligated entities also report suspicious transactions related to terrorist financing, and expanded the UIF's functions to include the ability to analyze reports related to terrorist financing. In July 2006, the GOP issued Supreme Decree 018-2006-JUS to better implement Law 28.306. The decree also introduces the specific legal framework for the supervision of obligated entities with regard to combating terrorist financing.

Law 28.306 establishes regulatory responsibilities for the UIF. Most obligated entities fall under the supervision of the Superintendence of Banks and Insurance (banks, the insurance sector, financial institutions), the Peruvian Securities and Exchange Commission (securities, bonds), and the Ministry of Tourism (casinos). All entities that are not supervised by these three regulatory bodies, such as auto dealers, construction and real estate firms, etc., fall under the supervision of the UIF. Under Supreme Decree 018-2006-JUS, the UIF may participate in the on-site inspections of obligated entities performed by the supervisory body. The UIF may also conduct the on-site inspections of the obligated entities that do not fall under the supervision of another regulatory body, such as notaries, money exchange houses, etc. The UIF can also request that a supervisor review an obligated entity that is not under its supervision. Supreme Decree 018-2006-JUS contains instructions for supervisors with prior UIF approval to establish which obligated entities must have a full-time compliance official (depending on each entity's size, patrimony, etc.), and allows supervisors to exclude entities with certain characteristics from maintaining currency transaction reports.

In spite of the expanded regulatory responsibilities of the UIF, some obligated entities remain unsupervised. For instance, the Superintendence of Banks only regulates money remittances that are done through special fund-transfer businesses (ETFs) that do more than 680,000 soles (about U.S. $200,000) in transfers per year, and remittances conducted through postal or courier services are supervised by the Ministry of Transportation and Communications. As a result, informal remittance businesses, including travel agencies and small wire transfer businesses, are not supervised. There is also difficulty in regulating casinos, as roughly 60 percent of that sector is informal. An assessment of the gaming industry conducted by GOP and U.S. officials in 2004 identified alarming deficiencies in oversight and described an industry that is vulnerable to being used to launder large volumes of cash. Approximately 580 slot houses operate in Peru, with less than 65 percent or so paying taxes. Estimates indicate that less than 42 percent of the actual income earned is being reported. This billion-dollar cash industry continues to operate with little supervision.

To assist with its analytical functions, the UIF may request information from such government entities as the National Superintendence for Tax Administration, Customs, the Securities and Exchange Commission, the Public Records Office, the Public or Private Risk Information Centers, and the National Identification Registry and Vital Statistics Office, among others. However, the UIF can only share information with other agencies—including foreign entities—if there is a joint investigation underway. The UIF disseminates STRs and other reports that require further investigation or prosecution to the Public Ministry.

Within the counternarcotics section of the Public Ministry, two specialized prosecutors are responsible for dealing with money laundering cases. As of September, the UIF had sent 6 suspected cases of

money laundering stemming from STRs to the Public Ministry for investigation in 2007. To date, there has not been a money laundering conviction in Peru.

In addition to being able to request any additional information from the UIF in their investigations, the Public Ministry may also request the assistance of the Directorate of Counter-Narcotics (DINANDRO) of the Peruvian National Police. Under Law 28.306, DINANDRO and the UIF may collaborate on investigations, although each agency must go through the Public Ministry to do so. DINANDRO may provide the UIF with intelligence for the cases the UIF is analyzing, while it provides the Public Ministry with assistance on cases that have been sent to the Public Ministry by the UIF.

The Financial Investigative Office of DINANDRO has seized numerous properties over the last several years, but few were turned over to the police to support counternarcotics efforts. While Peruvian law does provide for asset forfeiture in money laundering cases, and these funds can be used in part to finance the UIF, no clear mechanism exists to distribute seized assets among government agencies. The Garcia Administration included an asset forfeiture law in a package of organized crime legislation presented to the Peruvian Congress in July 2007. The law went into force in November 2007.

Legislative Decree No. 992, published on July 22, 2007, established the procedure for loss of dominion, which refers to the extinction of the rights and/or titles of assets derived from illicit sources, in favor of the GOP, without any compensation of any nature. Likewise, through Legislative Decree No, 635, the penal code was modified to provide more comprehensively for seizure of assets, money, earnings, or other products or proceeds of crime.

Terrorism is considered a particular and long-standing problem in Peru, which is home to the terrorist organization Shining Path. Although the Shining Path has been designated by the United States as a foreign terrorist organization pursuant to Section 219 of the Immigration and Nationality Act and under Executive Order (E.O.) 13224, and the United States and 100 other countries have issued freezing orders against its assets, the GOP has no legal authority to quickly and administratively seize or freeze terrorist assets. In the event that such assets are identified, the Superintendent for Banks must petition a judge to seize or freeze them and a final judicial decision is then needed to dispose of or use such assets. Peru also has not yet taken any known actions to thwart the misuse of charitable or nonprofit entities that can be used as conduits for the financing of terrorism. Nongovernmental organizations are obliged to report the origins of their funds, according to UIF regulations.

Peru is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the Inter-American Convention against Terrorism. However, terrorism has not yet been specifically and correctly established as a crime under Peruvian legislation as mandated by the UN Convention. The only reference to terrorism as a crime is in Executive Order 25.475, which establishes the punishment of any form of collaboration with terrorism, including economic collaboration. There are several bills pending in the Peruvian Congress concerning the correct definition of the crime of terrorist financing.

Peru is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GOP participates in the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group. Peru is a member of the Financial Action Task Force for South America (GAFISUD) and is scheduled to undergo its third GAFISUD mutual evaluation in April 2008. The UIF is a member of the Egmont Group of financial intelligence units. Although an extradition treaty between the U.S. Government and the GOP entered into force in 2003, there is no mutual legal assistance treaty or agreement between the two countries.

The Government of Peru has made advances in strengthening its anti-money laundering and counter-terrorist financing regime in recent years. However, some progress is still required to better comply

with international standards. Although there is an Executive Order criminalizing terrorist financing, Peru should pass legislation that criminalizes terrorist financing. The GOP should also enact legislation that allows for administrative as well as judicial blocking of terrorist assets. There are still a number of weaknesses in Peru's anti-money laundering system: bank secrecy must be lifted to allow the UIF to have access to certain cash transaction reports, smaller financial institutions are not regulated, and the UIF is not able to work directly with law enforcement agencies. There are a number of bills under review in the Peruvian Congress that would lift bank secrecy provisions for the UIF in matters pertaining to money laundering and terrorist financing and the GOP should ensure their expedient passage. Anti-corruption efforts in Peru should be a priority. The GOP should address these issues to strengthen its ability to combat money laundering and terrorist financing.

Philippines

Although the Philippines is not a regional financial center, the illegal drug trade in the Philippines has evolved into a billion dollar industry. The Philippines continues to experience an increase in foreign organized criminal activity from China, Hong Kong, and Taiwan. Insurgency groups operating in the Philippines partially fund their activities through local crime, the trafficking of narcotics and arms, and engage in money laundering through ties to organized crime. The proceeds of corrupt activities by government officials are also a source of laundered funds. Smuggling continues to be a major problem. The Federation of Philippine Industries estimates that lost government revenue from uncollected taxes on smuggled items could be over U.S. $2 billion annually, including substantial losses from illegal imported fuel and automobiles. Remittances and bulk cash smuggling are also channels of money laundering. The Philippines has a large expatriate community.

The Government of the Republic of the Philippines (GOP) initially established its AML/CTF regime by passing the Anti-Money Laundering Act (AMLA) of 2001. The GOP enacted Implementing Rules and Regulations for the AMLA in April 2002. The AMLA criminalized money laundering, an offense defined to include the conduct of activity involving the proceeds from unlawful activity in any one of 14 major categories of crimes, and imposes penalties that include a term of imprisonment of up to 14 years and a fine no less than 3,000,000 pesos (approximately U.S. $70,000) but no more than twice the value of proceeds or property involved in the offense. The Act also imposed identification, record keeping, and reporting requirements on banks, trusts, and other institutions regulated by the Central Bank, as well as insurance companies, securities dealers, foreign exchange dealers, money remitters, and dealers in valuable objects or cash substitutes regulated by the Securities and Exchange Commission (SEC). The GOP amended the AMLA in 2003 to correct certain inadequacies identified by the Financial Action Task Force. The amendments included lowering the threshold amount for covered transactions (cash or other equivalent monetary instrument) from 4,000,000 pesos to 500,000 pesos (approximately U.S. $100,000 to $12,000) within one banking day; expanded financial institution reporting requirements to include the reporting of suspicious transactions, regardless of amount; authorized the Central Bank (Bangko Sentral ng Pilipinas or BSP) to examine any particular deposit or investment with any bank or nonbank financial institution in the course of a periodic or special examination (in accordance with the rules of examination of the Central Bank); ensured institutional compliance with the Anti-Money Laundering Act; and deleted the prohibitions against the Anti-Money Laundering Council's examining particular deposits or investments opened or created before the Act.

The original AMLA established the Anti-Money Laundering Council (AMLC) as the country's financial intelligence unit (FIU). The Council is composed of the Governor of the Central Bank, the Commissioner of the Insurance Commission, and the Chairman of the Securities and Exchange Commission. By law, the AMLC Secretariat is an independent agency responsible for receiving, maintaining, analyzing, evaluating covered and suspicious transactions and investigating reports for possible criminal activity. It provides advice and assistance to relevant authorities and issues relevant

publications. The AMLC completed the first phase of its information technology upgrades in 2004. This allowed AMLC to electronically receive, store, and search "covered transaction reports" (CTRs) filed by regulated institutions. By the end of 2007, the AMLC had received more than 10,469 suspicious transaction reports (STRs) involving 18,269 suspicious transactions, and 103,714,619 CTRs. The AMLC has begun the second phase of its information technology upgrades by installing software to implement link analysis and visualization to enhance its ability to produce information in graphic form from the CTRs and STRs filed electronically by regulated institutions.

On February 28, 2007, the AMLC entered into a Memorandum of Understanding with the Central Bank setting forth the procedures for improved information exchange, compliance and enforcement policies. AMLC's role goes beyond traditional FIU responsibilities and includes the investigation and prosecution of money laundering cases. AMLC has the ability to seize assets involved in money laundering on behalf of the GOP after a money laundering offense has been proven beyond a reasonable doubt. To freeze assets allegedly connected to money laundering, the AMLC must establish probable cause that the funds relate to an offense enumerated in the Act, such as terrorism. The Court of Appeals then may freeze the bank account for 20 days. The AMLC may apply to extend a freeze order prior to its expiration. The AMCL is required to obtain a court order to examine bank records for activities not listed in the Act, except for certain serious offenses such as kidnapping for ransom, drugs, and terrorism-related crimes. The AMLC and the courts are working to shorten the time needed so funds are not withdrawn before the freeze order is obtained. The AMLC has frozen funds at the request of the UN Security Council, the United States, and other foreign governments. Through the end of 2007, the AMLC had frozen funds in excess of 1.4 billion Philippine pesos (approximately U.S. $32 million) and had received 67 official requests for anti-terrorism action, many concerning groups on the UNSCR 1267 Sanction Committee's consolidated list.

The Philippines has no comprehensive legislation pertaining to civil and criminal forfeiture. Various government authorities, including the Bureau of Customs and the Philippine National Police, have the ability to temporarily seize property obtained in connection with criminal activity. Money and property must be included in the indictment, however, to permit forfeiture. Because ownership is difficult to determine in these cases, assets are rarely included in the indictment and are rarely forfeited. The AMLA gives the AMLC the authority to seize assets involved in money laundering operations that may be forfeited after conviction, even if the assets constitute a legitimate business. In December 2005, the Supreme Court issued a rule covering civil forfeiture, asset preservation, and freeze orders. The new rule provides a way to preserve assets prior to any forfeiture action and lists the procedures to follow during the action. The rule also contains clear direction to the AMLC and the court of appeals on the issuance of freeze orders for assets under investigation, eliminating confusion arising from the amendment to the AMLA in 2003. As of December 2007, there have been 107 money laundering, civil forfeiture, and related cases in Philippines court system that involved AMLC investigations or prosecutions, including 37 for money laundering, 20 for civil forfeiture, and the rest pertaining to freeze orders and bank inquiries. The Philippines had its first conviction for a money laundering offense in early 2006.

Under the AMLA and the bank secrecy act, officers, employees, representatives, agents, consultants, and associates of financial institutions are exempt from civil or criminal prosecution for reporting covered transactions. These institutions must maintain and store records of transactions for a period of five years, extending beyond the date of account or bank closure.

The AMLC and the Central Bank jointly and closely monitor compliance by banks and other financial institutions with AMLA provisions. Both have full mechanisms in place to ensure that the financial community is adhering to reporting and other AMLA requirements. Commercial banks, whose assets account for 88 percent of the Philippine banking industry, adopted on October 15, 2007 an electronic money laundering transaction monitoring system which generates transaction reports and suspicious transactions reports in compliance with Central Bank rules. During regular bank examinations, Central

Bank examiners test the capabilities of the banks' electronic money laundering transaction monitoring system. The remaining 12 percent of the banking industry (without electronic monitoring systems) are still required to establish a system for flagging and monitoring suspicious transactions, regardless of the amount.

The AMLC continues to work to bring the numerous foreign exchange offices in the country under its purview. The Monetary Board issued a circular on January 24, 2005 to bring the registration and operations of foreign exchange dealers and remittance agents under the AMLA. To obtain a license, dealers must attend an AML/CTF training course conducted by the AMLC. To date, only about 5,000 of the estimated 15,000 exchange dealers/remittance agents have registered. There are still several sectors operating outside of AMLC control. Although the revised AMLA specifically covers exchange houses, insurance companies, and securities brokers, it does not cover accountants. The AMLC requires car dealers and vendors of construction equipment, which are emerging as money laundering methodologies, to report suspicious transactions to the AMLC. On March 15, 2007 the Central Bank issued Circular 564 establishing guidelines governing the acceptance of valid identification cards including the AMLA's "two-ID requirement" for conducting financial transactions with banks and nonbank financial institutions.

In 2006, the AMLC requested the chain of casinos operated by the state-owned Philippine Amusement and Gaming Corporation (PAGCOR) to submit covered and suspicious transaction reports, but it has not yet done so. There is increasing recognition that the 15 casinos nationwide offer abundant opportunity for money laundering, especially with many of these casinos catering to international clientele arriving on charter flights from around Asia. Several of these gambling facilities are located near small provincial international airports that may have less rigid enforcement procedures and standards for cash smuggling. PAGCOR is the sole franchisee in the country for all games of chance, including lotteries conducted through cell phones. At present, there are no offshore casinos in the Philippines, though the country is a growing location for Internet gaming sites that target overseas audiences in the region.

The Philippines has over 5,000 nongovernmental organizations (NGOs) that do not fall under the requirements of the AMLA. All nonstock and nonprofit organizations registered with the Securities and Exchange Commission (SEC) are required to annually submit General Information Sheets and Audited Financial Statements. Because of their ability to circumvent the usual documentation and reporting requirements imposed on banks for financial transfers, NGOs could be used as conduits for terrorist financing without detection. The AMLC is aware of the problem and is working with the SEC to bring charitable and not-for-profit entities under regulations for covered institutions. To promote transparency, SEC Circular 8 issued in June 2006 revised regulations on the registration, operations, and audit of foundations which are nonstock, nonprofit corporations.

There are seven offshore banking units (OBUs) established since 1976. OBUs account for less than two percent of total banking system assets in the country. The Central Bank regulates onshore banking and exercises regulatory supervision over OBUs, and requires OBUs to meet reporting provisions and other banking rules and regulations. In addition to registering with the SEC, financial institutions must obtain a secondary license from the Central Bank subject to relatively stringent standards that would make it difficult to establish shell companies in financial services of this nature. For example, a financial institution operating an OBU must be physically present in the Philippines. Anonymous directors and trustees are not allowed. The SEC does not permit the issuance of bearer shares for banks and other companies.

Despite the efforts of Philippine authorities to publicize regulations and enforce penalties, cash smuggling remains a major concern for the Philippines. Although there is no limit on the amount of foreign currency an individual or entity can bring into or take out of the country, any amount in excess of U.S. $10,000 equivalent must be declared upon arrival or departure. Based on the amount of foreign

currency exchanged and expended, there is systematic abuse of the currency declaration requirements and a large amount of unreported cash entering the Philippines.

The problem of cash smuggling is exacerbated by the large volume of foreign currency remitted to the Philippines by Overseas Filipino Workers (OFWs). The amount of remitted funds grew by 18 percent during the first ten months of 2007, and should exceed $14 billion for the year, equal to 11 percent of GDP. The Central Bank estimates that an additional $2-3 billion is remitted outside the formal banking system. Most of these funds are brought in person by OFWs or by designated individuals on their return home and not through any alternative remittance system. Since most of these funds enter the country in smaller quantities than $10,000, there is no declaration requirement and the amounts are difficult to calculate. The Philippines encourages local banks to set up offices in remitting countries and facilitate fund remittances, especially in the United States, to help reduce the expense of remitting funds. OFWs also use underground remittance systems such as hawala.

The Philippines is a founding member of the Asia/Pacific Group on Money Laundering (APG). The AMLC became the 101st member of the Egmont Group of FIUs in July 2005. The GOP is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime and to all 12 international conventions and protocols related to terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism. The GOP is a party to the UN Convention against Corruption. The Philippines is listed 131 out of 180 countries surveyed by Transparency International's 2007 International Corruption Perception Index.

On June 20, 2007 the ALMC filed 165 counts of money laundering against a retired Philippine Army Major General and family members charging them with amassing more than U.S. $6.5 million in ill-gotten wealth.

The Anti-Money Laundering Council must obtain a court order to freeze assets of terrorists and terrorist organizations placed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and other foreign governments. In 2007, the GOP enacted an anti-terrorism law that defines and criminalizes terrorism and terrorist financing. The Human Security Act which went into effect in July 15, 2007 criminalizes terrorism and conspiracy to commit terrorism; penalizes an offender on the basis of his participation; empowers Philippine law enforcement to use special investigative techniques, inquire into bank accounts, and freeze and forfeit terrorist related funds and assets; creates an Anti-Terrorism Council comprised of cabinet members and support agencies.

The Financial Action Task Force removed the Government of the Republic of the Philippines from its list of Non-Cooperative Countries and Territories in 2005 due to the progress the GOP had made in remedying the deficiencies that resulted in its being placed on the list in 2001.The GOP has continued to make progress enhancing and implementing its amended anti-money laundering regime, including the enactment in 2007 of new legislation that criminalizes terrorism and terrorist financing. The Central Bank should be empowered to levy administrative penalties against covered entities in the financial community that do not comply with reporting requirements. Accountants should be required to report CTRs and STRs. Casinos should be fully regulated and supervised for AML/CTF procedures and required to file STRs. The Philippines should enact comprehensive legislation regarding freezing and forfeiture of assets that would empower AMLC to issue administrative freezing orders to avoid funds being withdrawn before a court order is issued. The GOP should also consider establishing a civil forfeiture regime. The creation of an asset forfeiture fund would enable law enforcement agencies to draw on the fund to augment their budgets for investigative purposes. Such a fund would benefit the AMLC and enable it to purchase needed equipment. Finally, AMLC should separate its analytical and investigative responsibilities and establish a separate investigative division that would focus its attention on dismantling money laundering and terrorist financing operations.

Poland

Poland lies directly along one of the main routes between the former Soviet Union republics and Western Europe that narcotics traffickers and organized crime groups use. According to Polish Government estimates, narcotics trafficking, organized crime activity, auto theft, smuggling, extortion, counterfeiting, burglary, and other crimes generate criminal proceeds in the range of U.S. $3 to $5 billion each year. According to the Government of Poland (GOP), fuel smuggling, by which local companies and organized crime groups seek to avoid excise taxes by forging gasoline delivery documents, is a major source of proceeds to be laundered. With regard to economic offenses, the largest illegal income is connected with lost customs duties and taxes. Money laundering through trade in scrap metal and recyclable material is a fast developing trend. It is also believed that some money laundering in Poland originates in Russia or other countries of the former Soviet Union. The GOP estimates that the unregistered or gray economy, used primarily for tax evasion, may be as high as 13 percent of Poland's U.S. $460 billion gross domestic product (GDP). The GOP believes the black economy comprises only one percent of GDP.

Reportedly, some of Poland's banks serve as transit points for the transfer of criminal proceeds. As of June 2007, 51 commercial banks and 584 "cooperative banks" primarily serving the rural and agricultural community had licenses to operate. The GOP considers the nation's banks, insurance companies, brokerage houses, and casinos to be important venues of money laundering. The Finance Ministry maintains that the effectiveness of actions against money laundering involving transfer of money to so-called tax havens is limited. Poland's entry into the European Union (EU) in May 2004 increased its ability to control its eastern borders, thereby allowing Poland to become more effective in its efforts to combat all types of crime, including narcotics trafficking and organized crime.

Poland's anti-money laundering (AML) regime began in November 1992, when the President of the National Bank of Poland issued an order instructing banks how to deal with money entering the financial system through illegal sources. The August 1997 Banking Act and 1998 Resolution of the Banking Supervisory Commission, add customer identification requirements and institute a threshold reporting requirement.

The November 2000 Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources and on Counteracting the Financing of Terrorism, as amended, further improves Poland's ability to combat money laundering. This law, which the GOP has updated to conform to EU standards and to improve its operational effectiveness, increased penalties for money laundering and contains safe harbor provisions that exempt financial institution employees from normal restrictions on the disclosure of confidential banking information. Parliament has further amended the law to broaden the definition of money laundering to include assets originating from illegal or undisclosed sources. Poland's initial money laundering regime neglected to address many nonbank financial institutions that had traditionally been used for money laundering. To remedy this deficiency, the Parliament passed several amendments to the 2000 money laundering law. The amendments expand the scope of institutions subject to identity verification, record keeping, and suspicious transaction reporting requirements. Entities subject to the reporting requirements include banks, the National Depository for Securities, post offices, auction houses, antique shops, brokerages, casinos, insurance companies, investment and pension funds, leasing firms, private currency exchange offices, real estate agencies, notaries public, lawyers, legal counselors, auditors, and charities, as well as the National Bank of Poland in its functions of selling numismatic items, purchasing gold, and exchanging damaged banknotes. Lawyers strongly opposed the amendments, claiming that the law violates attorney-client confidentiality privileges. The Polish Bar mounted a challenge to some provisions, and submitted a motion to the Constitutional Tribunal to determine the consistency of certain regulations with ten articles in the Polish Constitution.

The law also requires casinos to report the purchase of chips worth 1,000 euros (approximately U.S. $1,400) or more. In addition to requiring that obliged entities notify the financial intelligence unit (FIU) of all financial deals exceeding 15,000 euros (approximately U.S. $21,000), covered institutions must also file reports of suspicious transactions, regardless of the size of the transaction. Polish law also requires financial institutions to put internal AML procedures into effect, a process that is overseen by the FIU.

The Criminal Code criminalizes money laundering for all serious crimes. Article 299 of the Criminal Code addresses self-laundering and criminalizes tipping off. The Polish Code of Criminal Procedure, Article 237, allows for certain Special Investigative Measures (SIM). Although money laundering investigations are not specifically discussed in relation to SIM, the organized crime provisions might apply in some cases. Poland's National Security Strategy rates the AML effort as a top priority.

The "Act on Counteracting Money Laundering and Terrorism Financing" is undergoing revisions. The revised legislation will implement the EU's Third Money Laundering Directive (Directive 2005/60/EC of the European Parliament and of the Council, on preventing usage of the financial system for money laundering and terrorist financing). The Directive was to be transposed into Polish legislation by 15 December 2007, but October 2007 parliamentary elections and the recent change of government delayed the implementation process.

As of June 15, 2007, travelers entering Poland from a nonEU country or traveling to a nonEU country with 10,000 euros (approximately $14,500) or more in cash must declare their cash or monetary instruments in writing. To comply with EU standards, Poland's customs law requires travelers to complete and present a customs and currency declaration if they are transporting more than 10,000 euros (approximately U.S. $14,700) in currency or financial instruments upon entry. In December 2007 the new Schengen countries, including Poland, were enveloped within EU borders. Land border controls between EU member states disappeared on December 20, 2007.

The 2000 AML law provides for the creation of a financial intelligence unit (FIU), the General Inspectorate of Financial Information (GIIF) within the Ministry of Finance, to collect and analyze large cash and suspicious transactions. The vast majority of required notifications to the GIIF come through the electronic reporting system. Only some small institutions lacking the equipment to use the electronic system submit notifications on paper. Although the new system is an important tool for Poland's AML regime, the efficient processing and analyzing of the large number of reports that are sent to the GIIF is a challenge for the understaffed FIU. To help improve the FIU's efficiency in handling the large volume of reports filed by obliged institutions, the GIIF continues work on a specialized IT program that will support complex data analysis and improve the FIU's efficiency in handling the increasing number of reports which it receives.

In 2006, the GIIF received over 26 million reports from obliged institutions, including 26.7 million cash transaction reports and 48,229 suspicious transaction reports (STRs), the majority of which were cash transaction reports and 90 percent of which came from the banking community. Of these, 47,817 related to money laundering and 412 related to terrorist financing. However, upon completion of preliminary analysis, it was determined that 68 percent of these STRs were erroneous due to a technical error by the filing institution or incomplete information provided on the STR. As a result, only 15,061 of the STRs were accurate and subject to further analysis by the GIIF. The FIU's analysis resulted in the production of 1,139 analytical reports. As a result of these 1,139 reports, GIIF sent 198 notifications to the Prosecutor's Office. At a minimum, all reports submitted by the GIIF to the Prosecutor's Office result in initial investigative proceedings. From 198 notifications sent to the prosecutor's office by the GIIF in 2006, two cases reached the court. As of September 2007, the courts are still investigating 175 notifications. In the past, many of the GIIF-instigated investigations have resulted in convictions for other nonfinancial offenses. The GIIF receives approximately 2.3 million reports per month on transactions exceeding the threshold level.

In addition to the Prosecutor's Office, the GIIF also cooperates with several domestic law enforcement agencies, including the General Investigative Bureau (a police unit), the Internal Security Agency (which investigates the most serious money laundering cases), and the Central Anti-Corruption Office. Coordination and information exchange between the GIIF and law enforcement entities, especially with regard to the suspicious transaction information that the GIIF forwards to the National Prosecutor's Office, has improved. The GIIF and the National Prosecutor's Office have signed a cooperation agreement that calls for the creation of a computer-based system that would facilitate information exchange between the two institutions. Work on the development of this new system is currently underway.

In 2006, GIIF conducted an assessment of the effectiveness of Poland's anti-money laundering reporting system. According to the GIIF's 2006 annual report, the analysis identified three main threats to efficiency of the system: disproportionate reporting among Poland's 16 provinces (three provinces had extremely high reporting rates); delays in prosecutorial handling of GIIF notifications; and inadequate use of the GIIF by domestic agencies in Poland (76 percent of all queries to the GIIF were from the Prosecutor's office).

The GIIF also conducts training for specified target groups as well as e-learning, which is available to all obligated institutions and cooperating entities. In 2006, the GIIF re-introduced the electronic learning course designed to familiarize obliged institutions with Poland's AML regulations. Over 1,800 individuals (mainly from obligated institutions) participated in the GIIF's electronic learning course.

The GIIF exchanges information with its foreign counterparts. The United States, along with the United Kingdom and Ukraine, is among its most active information-sharing partners. In 2006, GIIF sent official requests to foreign financial intelligence units on 158 cases concerning 287 national and foreign entities suspected of money laundering. Foreign FIUs sent 62 information requests concerning 154 national and foreign entities to the GIIF.

The GIIF has the authority to put a suspicious transaction on hold for 48 hours. The Public Prosecutor then has the right to suspend the transaction for an additional three months, pending a court decision. Article 45 of the criminal code reverses the burden of proof so that an alleged perpetrator must prove that his assets have a legal source; otherwise, the assets are presumed to be related to the crime and the government can seize them. Both the Ministry of Justice and the GIIF reportedly desire more aggressive asset forfeiture regulations. However, lingering political sensitivities reportedly hamper approval of stringent asset seizure laws. In the first half of 2007, funds totaling U.S. $46 million have been frozen and 39 notifications of possible crimes committed have been sent to the prosecutor's office, with the GIIF suspending one transaction worth U.S. $92,000 and blocking 59 accounts worth U.S. $5.1 million. In 2006, the GIIF suspended four transactions worth U.S. $2.6 million and blocked 92 accounts worth U.S. $16.6 million.

Poland has not yet criminalized terrorist financing as is required by UNSCR 1373, arguing that all possible terrorist activities are already illegal and serve as predicate offenses for money laundering and terrorist financing investigations. The Ministry of Justice has prepared a draft of amendments to the criminal code that would criminalize terrorist financing as well as elements of all terrorism-related activity, but withdrew the draft in 2007 before it had been approved by the Council of Ministers.

The GOP has created an office of counter-terrorist operations within the National Police, which coordinates and supervises regional counter-terrorism units and trains local police in counter-terrorism measures. In December 2006, the GOP established the Intra-ministerial Unit for Terrorist Threats. Poland has also created its own terrorist watch list of entities suspected of involvement in terrorist financing. The list contains the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the names of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224, and the names designated by the EU under

its relevant authorities. All obliged institutions must verify that their customers are not included on the watch list. In the event that a covered institution discovers a possible terrorist link, the GIIF has the right to suspend suspicious transactions and accounts. In 2006, the GIIF worked on eight terrorist financing cases involving 89 subjects. Upon completion of its analysis, the GIIF forwarded three reports to the Internal Security Agency (ABW) for further analysis. The cases involved transactions related to large amounts of cash being sent to Poland as well as numerous noncash transfers involving terrorist groups or transactors from a country supporting terrorism.

A Mutual Legal Assistance Treaty between the United States and Poland came into force in 1999. In addition, Poland has signed bilateral mutual legal assistance treaties with Sweden, Finland, Ukraine, Lithuania, Latvia, Estonia, Germany, Greece, and Hungary. Polish law requires the GIIF to have memoranda of understanding (MOUs) with other international competent authorities before it can participate in information exchanges. The GIIF has been diligent in executing MOUs with its counterparts in other countries, signing a total of 36 MOUs. The MOU between the Polish FIU and the U.S. FIU was signed in fall 2003. The FIU is also currently in the process of negotiating MOUs with six additional FIUs.

Poland is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), which in 2006 conducted its third round mutual evaluation of Poland. The report is not yet available. The GIIF is a member of the Egmont Group and is enrolled in FIU.NET, the EU-sponsored information exchange network for FIUs. All information exchanged between the GIIF and its counterparts in other EU states takes place via FIU.NET.

Poland is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Poland is also a party to the European Convention on Extradition and its Protocols, the European Convention on Mutual Assistance in Criminal Matters, and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

Over the past several years, the Government of Poland has worked to implement a comprehensive AML regime that meets international standards. However, work remains, as Poland's AML regime remains noncompliant with various Financial Action Task Force (FATF) standards. Most significantly, Poland must criminalize terrorist financing. No terrorist financing prosecutions have yet been undertaken or cases brought before the court. Under current provisions, it is unclear how Poland could prosecute the funding of a terrorist or terrorist organization. Poland must also strengthen AML regulations pertaining to customer due diligence obligations, DNFBPs, nonprofit organizations, politically exposed persons, cross-border correspondent banking, and suspicious transaction reporting as it pertains to terrorist financing. The GOP should promote additional training at the private sector level and improve communication and coordination between the General Inspectorate of Financial Information and relevant law enforcement agencies. The Code of Criminal Procedure should also be amended to specifically allow the use of Special Investigative Measures in money laundering investigations, which would assist law enforcement attain a better record of prosecutions and convictions.

Portugal

Portugal is an entry point for narcotics transiting into Europe, and officials of the Government of Portugal (GOP) indicate that most of the money laundered in Portugal is narcotics-related. The GOP also reports that criminals use currency exchanges, wire transfers, and real estate purchases to launder their proceeds.

The Portuguese Madeira Islands International Business Center (MIBC) has a free trade zone, an international shipping register, offshore banking, trusts, holding companies, stock corporations, and private limited companies. The latter two business groups, of which there are approximately 6,500 companies registered in Madeira, are similar to international business corporations. All entities established in the MIBC will remain tax exempt until 2011. Twenty-seven offshore banks have licenses to operate within the MIBC. Decree-Law 10/94 permits existing banks and insurance companies to establish offshore branches. Institutions submit applications to the Central Bank of Portugal. Institutions already in the European Union have a notification process, while nonEU or new entities receive authorization. The law allows establishment of "external branches" that conduct operations exclusively with nonresidents or other Madeira offshore entities, and "international branches" that conduct both offshore and domestic business. Although Madeira has some local autonomy, Portuguese and EU legislative rules regulate its offshore sector, and the competent oversight authorities supervise it. The Madeira Development Company supervises offshore banks. Exchange of information agreements contained in double taxation treaties allow for the disclosure of information relating to narcotics or weapons trafficking. Bearer shares are not permitted.

Accessing Internet gambling sites is illegal in Portugal. There are no known cases of casinos or Internet gaming sites whose Internet service provider (ISP) is headquartered in Portugal. However, Internet gaming is still widely available.

Portugal has a comprehensive anti-money laundering and counter-terrorist financing (AML/CTF) regime that criminalizes the laundering of proceeds of serious offenses, including terrorism, arms trafficking, kidnapping, and corruption. Article 11 of Law No. 59/2007, dated September 4, 2007, defines money laundering and expands the list of crimes related to money laundering, and makes legal entities criminally accountable.

Act 11/2004, which implements the European Union's (EU's) Second Money Laundering Directive, defines the legal framework for the prevention and suppression of money laundering. The law also mandates suspicious transaction reporting by financial and nonfinancial institutions, including credit institutions, investment companies, life insurance companies, traders in high-value goods (e.g., precious metals and stones, aircraft), regardless of transaction amount. Suspicious transaction reports (STRs) go to the Public Prosecutor's Office. If a regulated entity has knowledge of a transaction likely to be related to a money laundering offense, it must inform the Portuguese financial intelligence unit (FIU). The GOP may order the entity not to complete the transaction. If stopping the transaction is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, the government may also allow the entity to proceed with the transaction but require the entity to provide the authorities with complete details. "Tipping off" is prohibited and safe harbor provisions protect regulated entities making disclosures in good faith from liability.

All financial institutions, including insurance companies, must identify their customers, maintain records for a minimum of ten years, and demand written proof from customers regarding the origin and beneficiary of transactions that exceed 12,500 euros (approximately U.S. $18,250). Nonfinancial institutions, such as casinos, property dealers, lotteries, and dealers in high-value assets must also identify customers engaging in large transactions, maintain records, and report suspicious activities to the Office of the Public Prosecutor. Beyond the requirements to report large transactions, foreign exchange bureaus are not subject to any special requirements to report suspicious transactions. Portuguese law gives the GOP the authority to investigate suspicious transactions without notifying the targets of the investigation.

In 2007, through Decree-Law No. 61/2007, Portugal implemented EU regulation EC 1889/2005, on cash entering or leaving the European Community. The law requires all individuals to declare currency valued at 10,000 euros (approximately U.S. $14,600) or greater when entering or exiting the European Community. The law also stipulates that authorities gather and exchange information at the national

and international levels. Portugal is in the process of transposing the EU's Third Money Laundering Directive (Directive 2005/60/EC) into Portuguese law.

The three principal regulatory agencies for supervision of the financial sector in Portugal are the Central Bank of Portugal, the Portuguese Insurance Institute, and the Portuguese Securities Market Commission. The Gambling Inspectorate General, the Economic and Food Safety Authority, the Economic Activities Inspectorate General, the Registries and Notaries General Directorate, the National Association for Certified Public Accountants and the Association for Assistant Accountants, the Bar Association, and the Chamber of Solicitors also monitor and enforce the reporting requirements of the obliged entities.

Tax authorities can lift secrecy rules without authorization from the target of an investigation. Rules require companies to have at least one bank account and, for companies with more than 20 employees, to conduct their business through bank transfers, checks, and direct debits rather than cash. These rules are mainly designed to help the GOP investigate possible cases of tax evasion but may ease enforcement of other financial crimes as well.

Portuguese Securities Market Commission Regulation 7/2005 requires financial intermediaries to submit detailed annual Control and Supervision Reports to the Commission every June. The regulation entered into force on January 1, 2006.

There is no single body that oversees charitable organizations or their possible terrorist finance-related activities. The Intelligence Security Service, the Judicial Police, and the Public Prosecutor's office share supervisory authority. International financial transactions that may involve terrorist financing require the same monitoring protocol as those involving possible money laundering.

Decree-Law 304/2002 established Portugal's FIU, known as the Financial Information Unit, or Unidade de Informação Financeira (UIF), which operates independently as a department of the Portuguese Judicial Police (Polícia Judiciária). At the national level, the UIF is responsible for gathering, centralizing, processing, and publishing information pertaining to investigations of money laundering, tax crimes, and terrorism. It also facilitates cooperation and coordination with other judicial and supervising authorities. At the international level, the UIF coordinates with other FIUs. The UIF has policing duties but no regulatory authority.

In 2006, the UIF received 584 STRs. The FIU also received over 15,000 other reports, primarily from the General Inspectorate for Gaming. The UIF sent 272 cases for further investigation to the Judicial Police and other police departments. 2007 STR information is not yet available. Between January and September of 2007, the UIF seized or confiscated approximately 32.4 million euros (approximately U.S. $47.3 million).

Police may request files of individuals under investigation and, with a court order, can obtain and use audio and video recordings as evidence in court. Portuguese laws provide for the confiscation of property and assets connected to money laundering, and authorize the Judicial Police to trace illicitly obtained assets (including those passing through casinos and lotteries). The Judicial Police can do this even if the predicate crime is committed outside of Portugal. Act 5/2002 defines criminal assets as those owned by an individual at the time of indictment and thereafter. Act 5/2002 also shifted the burden of proof in cases of criminal asset forfeiture from the government to the defendant; an individual must prove that his or her assets were not obtained as a result of his illegal activities. The law also presumes that assets transferred by an individual to a third party within the previous five years still belong to the individual in question, unless proven otherwise. GOP law enforcement agencies have seized a total of 20.7 million euros (approximately U.S. $30.2 million) in nonmonetary goods in association with drug and money laundering investigations. The law allows the Public Prosecutor to request that a lien be placed on the assets of individuals being prosecuted, to facilitate asset seizures related to narcotics and weapons trafficking, terrorism, and money laundering. Portugal

has comprehensive legal procedures that enable it to cooperate with foreign jurisdictions and share seized assets.

Act 52/2003 specifically defines terrorist acts and organizations and criminalizes the transfer of funds related to the commission of terrorist acts. Portugal has created a Terrorist Financing Task Force that includes the Ministries of Finance and Justice, the Judicial Police, the Security and Intelligence Service, the Bank of Portugal, and the Portuguese Insurance Institution. Names of individuals and entities included on the UN Security Council Resolution 1267 Committee's consolidated list or that the United States and EU have linked to terrorism are passed to private sector organizations. The Bank of Portugal, the Stock Exchange Commission, and the Portuguese Insurance Institution circulate the lists to the obliged entities. In practice, while the government has the authority to immediately freeze funds, an actual seizure of assets would only occur once the EU's clearinghouse process resulted in agreement to the EU-wide seizure of assets of terrorists and terrorist-linked groups. Portugal is actively cooperating in the search and identification of assets used for terrorist financing. To date, no significant assets have been identified or seized.

Portugal is a member of the Financial Action Task Force (FATF), and underwent a mutual evaluation by that body in 2006. Portugal's FIU is a member of the Egmont Group. Portugal is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the UN International Convention for the Suppression of the Financing of Terrorism. Portugal is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. The U.S. and Portugal signed a mutual legal assistance agreement (MLAT) and an extradition agreement in 2005, designed to complement and implement the U.S.-European Union Mutual Legal Assistance and Extradition Treaties of 2003. These agreements are pending U.S. ratification.

Portugal should collect and maintain more information and data regarding the number of money laundering and terrorist financing investigations, prosecutions and convictions as well as the amount of property and assets frozen, seized and confiscated as it relates to money laundering and terrorist financing. The GOP should work to correct any identified deficiencies regarding its asset freezing and forfeiture regime, improve its mechanisms to determine the beneficial owners, and ensure that the terrorist financing law covers financing to individuals. The FIU should be the competent authority to receive and analyze all STRs. Portugal should strengthen its legal requirements relating to politically exposed persons. The GOP should also improve its implementation of AML/CTF rules for obliged nonfinancial businesses and professions.

Qatar

Qatar has fewer than one million residents with a low rate of general and financial crime. Historically, Qatar has not been an important regional financial center, though with the country's remarkable energy-driven growth in recent years it aims to become an increasingly important banking and financial services center in the Gulf.

The Qatar Central Bank (QCB) exercises regulatory authority over the financial sector. There are 17 licensed banks, including three Islamic banks and a specialized bank, the Qatar Industrial Development Bank. There is a separate Qatar Financial Center (QFC) that allows major international financial institutions and corporations to set up offices with 100 percent foreign ownership, unlike most business sectors in Qatar. There are currently 18 banks, 6 investment banks, 5 asset management companies, and 7 insurance companies authorized to operate in the QFC. QFC firms are limited to providing services to wholesale clients, except for insurance companies who can provide services to both wholesale and retail clients. The QFC has a separate, independent regulatory authority, the QFC Regulatory Authority, with a regulatory regime based on international standards. There are plans underway to create a unified regulatory authority for the country within the next two years. Qatar has

20 exchange houses, three investment companies and two commercial finance companies. Although Qatar still has a cash-intensive economy, authorities believe that cash placement by money launderers is a negligible risk due to the close-knit nature of the society and the rigorous "know your customer" procedures required by Qatari law.

Qatar has a clear legal framework for financial crimes that is based on a 2002 law on money laundering and a 2004 law on terrorist financing. The judicial system has yet to be tested as there have been no arrests or prosecutions for money laundering or terrorist financing crimes since enactment of the laws.

On September 11, 2002, the Amir (Head of State) of the State of Qatar signed the Anti-Money Laundering Law. According to Article 28, money laundering offenses involve the acquisition, holding, disposing of, managing, keeping, exchanging, depositing, investing, transferring, or converting of funds from illegal proceeds. The law imposes fines and penalties of imprisonment of five to seven years. The law expanded the powers of confiscation to include the identification and freezing of assets as well as the ultimate confiscation of the illegal proceeds upon conviction of the defendant for money laundering. Article Two includes any activities related to terrorist financing. Article 12 authorizes the Central Bank Governor to freeze suspicious accounts for up to ten days and to inform the Attorney General within three days of any action taken. The Attorney General may renew or nullify the freeze order for a period of up to three months.

The law requires all financial institutions to report suspicious transactions to the Financial Information Unit and retain records for up to 15 years. The law also gives the QCB greater powers to inspect suspicious bank accounts and grants the authorities the right to confiscate money in illegal transactions. Article 17 permits the State of Qatar to extradite convicted criminals in accordance with international or bilateral treaties.

The QFC law provides that Qatari criminal laws apply in the QFC, including those Qatari laws criminalizing money laundering and the financing of terrorism. In addition, the QFC has implemented its own anti-money laundering regulations and corresponding rules. The QFC Regulatory Authority is responsible for supervising QFC firms' compliance with QFC AML requirements.

The Anti-Money Laundering Law established the National Anti-Money Laundering Committee (NAMLC) to oversee and coordinate money laundering combating efforts. It is chaired by the Deputy Governor of the QCB and includes members from the Qatar Central Bank, FIU, Ministries of Interior, Labor and Social Affairs, Economy and Commerce, Finance, Justice, Customs and Ports Authority and the State Security Bureau.

In February 2004, the Government of Qatar (GOQ) passed the Combating Terrorism Law. According to Article Four of the law, any individual or entity that provides financial or logistical support, or raises money for activities considered terrorist crimes, is subject to punishment. The punishments are listed in Article Two of the law, which include the death penalty, life imprisonment, and 10 or 15 year jail sentences depending on the crime. Qatar has a national committee separate from the NAMLC to review the consolidated UN 1267 terrorist designation lists and to recommend any necessary actions against individuals or entities found in Qatar. The committee is chaired by the Minister of State for Interior Affairs and includes the FIU and various law enforcement representatives. The committee and the Central Bank circulate to financial institutions the individuals and entities included on the UN 1267 Sanctions Committee's consolidated list, but have thus far not identified or frozen any related assets.

The QCB updates regulations regarding money laundering and financing of terrorism on a regular basis, in accordance with international requirements. The QCB aims to increase the awareness of all banks operating in Qatar with respect to anti-money laundering efforts by explaining money laundering schemes and monitoring suspicious activities.

In October 2004, the GOQ established a financial intelligence unit (FIU) known as the Qatar Financial Information Unit (QFIU). The FIU is responsible for receiving and reviewing all suspicious and financial transaction reports, identifying transactions and financial activities of concern, ensuring that all government ministries and agencies have procedures and standards to ensure proper oversight of financial transactions, and recommending actions to be taken if suspicious transactions or financial activities of concern are identified. The FIU also obtains additional information from the banks and other government ministries. Suspicious transaction reports (STRs) are now sent to the FIU by hardcopy or electronically, but the FIU is developing an all-electronic system with bank compliance offices that should speed the reporting process. The QCB, Public Prosecutor and the Criminal Investigation Division (CID) of the Ministry of the Interior work together with the FIU to investigate and prosecute money laundering and terrorism finance cases. The FIU also coordinates closely with the Doha Securities Market (DSM) to establish procedures and standards to monitor all financial activities that occur in Qatar's stock market. The FIU coordinates the different regulatory agencies in Qatar. The FIU also works closely with the QFC Regulatory Authority to ensure that QFC firms, and specifically their Money Laundering Reporting Officers, understand and implement appropriate AML and counter-terrorist finance policies and procedures. The Qatari FIU became a member of the Egmont Group in 2005.

In December 2004, the QCB installed a central reporting system to assist the FIU in monitoring all financial transactions made by banks. All accounts must be opened in person. Banks are required to know their customers; the banking system is considered open in that in addition to Qatari citizens and legal foreign residents, nonresidents can open an account based on a reliable recommendation from his or her primary bank. Hawala transactions are prohibited by law in Qatar.

Law No. 13 from 2004 established The Qatar Authority for Charitable Works, which monitors all charitable activity in and outside of Qatar. The Secretary General of the Authority approves all international fund transfers by the charities. The Authority reports to the Ministry of Labor and Social Affairs and has primary responsibility for monitoring overseas charitable, development, and humanitarian projects that were previously under the oversight of several government agencies such as the Ministry of Foreign Affairs, the Ministry of Finance and the Ministry of Economy and Commerce. Overseas activities must be undertaken in collaboration with a nongovernmental organization (NGO) that is legally registered in the receiving country. The Authority prepares an annual report on the status of all projects and submits the report to relevant ministries. The Authority also regulates domestic charity collection. Article 13 of the law provides penalties of up to a year in prison, a fine of 50,000 Qatari riyals (approximately U.S. $13,750), and confiscation of the money involved for "anyone who collects donations, or transfers money outside the country, bestows or accepts loans or grants or donations or bequests or endowments" outside of The Authority's purview.

Qatar does not have mandatory cross-border currency reporting requirements. Customs officials are given authority under the law to, in suspicious cases, require travelers to fill out forms declaring cash currency or other negotiable financial instruments in their possession. Officials then forward the traveler's information to the FIU for evaluation. The FIU has received about 60 reports from Customs for evaluation. Immigration and customs authorities are reviewing their policies to expand their ability to enforce money declarations and detect trade-based money laundering.

The Government of Qatar is a party to the 1988 UN Drug Convention. Qatar has not signed the UN Convention for the Suppression of the Financing of Terrorism or the UN Convention against Corruption. The Ministerial Council approved Qatar's accession to the UN Convention against Transnational Organized Crime in fall 2007, but final approval is still pending. Qatar is ranked 32 out of 179 countries surveyed in Transparency International's 2007 Corruption Perception Index. Qatar is one of the original signatories of the 2004 memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENA-FATF), a FATF-style

regional body that promotes best practices to combat money laundering and terrorist financing in the region.

The Government of Qatar should continue to implement AML/CTF policies and procedures that adhere to world standards. Per FATF Special Recommendation Nine, Qatar should initiate and enforce in-bound and out-bound cross-border currency reporting requirements. The data should be shared with the FIU. The government should continue to work to ensure that law enforcement, prosecutors, and customs authorities receive the necessary training and technical assistance to improve their capabilities in recognizing and pursuing various forms of terrorist financing, money laundering and other financial crimes. Qatar should become a party to the UN International Convention for the Suppression of the Financing of Terrorism, and complete its accession to the UN Convention against Transnational Organized Crime.

Romania

Romania's geographical location makes it a natural transit country for trafficking in narcotics, arms, stolen vehicles, and persons. As such, the nation is vulnerable to financial crimes. According to law enforcement entities, estimates of crimes involving money laundering amount to approximately $15 million per year. Trans-border smuggling of counterfeit goods, tax fraud and fraudulent claims in relation to consumer lending are additional types of financial crimes prevalent in Romania. Romania also has one of the highest occurrences of cybercrime and online credit card fraud in the world, with the vast majority of victims residing in the United States.

Laundered money comes primarily from international crime syndicates who conduct their criminal activity in Romania and subsequently launder their illicit proceeds through illegitimate front companies. Another source of laundered money is the proceeds of illegally smuggled goods such as cigarettes, alcohol, gasoline, and other dutiable commodities. Corruption in Romania's customs and border control and as well in several neighboring Eastern European countries also facilitates money laundering. In 2003, Romania instituted an anti-corruption plan and passed a law criminalizing organized crime.

Romania's Law No. 21/99, On the Prevention and Punishment of Money Laundering, criminalizes money laundering and requires customer identification, record keeping, suspicious transaction reporting, and currency transaction reporting for transactions (including wire transfers) over 10,000 euros (approximately U.S. $14,700). The list of entities covered by Law No. 21/99 includes banks, nonbank financial institutions, attorneys, accountants, and notaries. Romania has also criminalized tipping off suspected money launderers. Romanian law permits the disclosure of client and ownership information to bank supervisors and law enforcement authorities, and safe harbor provisions protect banking officials when they cooperate with law enforcement.

The Law on the Prevention and Sanctioning of Money Laundering (Law 656/2002) expands the list of predicate offenses to include all crimes and expands the number and types of entities subject to anti-money laundering (AML) regulations. The additional entities include art dealers, travel agents, privatization agents, postal officials, money service businesses, and real estate agents. Although nonbank financial institutions are covered under Romania's AML law, regulatory supervision of this sector is weak and not as rigorous as that imposed on banks.

In keeping with international standards, Romania has taken steps to strengthen its know-your-customer (KYC) identification requirements. The National Bank of Romania's (BNR) 2003 Norm No. 3, "Know Your Customer," strengthens information disclosure requirements for outgoing wire transfers and correspondent banking by requiring banks to include information about the originator's name, address, and account. The same information is required for incoming wires as well. Banks are further required to undertake proper due diligence measures before entering into international

correspondent relations and are prohibited from opening correspondent accounts with shell banks. In 2006, the BNR widened the scope of its KYC norms by extending their application to all other nonbanking financial institutions falling under its supervision. The Insurance Supervision Commission has instituted similar regulations for the insurance industry.

Law 230/2005 provides for a uniform approach to combating and preventing money laundering and terrorist financing. With this law, Romania meets the requirements of two European Union (EU) Money Laundering Directives, as well as the requirements of the European Council's Framework Decision of June 2001 on Identification, Search, Seizure, and Confiscation of the Means and Goods Obtained from Such Offenses. The modified law also responds to Financial Action Task Force (FATF) recommendations and establishes a suspicious transactions reporting requirement for transactions linked to terrorist financing.

In 2006, Romania made further changes to its laws to bring the country into harmony with FATF recommendations and EU Directives. Romania amended its laws to increase the amount of fines corresponding to the inflation rate; to allow the use of undercover investigators; and to send reports from the financial intelligence unit (FIU) to the General Prosecutor's Office in an unclassified manner for use in operational investigations. The law also provides for confiscation of goods used in or resulting from money laundering activities; and an increase in the length of time that bank accounts may be frozen from ten days up to one month.

The FIU Board has issued regulations implementing KYC standards for nonfinancial reporting agencies that are not the subject of supervision by other national authorities. These norms are consistent with EU Directives and allow the FIU to increase supervision of entities (casinos, notaries, real estate brokers) previously unsupervised for compliance with AML regulations. As a member of the EU, Romania was required to fully adopt the EU's Third Money Laundering Directive, known as European Commission Directive 2005/60/EC, on preventing the use of the financial system for the purpose of money laundering and terrorist financing by December 15, 2007.

Romania's FIU, the National Office for the Prevention and Control of Money Laundering (NOPCML), was established in 1999. All obliged entities must submit their currency transaction reports and suspicious transaction reports (STRs) to the FIU. The FIU oversees the implementation of AML guidelines for the financial sector and works to ensure that all domestic financial institutions covered by the law receive adequate training. The FIU is also authorized to participate in inspections and controls in conjunction with supervisory authorities. In the first ten months of 2007, the FIU carried out 189 on-site inspections in cooperation with the Financial Guard or other supervision authorities—an increase from the 109 inspections for the same period in 2006.

Since its establishment, the FIU has faced numerous challenges, including charges against a former director for the destruction of public records and corruption. Under its current President, the FIU has worked to improve the quality of cases forwarded to prosecutors for judicial action. The FIU believes that the number of indictments, and eventual convictions, will increase over time as the FIU places greater emphasis on the quality of reports produced as opposed to the quantity of reports forwarded to the Prosecutor's Office.

During the first ten months of 2007, the FIU received 10,747 currency transaction reports for transactions exceeding the 10,000 euros (approximately U.S. $14,700) threshold, an increase from 9,110 in the same period in 2006. During the first nine months of 2007, the FIU received 6,511 reports of cross-border transfers, compared with 6,735 reports in 2006. During the same period, the total number of STRs received was 1,542, down from 2,218 reports in 2006. Of this figure, banks submitted 1,435 reports and individuals submitted 25 reports. Money transfer agents substantially increased their submissions, sending 18 reports compared with 10 reports last year; as did independent legal professionals, who submitted seven reports, up from three reports in 2006. The remainder came from various other entities, including: financial investment services; insurance/re-insurance firms; real

estate brokers; leasing companies; foreign exchange houses; consulting; and fiscal/accounting service providers.

During the first ten months of 2007, the FIU suspended one suspicious transaction (down from three suspensions in 2006). The total amount of fines levied by the FIU in the first ten months of 2007 amounted to U.S. $129,098 (up from $98,940).

Upon completion of its analysis, the FIU forwards its findings to the appropriate government agency for follow-up investigation. During the first nine months of 2007, the FIU sent 256 files on suspicion of money laundering to the General Prosecutor's Office; the Police General Inspectorate; the National Agency for Fiscal Administration; the Financial Guard; the National Anti-Corruption Department; and the Romanian Intelligence Service. In the same interval in 2006, the FIU forwarded 127 cases onward.

Efforts to prosecute these cases have been hampered by a lack of specialization and technical knowledge of financial crimes within the judiciary. Moreover, coordination between law enforcement and the justice system remains limited. In the first half of 2007, the Directorate for the Investigation of Organized Crime and Terrorism Offenses (DIICOT), the agency primarily responsible for the prosecution of money laundering cases, indicted 70 defendants in 27 cases involving money laundering totaling approximately U.S. $7 million. Of the 70 indicted, 15 defendants have been placed under preventive arrest. During this same period, DIICOT opened criminal investigations on 236 cases involving suspicion of money laundering.

In response to the events of September 11, 2001, Romania passed a number of legislative measures designed to criminalize acts contributing to terrorism. Emergency Ordinance 141, passed in October 2001, provides that the production or acquisition of means or instruments, with intent to commit terrorist acts, are offenses of exactly the same level as terrorist acts themselves. These offenses are punishable with imprisonment ranging from five to 20 years. The Supreme Defense Council of the Country (CSAT) has adopted a National Security Strategy, which includes the General Protocol on the Organization and Functioning of the National System on Preventing and Combating of Terrorist Acts. This system, effective July 2002, and coordinated through the Intelligence Service, brings together and coordinates a multitude of agencies, including 14 ministries, the General Prosecutor's Office, the central bank, and the FIU. The Government of Romania (GOR) has also set up an inter-ministerial committee to investigate the potential use of the Romanian financial system by terrorist organizations. A revised Criminal Procedure Code entered into force in July 2003, containing provisions for authorizing wiretaps and intercepting and recording telephone calls in money laundering and terrorist financing cases.

Romanian law has some limited provisions for asset forfeiture in the Law on Combating Corruption, No. 78/2000, and the Law on Prevention and Combat of Tax Evasion, No. 241, introduced in July 2005. The GOR, and particularly the Central Bank, has been cooperative in seeking to identify and freeze terrorist assets. Emergency Ordinance 159, passed in late 2001, includes provisions for preventing the use of the financial and banking system to finance terrorist attacks and sets forth the parameters for the government to combat such use. Emergency Ordinance 153 strengthens the government's ability to carry out the obligations under UNSCR 1373, including the identification, freezing, and seizure of terrorist funds or assets. Legislative changes in 2005 extended the length of time a suspect account may be frozen. The FIU is now authorized to suspend accounts suspected of money laundering activity for three working days, as opposed to the previous two-day limit. In addition, once the case is sent to the General Prosecutor's Office, it may further extend the period by four working days instead of the previously allowed three working days.

Law 535/2004 on preventing and combating terrorism abrogates some of the previous government ordinances and incorporates many of their provisions. The law includes a chapter on combating the financing of terrorism by prohibiting financial and banking transactions with persons included on

international terrorist lists, and requiring authorization for transactions conducted with entities suspected of terrorist activities in Romania.

The Central Bank receives lists of individuals and terrorist organizations provided by the United States, the UNSCR 1267 Sanctions Committee, and the EU, and it circulates these to banks and financial institutions. The new law on terrorism provides for the forfeiture of assets used or provided to terrorist entities, together with finances resulting from terrorist activity. To date, no terrorist financing arrests, seizures, or prosecutions have been reported

The FIU is aware of the potential misuse of charitable or nonprofit entities as conduits for terrorist financing. In 2007, the FIU conducted two training events with charitable foundations and associations on preventing and combating money laundering and terrorist financing. The FIU has drafted guidelines concerning reporting entities' obligations in this respect, and has published them on its website.

The GOR recognizes the link between organized crime and terrorism. Romania is a member of and host country for the headquarters of the Southeast European Cooperative Initiative's (SECI) Center for Combating Transborder Crime, a regional center that focuses on intelligence sharing related to criminal activities, including terrorism. Romania also participates in a number of regional initiatives to combat terrorism. Romania has worked within the South East Europe Security Cooperation Steering Group (SEEGROUP) a working body of the NATO initiative for southeast Europe to coordinate counter-terrorist measures undertaken by the states of southeastern Europe. The Romanian and Bulgarian Interior Ministers have signed an inter-governmental agreement to cooperate in the fight against organized crime, drug smuggling, and terrorism.

The FIU is a member of the Egmont Group and participates as a member in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The most recent mutual evaluation of Romania was conducted in May 2007 by MONEYVAL and is scheduled to be discussed and adopted by that body in 2008.

A Mutual Legal Assistance Treaty signed in 2001 between the United States and Romania entered into force in October 2001. The GOR has demonstrated its commitment to international anti-crime initiatives by participating in regional and global anti-crime efforts. Romania is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. Romania also is a party to the UN International Convention for the Suppression of the Financing of Terrorism. The FIU has signed bilateral memoranda with fifteen countries and in 2007, concluded bilateral memoranda of understanding with FIUs from the United States, United Kingdom, Hungary, Israel, and Russia.

While Romania's AML legislation and regulations will soon be compliant with many FATF and EU standards, implementation has moved at a slower pace. The FIU has improved the timeliness and quality of its analysis and case reporting. However, these investigations have resulted in only a handful of successful prosecutions to date. With the conclusion of the Romanian capital account liberalization in 2006, the risk of money laundering through nonbank entities has been on the rise. Romania should continue its efforts to ensure that nonbank financial institutions are adequately supervised and that the sector is trained on identification of suspicious transaction and reporting and record-keeping responsibilities. Romania should continue to improve communication between reporting and monitoring entities, as well as between prosecutors and the FIU. The General Prosecutor's Office should continue to place a high priority on money laundering cases. Romania should improve implementation of existing procedures for the timely freezing, seizure, and forfeiture of criminal or terrorist-related assets. Romania should continue to make progress in combating corruption in commerce and government. Romania should enact and implement legislation to subject nongovernmental organizations (NGOs) and charitable organizations to reporting requirements.

Russia

Russia is a regional center. Its financial system does not attract a significant number of depositors, although due to rapid economic growth in various sectors, the number of depositors has steadily been increasing. Criminal elements from Russia and neighboring countries continue to use Russia's financial system to launder money because of familiarity with the language, culture, and economic system. The majority of laundered funds do not appear to be from activities related to narcotics production or trafficking, although these activities occur. Experts believe that most of the illicit funds flowing through Russia derive from domestic criminal activity, including evasion of tax and customs duties and smuggling operations. Despite making progress in combating financial crime, Russia remains vulnerable to such activity because of its vast natural resource wealth, the pervasiveness of organized crime, and, reportedly, a high level of corruption. Other vulnerabilities include porous borders, Russia's role as a geographic gateway to Europe and Asia, a weak banking system with low public confidence in it, and under funding of regulatory and law enforcement agencies. Russia's financial intelligence unit (FIU) estimates that Russian citizens may have laundered as much as U.S. $11 billion in 2007.

Russia has recently changed its laws to allow direct foreign ownership and investment in Russian financial institutions. Net private capital inflows for 2007 reached U.S. $82.3 billion according to the Russian Central Bank, an increase from U.S. $41.6 billion in 2006.

The Russian Federation has a legislative and regulatory framework in place to pursue and prosecute financial crimes, including money laundering and terrorism finance. Federal Law No. 115-FZ "On Combating Legalization (Laundering) of Criminally Gained Income and Financing of Terrorism," introduced in 2001, obliges banking and nonbanking financial institutions to monitor and report certain types of transactions, maintain records, and identify their customers. According to RF 115-FZ, institutions legally required to report include banks, credit organizations, securities market professionals, insurance and leasing companies, the federal postal service, jewelry and precious metals merchants, betting shops, and companies managing investment and nonstate pension funds. Other obliged entities include real estate agents, lawyers and notaries, and to persons rendering legal or accounting services that involve certain transactions.

Various regulatory bodies ensure compliance with Russia's anti-money laundering and counterterrorism finance (AML/CTF) laws. The Central Bank of Russia (CBR) supervises credit institutions; the Federal Insurance Supervision Service oversees insurance companies; the Federal Service for Financial Markets regulates entities managing nongovernmental pension and investment funds, as well as professional participants in the securities sector; the Federal Service for Financial Monitoring (FSFM) regulates real estate and leasing companies, pawnshops, and participants in the gaming industry; and the Assay Chamber (under the Ministry of Finance) supervises entities buying and selling precious metals or stones.

The CBR has issued guidelines regarding AML practices within credit institutions, including "know your customer" (KYC) and bank due diligence programs. Banks must obtain, and retain for a minimum of five years from the date of the termination of the business relationship, information regarding individuals, legal entities and the beneficial owners of corporate entities. Banks must also adopt internal compliance rules and procedures and appoint compliance officers. The AML Law (Law 115-FZ) requires banks to identify their customers before providing natural or legal persons with financial services. Banks are required to report all transactions subject to mandatory or suspicious transaction requirement to the to the financial intelligence unit (FIU). Credit institutions that fail to meet mandatory or suspicious reporting requirements face revocation of their licenses, limits on certain banking operations, and possible criminal or administrative penalties. The CBR can levy administrative fines on credit institutions and officials of credit institutions for violations of Russia's AML/CTF law. Criminal liability does not apply to legal persons under Russian law. The maximum

criminal penalty for natural persons convicted of money laundering or financing terrorism is 10 years in prison in addition to applicable fines.

All obligated financial institutions must monitor and report to the government any transaction that equals or exceeds 600,000 rubles (approximately U.S. $22,700) and involves or relates to cash payments, remittances, bank deposits, gaming, pawn shop operations, precious stones and metals transactions, payments under life insurance policies, or persons domiciled in countries determined by the Russian Government to be deficient in AML/CTF. Obligated institutions must also report real estate transactions valued at 3,000,000 rubles (approximately U.S. $115,400) or more. Financial institutions must develop criteria for determining suspicious transactions and report such transactions to the FIU in a timely fashion. All transactions involving an entity or person included on the Russian government's list of those involved in extremist activities or terrorism must be reported to the FIU an

Under Order 1317-U, Russian financial institutions must inform the CBR when it establishes correspondent relationships with nonresident banks in operating in offshore zones (as defined by the Russian Federation in Annex 1 of this Order). The CBR recommends that financial institutions apply enhanced due diligence to transactions with nonresident institutions. Foreign banks may only open subsidiary operations on the territory of Russia. The CBR must authorize the establishment of a subsidiary operation, and these subsidiaries must be subject to domestic Russian supervisory authorities. Foreign banks are not permitted to open branches in Russia. Russian banks must also obtain CBR approval to open operations abroad.

According to the Law No. 395-I "On Banks and Banking Activities," credit institutions must identify and inform the CBR of all appointments of individuals to senior management positions and to the managing and supervisory boards. Russian law prohibits the appointment of anonymous parties or proxy individuals to a credit institution's managing or supervisory board. The CBR has the authority to deny the appointment of a senior official if the official does not meet "fit and proper" requirements established by the CBR.

Russia has established a Deposit Insurance System (DIS) for banks. To gain admission to the DIS, a bank must verifiably demonstrate to the CBR that it complies with applicable banking and AML/CTF laws. Currently, 911 of Russia's 1,145 banks participate in the DIS.

Article 8 of Law 115-FZ provides for the establishment of Russia's FIU, called the Federal Service for Financial Monitoring (FSFM). FSFM is an independent executive agency that was administratively subordinated to the Ministry of Finance until September 2007, but which is now subordinated to the Prime Minister. The FSFM is responsible for receiving, analyzing, and disseminating reports from those entities obligated to file mandatory and suspicious reports. Nearly all financial institutions submit reports to the FSFM via encrypted software provided by the FSFM. According to the FSFM's annual report for 2006, Russia's national database contains 6.3 million reports on operations with monetary funds or other assets, with a total value of approximately $900 billion. The FSFM receives approximately 30,000 transaction reports daily. The FSFM is also the regulator for real estate and leasing companies, pawnshops, and gaming outlets. The FSFM is authorized to provide information to relevant law enforcement authorities for further investigation, i.e., the Economic Crimes Unit of the Ministry of Interior (MVD) for criminal matters, the Federal Drug Control Service (FSKN) for narcotics-related activity, or the Federal Security Service (FSB) for terrorism-related cases. As an administrative unit, it has no law enforcement or investigative powers.

The head of the FSFM chairs an Interagency Commission on Money Laundering, which is responsible for monitoring and coordinating the government's activity on money laundering and terrorist financing. Twelve ministries and government departments sit on the Commission.

Each of the seven federal districts comprising the Russian Federation contains an FSFM territorial office. The Central Federal District office is headquartered in Moscow; the remaining six are located

in the major financial and industrial centers throughout Russia (St. Petersburg, Ekaterinburg, Nizhny Novgorod, Khabarovsk, Novosibirsk and Rostov-on-Don). The territorial offices coordinate with regional law enforcement and other authorities to enhance the information flow into the FSFM, and to supervise compliance with anti-money laundering and counter-terrorist financing (AML/CTF) legislation by the institutions that the FSFM supervises. Additionally, the territorial offices must identify and register at the regional level all pawnshops, leasing companies, real estate firms, and gaming entities under their jurisdiction. The regional offices also coordinate the efforts of the CBR and other supervisory agencies to implement AML/CTF regulations. Russia's AML legislation provides the FSFM with the appropriate authority to gather information regarding the activities of investment foundations, nonstate pension funds, gambling businesses, real estate agents, lawyers and notaries, persons rendering legal or accounting services, and sellers of precious metals and stones.

During the first half of 2007, the FSFM registered 5,603 crimes involving money laundering, compared to 7,957 reports for all of 2006. Interior Ministry officials reported that 4,535 of the 2007 cases went to trial. Both the FSFM and MVD report that the number of suspicious transaction reports (STRs) for the year roughly equaled those of 2006 and credit increased cooperation among law enforcement agencies for the number of cases brought to trial.

With its legislative and enforcement mechanisms in place, Russia has begun to prosecute high-level money laundering cases. During 2007, the CBR revoked the licenses of 44 banks for failing to observe banking regulations. Of these, 30 banks lost their licenses for violating Russia's AML laws. The CBR's initiative to prohibit individuals convicted of money laundering from serving in leadership positions in the banking community—a cause championed by Andrey Kozlov, the First Deputy Chairman of the CBR who was assassinated in 2006—remains pending.

Russian legislation provides for the tracking, seizure and forfeiture of all criminal proceeds, not just those linked to narcotics trafficking. Russian law also provides law enforcement bodies the authority to use investigative techniques such as search, seizure, and the identification, freezing, seizing, and confiscation of funds or other assets. Authorities can compel individuals to produce documents related to criminal activity, including money laundering. Investigators and prosecutors can apply to the court to freeze or seize property obtained as the result of crime, although there are some exceptions in the law restricting seizure of property identified as a primary residence. Law enforcement agencies have the power to identify and trace property that is, or may become, subject to confiscation or is suspected of being the proceeds of crime or terrorist financing. According to the AML/CTF law, financial institutions must freeze transactions suspected of involvement in terrorism finance for up to two days and report the transaction to the FIU. The FSFM may extend the freeze by an additional five days. A court order is required to extend the freeze beyond seven days.

In accordance with its international agreements, Russia recognizes rulings of foreign courts relating to the confiscation of proceeds from crime within its territory and can transfer confiscated proceeds of crime to the foreign state whose court issued the confiscation order. However, Russian law still does not provide for the seizure of instruments of crime. Authorities can seize businesses only if they can demonstrate that the businesses were acquired with criminal proceeds. Legitimate businesses cannot be seized solely on the basis that they were used to facilitate the commission of a crime.

Russia's Presidential Administration as well as law enforcement agencies have, however, expressed concern about ineffective implementation of Russia's confiscation laws. The government has proposed amendments that are currently under review by the Duma These amendments would facilitate the identification and seizure of criminal instrumentalities and proceeds. Russian law enforcement has adequate police powers to trace assets, and the law permits confiscation of assets. However, most Russian law enforcement personnel reportedly lack experience and expertise in these areas.

The Russian Federation has enacted several pieces of legislation and issued executive orders to strengthen its ability to fight terrorism. The decree entitled "On Measures to Implement the UN

Security Council Resolution (UNSCR) No. 1373 of September 28, 2001" introduces criminal liability for intentionally providing or collecting assets for terrorist use and instructs relevant agencies to seize assets of terrorist groups. Article 205.1 of the criminal code, enacted in October 2002, criminalizes terrorist financing. Banks can freeze assets suspected of involvement in terrorism finance immediately pursuant to UNSCR 1373.

The FSFM reports that it is monitoring 1,300 entities suspected of financing terrorism, including over 900 Russian citizens, 170 Russian organizations, and over 200 foreign entities. The Russian Government maintains a list of domestic and international organizations and individuals involved in extremist activities or terrorism. This list is distributed to all institutions subject to the AML/CTF law and is used by law enforcement agencies to target and seize assets. Russian authorities rely on five sources of information to compile the designated entities list: a) international organizations, such as the UN 1267 Sanctions Committee lists; b) Russian court decisions; c) designations made by the Prosecutor General; d) Ministry of Interior investigations (provided that subsequent court decisions do not reverse or dismiss the investigation's findings); and e) bilateral agreements to designate entities mutually determined to be involved in extremist or terrorist activity. At the request of the General Procuracy, the Russian Supreme Court has, to date, authorized an official list of 17 terrorist organizations.

The United States and Russia signed a Mutual Legal Assistance Treaty in 1999, which entered into force on January 31, 2002. Although Russia has assisted the U.S. in investigating cases involving terrorist financing, Russia and the U.S. continue to differ about the purpose of the UN 1267 Sanctions Committee's designation process. These political differences have hampered bilateral cooperation in this forum. U.S. law enforcement agencies exchange operational information with their Russian counterparts on a regular basis. The close cooperation between Russian and U.S. agencies has continued and strengthened in 2007.

Russia is a member of the Financial Action Task Force (FATF) and underwent its third mutual evaluation during the fourth quarter of 2007. The FATF's mutual evaluation report (MER) is expected to be released in June 2008. Russia is also a member of two FATF-style regional bodies (FSRBs). It is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and the Eurasian Group on Combating Legalization of Proceeds from Crime and Terrorist Financing (EAG), of which it was a co-founder. The EAG Secretariat is located in Moscow. The FSFM has established the International Training and Methodological Center of Financial Monitoring (ITMCFM) that exists to provide technical assistance, primarily in the form of staff training for FIUs and other interested ministries and agencies involved in AML/CTF efforts. The ITMCFM also conducts research on AML/CTF issues. As Chair of the EAG, Russia's FIU continues to play a strong leadership role in the region. The FSFM is a member of the Egmont Group The FSFM has signed cooperation agreements with the Financial Intelligence Units (FIUs) of 24 countries, including the United States.

Russia ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime in January 2001. Russia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption.

Through aggressive enactment and implementation of comprehensive AML/CTF legislation, Russia has established legal and enforcement frameworks to deal with money laundering and terrorist financing. Russia has also contributed to improving the region's capacity for countering money laundering and terrorist financing. Nevertheless, serious vulnerabilities remain. Russia is home to some of the world's most sophisticated perpetrators of fraud and money laundering, who rely heavily on electronic and Internet-related means. Russia should improve federal oversight of shell companies and scrutinize more closely those banks that do not carry out traditional banking activities. To prevent

endemic corruption and deficiencies in the business environment from undermining Russia's efforts to establish a well-functioning anti-money laundering and counter-terrorism finance regime, Russia should strive to stamp out official corruption, and to increase transparency in the financial sector and the corporate environment. Russia should also commit adequate resources to its regulatory and law enforcement entities to enable them to fulfill their responsibilities. Russia should work to increase the effectiveness of its asset forfeiture laws and their implementation including enacting legislation providing for the seizure of instruments, in addition to the proceeds, of criminal activity. Finally, Russia should continue to play a leadership role through sustained involvement in the regional and international bodies focusing on AML/CTF regime implementation.

Samoa

Samoa does not have major organized crime, fraud, or drug problems. The most common crimes that generate revenue within the jurisdiction are primarily the result of low-level fraud and theft. However, according to law enforcement intelligence sources, criminal organizations based in Hawaii and California are involved in the trafficking of cocaine, MDMA and crystal methamphetamine into the island nations including Samoa. Additionally, South American and Australian based organizations use the South Pacific islands as transhipment locations for cocaine being shipped from South America into Australia and New Zealand

The domestic banking system is very small, and there is relatively little risk of significant money laundering derived from domestic sources. Samoa's offshore banking sector is relatively small. The Government of Samoa (GOS) initially enacted the Money Laundering Prevention Act (the Act) in 2000 that was repealed and replaced by the new Money Laundering Prevention Act 2007. This law criminalizes money laundering associated with numerous crimes sets measures for the prevention of money laundering and requires related financial supervision. Under the Act, a conviction for a money laundering offense is punishable by a fine not to exceed Western Samoa Tala (WST) one million (approximately U.S. $354,000), a term of imprisonment not to exceed seven years, or both. This penalty is not found in the 2007 Act itself but derives from the separate Proceeds of Crime Act of 2007, which includes specific penalties for money laundering.

The Act requires financial institutions to report transactions considered suspicious to the Samoa Financial Intelligence Unit (FIU) established by the Money Laundering Prevention Authority presently under the auspices of the Governor of the Central Bank. The FIU receives and analyses disclosures from either a local financial or government institution or agency (either domestic or of a foreign state). If it establishes reasonable grounds to suspect that a transaction is suspicious, it may disclose the report to an appropriate local or foreign government or law enforcement agency. A Money Laundering Prevention Task Force (MLPTF) is established under the new Act to advise or make recommendations to the MLPA. More importantly, the MLPTF is tasked to ensure close liaison and cooperation and coordination between various GOS departments and corporations. In 2003, Samoa established under the authority of the Ministry of the Prime Minister an independent and permanent Transnational Crime Unit (TCU). The TCU is staffed by personnel from the Samoa Police Service, Immigration Division of the Ministry of the Prime Minister and Division of Customs. The TCU is responsible for intelligence gathering and analysis and investigating transnational crimes, including money laundering, terrorist financing and the smuggling of narcotics and people.

The Act requires financial institutions to establish and maintain with appropriate backup or recovery all business transactions records and correspondence records for a minimum of five years, and to identify and verify a customer's identity when establishing a business relationship; when there is a suspicion of a Money Laundering offense or terrorist financing; or when there is doubt about the veracity or adequacy of the customer identification, or verification, documentation, or information previously obtained.

Section 31 of the Act requires that all financial institutions have an obligation to appoint a compliance officer responsible for ensuring compliance with the Act, and to establish and maintain procedures and systems to implement customer identification requirements, implement record keeping, retention, and reporting requirements and to make its officers and employees aware of procedures, policies and audit systems. Each financial institution is also required to train its officers, employees and agents to recognize suspicious transactions. A financial institution required to be audited must incorporate compliance with the MLPA 2007 as part of its audit to be confirmed by the auditor. Currency reporting at the border requires any person leaving or entering Samoa with more than $20,000 or other prescribed amount in cash or negotiable bearer instruments (in Samoan currency or equivalent foreign currency) either on their person or in their personal luggage to report this to the Financial Intelligence Unit.

The Act removes secrecy protections and prohibitions on the disclosure of relevant information. Moreover, it provides protection from both civil and criminal liability for disclosures related to potential money laundering offenses to the competent authority.

The Central Bank of Samoa, the Samoa International Finance Authority (SIFA) and the MLPA regulate the financial system. There are four locally incorporated commercial banks, supervised by the Central Bank. The SIFA has responsibility for regulation and administration of the offshore sector. There are no casinos, but two local lotteries are in operation.

Samoa is an offshore financial jurisdiction with six offshore banks licensed. For entities registered or licensed under the various Offshore Finance Centre Acts, there are no currency or exchange controls or regulations, and no foreign exchange levies payable on foreign currency transactions. No income tax or other duties, nor any other direct or indirect tax or stamp duty is payable by registered/licensed entities. In addition to the six offshore banks, Samoa currently has 25,383 international business corporations (IBCs) three international insurance companies, seven trustee companies, and 182 international trusts. Section 19 of the International Banking Act requires the directors and Chief Executive to be “fit and proper” and prohibits any person from applying to be a director, manager, or officer of an offshore bank who has been sentenced for an offense involving dishonesty. The prohibition is also reflected in the application forms and personal questionnaire that are completed by prospective applicants that detail the licensing requirements for offshore banks. The application forms list the required supporting documentation for proposed directors of a bank. These include references from a lawyer, accountant, and a bank, police clearances, curriculum vitae, certified copies of passports, and personal statements of assets and liabilities (if also a beneficial owner). The Inspector of International Banks must be satisfied with all supporting documentation that a proposed director is “fit and proper” in terms of his integrity, competence and solvency, which is defined in section 3 of the Act.

International cooperation can occur in several ways under the provisions of three pieces of legislation: the Money Laundering Prevention Act 2007, the Proceeds of Crime Act 2007, and Mutual Assistance in Criminal Matters Act 2007. All cooperation under the MLPA is through the Financial Intelligence Unit (FIU) under the new Money Laundering Prevention Act 2007, which allows exchange of information not only on a national but also on an international basis between the FIU and other domestic law enforcement and regulatory agencies. Under the Proceeds of Crime Act 2007, a foreign State can request assistance to issue a restraining order in respect of a foreign serious offense. The Attorney General under the Mutual Assistance in Criminal Matters Act 2007 can authorize the giving of assistance to a foreign state. Assistance to a foreign state can be in the form of locating or identifying persons or providing evidence or producing documents or other articles in Samoa. In 2002, Samoa enacted the Prevention and Suppression of Terrorism Act. The Act defines and criminalizes terrorist offenses, including offenses dealing specifically with the financing of terrorist activities. The combined effect of the Money Laundering Prevention Act of 2007 and the Prevention and Suppression

of Terrorism Act of 2002 is to make it an offense for any person to provide assistance to a criminal to obtain, conceal, retain or invest funds or to finance or facilitate the financing of terrorism.

Samoa is a member of the Asia/Pacific Group on Money Laundering and the Pacific Islands Forum. Samoa hosted the annual plenary of the Pacific Islands Forum in August 2004. Samoa has not signed the 1988 UN Drug Convention or the UN Convention against Transnational Organized Crime. Samoa became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. However there is no information to indicate whether Samoa circulates either the UNSCR 1267 or the U.S. lists of designated terrorist entities.

The Financial Intelligence Unit (FIU) within the Central Bank has continued to strengthen its anti-money laundering regime as evident in the new Money Laundering Prevention Act 2007. The new Act is explicitly mandates that all financial institutions conduct customer due diligence and prohibit any transactions where there is no satisfactory evidence of a customers identity. A financial institution is obliged to keep records of all business transaction records and related correspondence, records of a customer's identity, and of all reports made to the FIU, and any enquiries made to it by the FIU on money laundering and terrorist financing matters. Anonymous accounts are strictly prohibited, and transactions are required to be monitored by financial institutions. The scope of record keeping by financial institutions (like banks and money transmission service providers) is extended to include accurate originator information and other related messages made via electronic fund transfers.

The Government of Samoa (GOS) has made progress in developing its anti-money laundering/counter-terrorist finance regime in 2007 by enacting the Money Laundering Prevention Act. The GOS should ensure that financial institutions submit suspicious transaction reports (STRs) to the FIU and that the FIU forwards any STR worthy of investigation to law enforcement for possible prosecution. The GOS should effectively regulate its offshore financial sector by ensuring that the names of the actual beneficial owners of international business companies and banks are on a registry accessible to law enforcement. The GOS should ensure that the UNSCR 1267 Sanctions Committee Consolidated and U.S. lists are circulated and an effective asset forfeiture regime is established and implemented. The GOS should adhere to the FATF's 9 Special Recommendations on Terrorist Financing. In particular, Samoa should take steps to implement Special Recommendation IX on cash couriers and ensure that its entry and exit points are not used for either the transhipment of narcotics, the sale of imported narcotics, or the funds derived from either illicit activity.

Saudi Arabia

Saudi Arabia is a growing financial center in the Gulf Region of the Middle East. There is little known narcotics related money laundering in the Kingdom. Saudi officials acknowledge difficulty in detecting terrorist financing due to the abundance of cash funds in the country. All eleven commercial banks in Saudi Arabia operate as standard "western-style" financial institutions and all banks operate under the supervision of the central bank, Saudi Arabian Monetary Agency (SAMA). Saudi Arabia is not an offshore financial center. There are no free zones for manufacturing, although there are bonded transit areas for the trans-shipment of goods not entering the country. There was no significant increase in financial crimes during 2007, although the proceeds of crime from stolen cars and counterfeit goods are substantial. A definitive determination is hard to make because of the absence of official criminal statistics.

Saudi donors and unregulated charities have been a major source of financing to extremist and terrorist groups over the past 25 years. However, the Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission") found no evidence that either the Saudi Government, as an institution, or senior Saudi Government officials individually, funded al-Qaida. Following the al-Qaida bombings in Riyadh on May 12, 2003, the Saudi Arabian government (SAG) has taken significant steps to counteract terrorist financing.

In 2003, Saudi Arabia approved a new Anti-Money Laundering Law that for the first time contains criminal penalties for money laundering and terrorist financing. The law bans conducting commercial or financial transactions with persons or entities using pseudonyms or acting anonymously; requires financial institutions to maintain records of transactions for a minimum of ten years and adopt precautionary measures to uncover and prevent money laundering operations; requires banks and financial institutions to report suspicious transactions; authorizes government prosecutors to investigate money laundering and terrorist financing; and allows for the exchange of information and judicial actions against money laundering operations with countries with which Saudi Arabia has official agreements.

SAMA guidelines generally correspond to the Financial Action Task Force (FATF) 40 Recommendations and the Nine Special Recommendations on Terrorist Financing. On May 27, 2003, SAMA issued updated anti-money laundering and counter-terrorist finance guidelines for the Saudi banking system. The guidelines require that banks have mechanisms to monitor all types of "Specially Designated Nationals" as listed by SAMA; that fund transfer systems be capable of detecting specially designated nationals; banks strictly adhere to SAMA circulars on opening accounts and dealing with charity and donation collection; and the banks be able to provide the remitter's identifying information for all outgoing transfers. The guidelines also require banks to use software to profile customers to detect unusual transaction patterns; establish a monitoring threshold of 100,000 Saudi Riyals (U.S. $26,667); and develop internal control systems and compliance systems. SAMA also issued "know your customer" guidelines, requiring banks to freeze accounts of customers who do not provide updated account information. Saudi law prohibits nonresident individuals or corporations from opening bank accounts in Saudi Arabia without the specific authorization of SAMA. There are no bank secrecy laws that prevent financial institutions from reporting client and ownership information to bank supervisors and law enforcement authorities. The SAG provides anti-money laundering training for bank employees, prosecutors, judges, customs officers and other government officials.

In 2003, the SAG established an anti-money laundering unit in SAMA, and in 2005 the SAG established the Saudi Arabia Financial Investigation Unit (SAFIU), which acts as the country's financial intelligence unit (FIU) within the Ministry of Interior. Saudi banks are required to have anti-money laundering units with specialized staff to work with SAMA, the SAFIU and law enforcement authorities. All banks are also required to file suspicious transaction reports (STR) with the SAFIU. The SAFIU collects and analyzes STRs and other available information and makes referrals to the Bureau of Investigation and Prosecution, the Mabahith (the Saudi Security Service), and the Public Security Agency for further investigation and prosecution. The SAFIU is staffed by officers from the Mabahith and SAMA. The SAFIU is not yet a member of the Egmont Group of FIUs.

Hawala transactions outside banks and licensed moneychangers are illegal in Saudi Arabia. Some instances of money laundering and terrorist finance in Saudi Arabia have involved hawala. To help counteract the appeal of hawala, particularly to many of the approximately six million expatriates living in Saudi Arabia, Saudi banks have taken the initiative to create fast, efficient, high quality, and cost-effective fund transfer systems that have proven capable of attracting customers accustomed to using hawala. An important advantage for the authorities in combating potential money laundering and terrorist financing in this system is that the senders and recipients of fund transfers through this formal financial sector are clearly identified. In an effort to further regulate the more than $16 billion in annual remittances that leave Saudi Arabia, SAMA consolidated the eight largest moneychangers into a single bank, Bank Al-Bilad, in 2005.

In June 2007 the SAG enacted stricter regulations on the cross-border movement of money, precious metals, and jewels. Money and gold in excess of U.S. $16,000 must be declared upon entry and exit from the country using official Customs forms.

Contributions to charities in Saudi Arabia usually consist of Zakat, which refers to an Islamic religious duty with specified humanitarian purposes. In 2002, Saudi Arabia announced its intention to establish a National Commission for Relief and Charitable Work Abroad (aka the Charities Commission), a mechanism that would oversee all private charitable activities abroad. Until the Charities Commission is established, no Saudi charity can send funds abroad. As of October 2007, the proposal was still under review by Saudi officials. As required by regulations in effect for over 20 years, domestic charities in Saudi Arabia are licensed, registered audited, and supervised by the Ministry of Social Affairs. The Ministry has engaged outside accounting firms to perform annual audits of charities' financial records and has established an electronic database to track the operations of such charities. New banking rules implemented in 2003 that apply to all charities include stipulations that they can be only opened in Saudi Riyals; must adhere to enhanced identification requirements; must utilize one main consolidated account; and must make payments only by checks payable to the first beneficiary, which then must be deposited in a Saudi bank. Regulations also forbid charities from using ATM and credit cards for charitable purposes, and making money transfers outside of Saudi Arabia. According to SAG officials, these regulations apply to international charities as well and are actively enforced.

Saudi Arabia participates in the activities of the FATF through its membership in the Gulf Cooperation Council (GCC). In July 2004, reporting on the results of a mutual evaluation conducted in September 2003, the FATF concluded that the framework of Saudi Arabia's anti-money laundering regime met FATF recommendations for combating money laundering and financing of terrorism, but noted the need to implement these new laws and regulations. Saudi Arabia also supported the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF) in November 2004 and was one of MENAFATF's original charter signatories.

It is the policy and practice of the SAG to comply with obligations under UN Security Council resolutions (UNSCR) on terrorist financing. SAMA circulates to all financial institutions under its supervision the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list.

The SAG is a party the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The SAG has signed but has not yet ratified the UN Convention against Corruption. In August 2007, Saudi Arabia ratified the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Saudi Arabia is taking steps towards enforcing its anti-money laundering/counter-terrorist finance laws, regulations, and guidelines. However, it needs to take concrete steps to establish the Charities Commission and to enhance its oversight and control of Saudi charities with overseas operations. Charitable donations in the form of gold, precious stones and other gifts should be scrutinized. There is still an over-reliance on suspicious transaction reporting to generate money laundering investigations. Law enforcement agencies should take the initiative and proactively generate leads and investigations, and be able to follow the financial trails wherever they lead. The public dissemination of statistics regarding predicate offenses and money laundering prosecutions would facilitate the evaluation and design of enhancements to the judicial aspects of its AML system. The SAG should ratify the UN Convention against Corruption.

Senegal

A regional financial center with a largely cash-based economy, Senegal is vulnerable to money laundering. Reportedly, most money laundering involves domestically generated proceeds from corruption and embezzlement. Recent arrests of opposition politicians, journalists, and a corruption scandal that resulted in the early retirement, rather than prosecution of the implicated judges, illustrate these vulnerabilities. There is also concern that criminal figures launder and invest their own and their organization's proceeds from the growing West Africa narcotics trade. There is also evidence of

increasing criminal activity by foreigners, such as narcotics trafficking by Latin American groups and illegal immigrant trafficking involving Pakistanis.

Dakar's active real estate market is largely financed by cash and property ownership and transfer is nontransparent. The building boom and high property prices suggest that an increasing amount of funds with an uncertain origin circulates in Senegal. Trade-based money laundering (TBML) is centered in the region of Touba, a largely autonomous and unregulated free-trade zone under the jurisdiction of the Mouride religious authority. Touba reportedly receives between U.S. $550 and $800 million per year in funds repatriated by networks of Senegalese traders and vendors abroad. Other areas of concern include cash, gold and gems transiting Senegal's airport and porous borders, as well as real estate investment in the Petite Cote south of Dakar.

Seventeen commercial banks operate alongside thriving micro credit and informal sectors. The Government of Senegal (GOS) is attempting to discourage its civil servants from using cash by depositing salaries into formal bank accounts, and the Banking Association has begun a publicity campaign to encourage the populace to use the formal banking system. Western Union, Money Gram and Money Express, associated with banks, compete with Senegal's widespread informal remittance systems, including hawala networks and the use of cash couriers. Small-scale, unregulated and nonlicensed currency exchange operations are also common, especially outside urban centers. The Banque de l'Habitat du Senegal (BHS), a Senegalese bank, has affiliates licensed as money remitters in the United States. New York State authorities have brought an enforcement action against BHS New York for failing to comply with anti-money laundering (AML) regulations.

The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the eight countries in the West African Economic and Monetary Union (WAEMU or UEMOA), including Senegal, and uses the CFA franc currency. The Commission Bancaire, the BCEAO division responsible for bank inspections, is based in Abidjan. However, it does not execute a full AML examination during its standard banking compliance examinations. Senegal has no offshore banking sector.

Senegal's currency control and reporting requirements are not uniform and are reportedly laxly enforced. There is no publicity about currency declaration requirements at major points of entry. Nonresidents on entry must declare any currency they are transporting from outside the "zone franc" greater than one million CFA (approximately U.S. $2,000). They must also declare monetary instruments denominated in cash in any amount. When departing Senegal, nonresidents must declare any currency from outside the franc zone greater than approximately U.S. $1,000 as well as all monetary instruments from foreign entities. The law does not require residents to declare currency on entry; on exit, they must declare amounts any foreign currency and any monetary instruments greater than approximately U.S. $4,000. All declarations must be in writing. Customs authorities are primarily concerned with the importation of dutiable goods. Because land border crossings are patrolled by other authorities with differing mandates, currency control is not a priority.

The legal basis for Senegal's anti-money laundering/counter-terrorist financing (AML/CTF) framework is Loi Uniforme Relative a Lutte Contre le Blanchiment de Capiteaux No. 2004-09 of February 6, 2004, or the Anti-Money Laundering Uniform Law (Uniform Law). As the common law passed by the members of l'UEMOA/WAEMU, all member states are bound to enact and implement the legislation. Among the union, Senegal is the first country to have the legal framework in place. Senegal has an "all crimes" approach to money laundering. Self launderers may be prosecuted and it is not necessary to have a conviction for the predicate offense. Intent may be inferred from objective factual circumstances. Criminal liability applies to all legal persons as well as natural persons.

The new legislation meets many international standards with respect to money laundering, and eclipses them in some areas such as with regard to the microfinance sector, but does not comply with all Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations.

The legislation also lacks certain compliance provisions for nonfinancial institutions. Although Senegal has not passed a CTF law, the penal code was amended in March 2007 to incorporate the United National Security Council Resolution (UNSCR) requirements for terrorist financing. In July 2007, l'UEMOA/WAEMU released guidance on terrorist financing for the sub-region alongside Directive No. 04/2007/CM/UEMOA, obliging member states to pass domestic CTF legislation.

The law requires banks and other financial institutions to know their customers and record and report the identity of any engaged in significant transactions, including the recording of large currency transactions. Banks monitor and record the origin of any deposit higher than 5 million CFA (approximately U.S. $10,000) for a single individual account and 20 to 50 million CFA (approximately U.S. $40,000 to 100,000) for any business account. Commercial banks in Senegal are improving their internal controls and enhancing their "know your customer" (KYC) requirements. The law also contains safe harbor provisions for individuals who file reports.

Cellule Nationale de Traitement des Informations Financiers (CENTIF), Senegal's financial intelligence unit (FIU) became operational in August 2005. The FIU currently has a staff of 27, including six appointed members: the President of the FIU, who by law is chosen from the Ministry of Economy and Finance, and five others detailed from the Customs Service, the BCEAO, the Judicial Police, and the Ministry of Justice. Senegal's FIU is working to improve its operational abilities and is raising the awareness of the threat of money laundering in Senegal. CENTIF has provided outreach and training for obliged entities to familiarize them with their requirements and to improve the quality and variety of STRs that the FIU receives. Senegal's FIU has applied for membership in the Egmont Group.

The police, gendarmerie and Ministry of Justice's judicial police are technically responsible for investigating money laundering and terrorist financing. However, in reality, CENTIF reportedly retains its information and tasks law enforcement entities to investigate or retrieve information for its cases. CENTIF reportedly does not share or disseminate its information or financial intelligence to law enforcement. In 2007, CENTIF received 71 suspicious transaction reports (STRs), mostly from banks, and referred 11 cases to the Prosecutor General who, in turn, passed the cases directly to the investigating judge. No cases have concluded, although authorities have made one arrest. Official statistics regarding the prosecution of financial crimes are unavailable. There is one known conviction for money laundering since 2005. The conviction led to the confiscation of a private villa.

The Uniform Law provides for the freezing, seizing, and confiscation of property by judicial order. In addition, the FIU can order the suspension of the execution of a financial transaction for 48 hours. The BCEAO can also order the freezing of funds held by banks. The Uniform Law allows explicitly for criminal forfeiture. There is no provision for civil forfeiture.

The BCEAO has released a Directive against Terrorist Financing. Member states must enact a law against terrorist financing, which is a Uniform Law to be adopted by all WAEMU/UEMOA members parallel to the AML law. Like the AML law, the terrorist financing law is a penal law. Each national assembly must enact enabling legislation to adopt the new terrorist finance law. The FATF-style regional body (FSRB) for the 15 members of the Economic Community of Western African States (ECOWAS) known as the Intergovernmental Action Group Against Money Laundering in West Africa (GIABA) has also drafted a uniform law, which it hopes that all of its member states will enact. Senegal is a member of this body, which evaluated Senegal in 2007.

The BCEAO and the FIU circulate the UN 1267 Sanctions Committee consolidated list to commercial financial institutions. To date, no entity has been identified. The WAEMU/UEMOA Council of Ministers issued a directive in September 2002 requiring banks to freeze the assets of any entities designated by the Sanctions Committee.

Senegal has entered into bilateral criminal mutual assistance agreements with France, Tunisia, Morocco, Mali, The Gambia, Guinea Bissau, and Cape Verde. Multilateral ECOWAS treaties address extradition and legal assistance among the member countries. Under the Uniform Law, the FIU may share information freely with other WAEMU/UEMOA FIUs. However, Senegal has the only operational FIU within this community. CENTIF has signed a Memorandum of Understanding (MOU) for information exchange with the FIUs of Belgium, Nigeria, Algeria and Lebanon, and is working on other accords. CENTIF is open to information exchange on a reciprocity basis and shares information with FIUs of the Egmont group even without signed MOUs. The Senegalese government and law enforcement agencies are generally willing to cooperate with United States law enforcement agencies. The Government of Senegal (GOS) has also worked with INTERPOL, Spanish, and Italian authorities on international anti-crime operations.

Senegal is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the 1999 UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. In 2007, Senegal was ranked 71 out of 180 countries in Transparency International's Corruption Perceptions Index.

The Government of Senegal should continue to work with its partners in WAEMU/UEMOA and ECOWAS to establish a comprehensive anti-money laundering and counter-terrorist financing regime. Senegal should work on achieving transparency in its financial and real estate sectors, and continue to encourage the populace to use the formal banking system, steering them away from cash transactions. Senegal should increase the frequency and effectiveness of financial reviews and audits and continue to battle corruption. Senegal should lead its regional partners and establish better uniform control of cross-border flow of currency and other bearer-negotiable instruments for both residents and nonresidents. Senegalese law enforcement and customs authorities need to develop their expertise in identifying and investigating both traditional money laundering and money laundering within the informal economy. CENTIF should perform more outreach for obliged nonbank financial institutions to ensure a better understanding of STRs, when to file them and the information they should contain. CENTIF, law enforcement and Ministry of Justice authorities should work together to coordinate roles and responsibilities with regard to case investigation and assembly, and develop a deeper interagency understanding of money laundering and terrorist financing. Senegal should amend its AML legislation to address the remaining shortcomings, and criminalize terrorist financing.

Serbia

Serbia is not a regional financial center. At the crossroads of Europe and on the major trade corridor known as the "Balkan Route," Serbia confronts narcotics trafficking, smuggling of persons, drugs, weapons and pirated goods, money laundering, and other criminal activities. Serbia continues to be a significant black market for smuggled goods. Illegal proceeds are generated from drug trafficking, corruption, tax evasion and organized crime, as well as other types of crimes. Proceeds from illegal activities are invested in all forms of real estate. Trade-based money laundering (TBML), in the form of over- and under-invoicing, is commonly used to launder money.

A significant volume of money flows to Cyprus, reportedly as the payment for goods and services. The records maintained by various government entities vary significantly on the volume and value of imports from Cyprus. According to Government of the Republic of Serbia (GOS) officials, much of the difference is due to payments made to accounts in Cyprus for goods, such as Russian oil, that actually originate in a third jurisdiction.

Serbia's banking sector is more than 80 percent foreign-owned. There is no provision in the banking law that allows the establishment of offshore banks, shell companies or trusts. Serbia has 14 designated free trade zones, three of which are in operation. Serbia established the free trade zones to attract investment by providing tax-free areas to companies operating within them. These companies

are subject to the same supervision as other businesses in the country. Reportedly, there is no evidence of any alternative remittance systems operating in the country. Nor, reportedly, is there evidence of financial institutions engaging in currency transactions involving international narcotics trafficking proceeds.

Serbia's expanded definition of money laundering in the Penal Code broadens the scope of money laundering and aims to conform to international standards. This legislation also gives police and prosecutors more flexibility to pursue money laundering charges. The penalty for money laundering is a maximum of 10 years imprisonment. Under this law and attendant procedure, money laundering falls into the serious crime category and permits the use of Mutual Legal Assistance (MLA) procedures to obtain information from abroad.

Under Serbia's 2005 revised anti-money laundering law (AMLL) obliged entities must report suspicious transactions in any amount to the FIU. The law expands those sectors subject to reporting and record keeping requirements, adding attorneys, auditors, tax advisors and accountants, currency exchanges, insurance companies, casinos, securities brokers, dealers in high value goods, real estate agencies, and travel agents to those already required to comply with the AMLL provisions. The AMLL also expands the number of entities required to collect certain information and file currency transaction reports (CTRs) with the financial intelligence unit (FIU) on all cash transactions exceeding 15,000 euros (approximately U.S. $22,000), or the dinar equivalent. These entities must also retain records for five years. Financial institutions have realized significant improvement in their compliance, i.e., gathering and keeping records on customers and transactions. The AMLL requires obligated entities and individuals to monitor customers' accounts when they have a suspicion of money laundering, in addition to reporting to the FIU. Safe harbor provisions protect the entities with respect to their cooperation with law enforcement entities. The flow of information to the FIU has been steadily increasing, but not all entities are yet subject to implementing bylaws. The AMLL also eliminates a previous provision limiting prosecution to crimes committed within Serbian territory.

The Law on Foreign Exchange Operations, adopted in 2006, criminalizes the use of false or inflated invoices or documents to conceal the illicit transfer of funds out of the country. Serbia enacted this law in part to counter the perceived problem of import-export fraud and TBML. The Foreign Currency Inspectorate, part of the Ministry of Finance, is responsible for supervising import/export companies for compliance. The law also requires residents and nonresidents declare to Customs authorities all currency (foreign or dinars), or securities in amounts exceeding 5,000 euros (approximately U.S. $7,000) transported across the border.

The National Bank of Serbia (NBS) has supervisory authority over banks, currency exchanges, insurance and leasing companies. The NBS has issued regulations requiring banks to have compliance and know-your-customer (KYC) programs in place and to identify the beneficial owners of new accounts. In June 2006, the NBS expanded its customer identification and record keeping rules by adopting new regulations mandating enhanced due diligence procedures for certain high risk customers and politically exposed persons. The NBS is developing similar regulations for insurance companies. The Law on Banks includes a provision allowing the NBS to revoke a bank's license for activities related to, among other things, money laundering and terrorist financing, but the NBS has not yet used this revocation authority. Although the legal framework is in place, the NBS currently lacks the expertise needed for effective bank supervision. It is building these capacities through training and staff development.

The Securities Commission (SC) supervises broker-dealers and investment funds and monitors its obligors' compliance with the AML Laws. The SC is developing regulations to implement this authority. The Law on Investment Funds and the Law on Securities and Other Financial Instruments Market provide the SC with the authority to "examine" the source of investment capital during licensing procedures.

Serbia introduced a value-added tax (VAT) in 2005, and the full impact of refund fraud associated with the administration of the VAT is still not clear. Serbia's Tax Administration lacks the audit and investigative capacity or resources to adequately investigate the large number of suspicious transactions that are forwarded by Serbia's FIU. In addition, current tax law sets a low threshold for auditing purposes and has increased the burden on the Tax Administration. This has created a situation where criminals can spend and invest criminal proceeds freely with little fear of challenge by the tax authorities or other law enforcement agencies.

The Administration for the Prevention of Money Laundering (APML) serves as Serbia's FIU. The revised AMLL elevates the status of the FIU to that of an administrative body under the Ministry of Finance. This provides more autonomy for the agency to carry out its mandate, as well as additional resources. APML has its own line item operating budget. The FIU has developed listings of suspicious activity red flags for banks, currency exchange offices, insurance companies, securities brokers and leasing companies. APML also has the authority to freeze transactions for 72 hours. The FIU has signed memoranda of understanding (MOU) on the exchange of information with the NBS and Customs and is negotiating one with the Tax Administration.

From January 1, 2007 through November 19, 2007, the FIU received 1,572 suspicious transaction reports (STRs). Nearly all of the STRs received by the FIU have been filed by commercial banks. In 2007, the FIU opened 46 cases and referred 119 cases to law enforcement, investigative agencies, or the prosecutor's office for further investigation. A total of six criminal charges were submitted for money laundering charges in 2007. The most common predicate crime is "abuse of office".

In Serbia, it is difficult to convict a suspect of money laundering without a conviction for the predicate crime. In addition, courts are unwilling to accept circumstantial evidence to support money laundering or tax evasion charges. This hampers law enforcement and prosecutorial authorities from effectively using the anti-money laundering laws. The Suppression of Organized Crime Service (SOCS) of the Ministry of Interior houses a new Anti-Money Laundering Section to counter these challenges and better focus financial investigations.

The GOS has established the Permanent Coordinating Group (PCG), an interagency working group originally tasked with developing an implementation plan for the recommendations from the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures' (MONEYVAL), first-round evaluation. Subgroups have since worked to draft amendments to the AMLL that will bring the country's laws into compliance with the European Union's Third Directive on money laundering. The PCG and the working groups meet intermittently as required for completing specific tasks. However, the GOS still lacks consistent interagency coordination.

Under the law, the GOS can, upon conviction for an offense, confiscate assets derived from criminal activity or suspected of involvement in terrorist financing. The FIU enforces the United Nations Security Council Resolution (UNSCR) 1267 provisions regarding suspected terrorist lists. Although the FIU routinely provides the UN list of suspected terrorist organizations to the banking community, examinations for suspect accounts have revealed no evidence of terrorist financing within the banking system. The SOCS, the Special Anti-Terrorist Unit (SAJ), and Gendarmarie, in the Ministry of Interior, are the law enforcement bodies responsible for planning and conducting the most complex antiterrorism operations. SOCS cooperates and shares information with its counterpart agencies in all of the countries bordering Serbia. Although Serbia has criminalized the financing of terrorism, the freezing, seizing and confiscation of assets of terrorists in accordance with UN Security Council resolutions still lacks a legal basis, pending enactment of draft anti-terrorism finance legislation. This draft law on terrorist financing, now pending Parliamentary approval, will apply all provisions of the AMLL to terrorist financing, require reporting to the FIU of transactions suspected to be terrorist financing and will create mechanisms for freezing, seizing and confiscation of suspected terrorist assets based on UNSCR provisions.

Serbia has no laws governing its cooperation with other governments related to narcotics, terrorism, or terrorist financing. Bases for cooperation include participation in Interpol, bilateral cooperation agreements, and agreements concerning international legal assistance. There are no laws at all governing the sharing of confiscated assets with other countries.

Serbia does not have a mutual legal assistance arrangement with the United States, but information exchange via a letter rogatory is standard. The 1902 extradition treaty between the Republic of Serbia and the United States remains in force. The GOS has bilateral agreements on mutual legal assistance with 31 countries. As a member of MONEYVAL, Serbia will undergo a mutual evaluation in 2009. The FIU is a member of the Egmont Group and participates in information exchanges with counterpart FIUs including FinCEN. APML has also signed information sharing memoranda of understanding (MOUs) with eleven counterpart FIUs.

Serbia is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN Convention Against Transnational Organized Crime. The GOS also is a party to all 12 UN Conventions and protocols dealing with terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism. Domestic implementation procedures, however, do not provide the framework for full application of Convention provisions.

Serbia should continue to work toward eliminating the abuses of office and the culture of corruption that enables money laundering and financial crimes. The GOS should take action to realize and implement the pending legislative initiatives necessary for Serbia to fully comply with international standards. These include the laws providing for the liability of legal persons and regulations applying all requirements of the AMLL to covered nonbank financial institutions. The GOS should enforce anti-money laundering regulations pertaining to money service businesses and obligated nonfinancial business and professions. Serbia should complete its supervisory scheme, and enact binding implementing regulations for the insurance and securities sectors. The GOS should also enact legislation to establish a robust asset seizure and forfeiture regime and legislation providing for the sharing of seized assets. Serbia also needs to enact and implement legislation needed to comply with UN Security Council resolutions regarding the freezing, seizing and confiscation of suspected terrorist assets and to require suspicions of terrorist financing to be reported to the FIU. The National Bank and other supervisory bodies need to enhance their knowledge and receive additional staff. On an operational level, law enforcement needs audit and investigative capacity to investigate the STRs that the FIU disseminates. Prosecutors and judges also need a better understanding of money laundering and terrorist financing to ensure successful prosecutions. Rather than address specific tasks as an ad hoc group, the PCG should meet on a regular basis to discuss issues and projects, and work to improve interagency coordination in such areas as information sharing, record keeping, and statistics.

Seychelles

Seychelles is a not a major financial center. The existence of a developed offshore financial sector, however, makes the country vulnerable to money laundering. The Government of Seychelles (GOS), in efforts to diversify its economy beyond tourism, developed an offshore financial sector to increase foreign exchange earnings and actively markets itself as an offshore financial and business center that allows the registration of nonresident companies. As of September 2007, there were 34,000 registered international business companies (IBCs) and 160 trusts that pay no taxes in Seychelles, and are not subject to foreign exchange controls. The Seychelles International Business Authority (SIBA), a body with board members from both the government and the private sector, registers, licenses and regulates offshore activities. The SIBA licenses and registers agents who carry out due diligence tests when registering new companies in the Seychelles offshore sector. The SIBA also regulates activities of the Seychelles International Trade Zone.

In addition to IBCs and trusts, Seychelles permits offshore insurance companies, mutual funds, and offshore banking. In November 2006, the GOS established the Non-Bank Financial Services Authority, which is responsible for regulating these sectors under the Mutual Funds Act, the Securities Act, and the Insurance Act. Three offshore insurance companies have been licensed: one for captive insurance and two for general insurance. Seychelles has one offshore bank to date: Barclays Bank (Offshore Unit). The International Corporate Service Providers Act 2003, designed to regulate all activities of corporate and trustee service providers, entered into force in 2004.

In its 2007-2017 Strategic Plan, the Seychelles Government proposes to facilitate the development of the financial services sector as a third pillar of the economy. It plans to achieve this through actively promoting Seychelles as an internationally recognized offshore jurisdiction, with emphasis on IBCs, mutual funds, special license companies and insurance companies.

In 1996, the GOS enacted the Anti-Money Laundering Act (AMLA), which criminalized the laundering of funds from all serious crimes, required covered financial institutions and individuals to report suspicious transactions to the Central Bank, which now houses the financial intelligence unit (FIU), and established safe harbor protection for individuals and institutions filing such reports. The AMLA also imposed record keeping and customer identification requirements for financial institutions, and provided for the forfeiture of the proceeds of crime. In October 2004, the International Monetary Fund (IMF) released a report on its 2002 financial sector assessment of the Seychelles. The IMF report noted deficiencies in the AMLA and its implementation, and recommended closing existing loopholes as well as updating the AMLA to reflect current international standards and best practices.

In May 2006, the Anti-Money Laundering Act 2006 came into force. This new legislation replaces the AMLA of 1996 and addresses many of the deficiencies cited by the IMF report. Under the new AMLA, money laundering controls, including the obligation to submit suspicious transaction reports (STRs), are applied to the same financial intermediaries as under the 1996 law, as well as nonbank financial institutions, such as exchange houses, stock brokerages, insurance agencies, lawyers, notaries, accountants, and estate agents. Offshore banks are also explicitly covered. The gaming sector is also obliged to report. However, although Internet gaming is also obligated, the law does not state explicitly that offshore gaming is covered in an identical manner. No offshore casinos or Internet gaming sites have been licensed to operate. There is no cross-border currency-reporting requirement. The 2006 AMLA discusses record-keeping and institutional protocol requirements, sets a maximum delay of two working days to file an STR, criminalizes tipping off, and sets safe harbor provisions. The new law also requires reporting entities to take “reasonable measures” to ascertain the purpose of any transaction in excess of Seychelles rupees 100,000 (approximately U.S. $12,500), or of rupees 50,000 (approximately U.S. $6,250) in the case of cash transactions, and the origin and destination of the funds involved in the transaction. However, it leaves open exceptions for “an existing and regular business relationship with a person who has already produced satisfactory evidence of identity”; for “an occasional transaction under rupees 50,000” (approximately U.S. $6,250); and in other cases “as may be prescribed”.

Under the AMLA, anyone who engages directly or indirectly in a transaction involving money or other property (or who receives, possesses, conceals, disposes of, or brings into Seychelles any money or property) associated with a crime, knowing or having reasonable grounds to know that the money or property is derived from an illegal activity, is guilty of money laundering. In addition, anyone who aids, abets, procures, or conspires with another person to commit the crime, while knowing, or having reasonable grounds for knowing that the money was derived from an illegal activity, is likewise guilty of money laundering. Money laundering is sanctioned by imprisonment for up to fifteen years and/or rupees 3,000,000 (approximately U.S. $375,000) in penalties. While there have been 49 investigations, there have been no arrests or prosecutions for money laundering or terrorist financing since January 1,

2003. Of the 49 cases, eight were closed due to lack of evidence. In three cases, the suspects had left Seychelles, and in one case, the suspect had died. The remaining cases are still pending investigation.

The Financial Institutions Act of 2004 imposes more stringent rules on banking operations and brings the Seychelles' regulatory framework closer to compliance with international standards. The law aims to ensure greater transparency in financial transactions by regulating the financial activities of both domestic and offshore banks. Among other provisions, the law requires that banks change their auditors every five years. Auditors must notify the Central Bank if they uncover criminal activity such as money laundering in the course of an audit.

The Financial Intelligence Unit (FIU) was established under Section 16 of the 2006 AMLA. The FIU operates within the Central Bank of Seychelles. Prior to the establishment of the FIU, the Bank Supervision Division of the Central Bank of Seychelles performed the duties of the FIU. The FIU is the focal point for receiving, analyzing, and disseminating reports of transactions related to money laundering or the financing of terrorism to the appropriate law enforcement and supervisory agencies in Seychelles. To support these core functions, the FIU is authorized to collect information that it considers pertinent and is also empowered to request additional information from reporting entities, law enforcement and supervisory agencies. The law provides for the FIU to have a proactive targeting section to research trends and developments in money laundering and terrorist financing. The FIU also performs examinations of the reporting entities and, in concert with regulators, issues guidance related to customer identification, identification of suspicious transactions, and record keeping and reporting obligations. The FIU is currently in the process of updating a set of guidelines on anti-money laundering/counter-terrorist financing (AML/CTF), which dates back to 1998, for the reporting entities in accordance with the requirements of the AMLA 2006. In December 2006, the Seychelles Government established a National Anti-Money Laundering Committee to better coordinate the efforts of the various law enforcement agencies in combating financial crimes. The Committee is chaired by the FIU, and comprises representatives of the Police, the Attorney General's Office, Customs, Immigration, the Seychelles Licensing Authority, and the Seychelles International Business Authority.

The FIU cannot freeze or confiscate property but can get a court order to effect an asset freeze. The courts have the authority to freeze or confiscate money or property. Judges in the Supreme Court have the authority to restrain a target from moving or disposing of his or her assets, and will do so if a law enforcement officer requests it, provided that the Court is "satisfied that there are reasonable grounds" for doing so. The Court also has the authority to determine the length of time for the restraint order and the disposition of assets, should it become necessary. Should the target violate the order, he or she becomes subject to financial penalties. Law enforcement may seize property subject to this order to prevent property from being disposed of or moved contrary to the order. The Court also is authorized to order the forfeiture of assets.

In 2004, the GOS enacted the Prevention of Terrorism Bill. The legislation specifically recognizes the government's authority to identify, freeze, and seize terrorist finance-related assets. The 2006 AMLA also makes the legal requirements applicable to money laundering applicable to suspected terrorist financing transactions. Assets used in the commission of a terrorist act can be seized and legitimate businesses can be seized if used to launder drug money, support terrorist activity, or support other criminal activities. Both civil and criminal forfeiture are allowed under current legislation.

The Mutual Assistance in Criminal Matters Act of 1995 empowers the Seychelles Central Authority to provide assistance in connection with a request to conduct searches and seizures relating to serious offenses under the law of the requesting state. The Prevention of Terrorism Act extends the authority of the GOS to include the freezing and seizing of terrorism-related assets upon the request of a foreign state. To date, no such assets have been identified, frozen, or seized.

The Government of Seychelles is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. Seychelles underwent a mutual

evaluation review conducted by ESAAMLG in November 2006; however, the report has not been presented to the plenary body or finalized. The Seychelles is a party to the 1988 UN Drug Convention, the UN Convention Against Corruption, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. Seychelles circulates to relevant authorities the updated lists of names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224.

Seychelles should expand its anti-money laundering efforts by prohibiting bearer shares and clarifying the new legislation regarding the complete identification of beneficial owners. Seychelles should also clarify the legislation to state explicitly that all offshore activity is covered in the same manner and to the same degree as onshore. Seychelles should continue to work with its FIU to ensure it has the training and resources needed for outreach, analysis and dissemination, and comports with the membership criteria of the Egmont Group of FIUs. The GOS should also consider codifying the ability to freeze assets rather than issuing restraining orders, and develop a currency-reporting requirement for entry into its borders. Seychelles should participate more actively in ESAAMLG, and when the mutual evaluation report is finalized, address any further identified deficiencies.

Sierra Leone

Sierra Leone has a cash-based economy and is not a regional financial center. Government of Sierra Leone (GOSL) officials have reportedly stated that money laundering activities are pervasive, particularly in the diamond sector. Although there have been some attempts at tighter regulation, monitoring, and enforcement, in some areas significant diamond smuggling still exists. Loose oversight of financial institutions, weak regulations, pervasive corruption, and a widespread informal money-exchange and remittance system also work to create an atmosphere conducive to money laundering.

Former President Kabbah signed the Anti-Money Laundering Act (AMLA) in July 2005. The AMLA incorporates international standards, including setting safe harbor provisions, know your customer and identification of beneficial owner requirements, as well as mandatory five-year record-keeping for obliged entities. There is a currency reporting requirement for deposits larger than 25 million leones (approximately U.S. $8,330) and no minimum for suspicious transaction reporting. The law requires that international financial transfers over U.S. $10,000 use formal financial channels. The AMLA also institutes cross-border currency reporting requirements for cash or securities in excess of U.S. $10,000. The law designates the Governor of the Bank of Sierra Leone as the national Anti-Money Laundering Authority.

Subject to the AMLA reporting requirements are financial sector institutions such as depository and credit institutions, money transmission and remittance service centers, insurance brokers, investment banks and businesses including securities and stock brokerage houses, and currency exchange houses. The AMLA also imposes reporting requirements on designated nonfinancial businesses and professions such as casinos, realtors, dealers in precious metals and stones, notaries, legal practitioners, and accountants.

A financial intelligence unit (FIU) exists but lacks the capacity to effectively monitor and regulate financial institution operations, and in particular lacks the technological capability necessary to maintain databases, track actors and patterns, and monitor online transactions. Law enforcement and customs authorities have limited resources and lack training. There have reportedly been a small number of arrests under the AMLA but no convictions due to lack of capacity by police investigators and judicial authorities.

The AMLA empowers the courts to freeze assets for seventy-two hours if a suspect has been charged with money laundering or if a charge is imminent. Upon a conviction for money laundering, all property is treated as illicit proceeds and can be forfeited unless the defendant can prove that possession of some or all of the property was obtained through legal means. The AMLA also provides for mutual assistance and international cooperation.

In July 2006, the Bank of Sierra Leone hosted a training workshop with the United Nations Office on Drugs and Crime and Intergovernmental Group for Action Against Money Laundering (GIABA) on strategy development for anti-money laundering and combating financing of terrorism. Workshop participants recommended that the Bank of Sierra Leone draft a national anti-money laundering strategy and regulatory regime for reporting suspicious transactions to the FIU. Other recommendations focused on the FIU itself, including developing regulations for the operations of the FIU and establishing a system for the receipt, analysis, and dissemination of financial disclosures. Preparation of Sierra Leone's strategy paper has been delayed because new individuals are now involved with implementing the AMLA following the August 2007 parliamentary elections. As of late 2007, the Bank of Sierra Leone prepared the draft and recommended improving governance, setting up robust AMLA enforcement, reforming the financial sector and improving cooperation among local and regional institutions with regard to monitoring and reporting money laundering activities

Workshop participants also recommended creating a special unit comprised of four staff from the police—two from the organized crime unit and two from the counterterrorism unit—to work specifically on anti-money laundering issues. They also recommended creating protocols to improve the exchange of information between the government offices involved, including the Attorney General's Office, Sierra Leone Police, National Revenue Authority, and Anti-Corruption Commission.

Sierra Leone is member of the Inter-Governmental Action Group against Money Laundering and Terrorist Financing in West Africa (GIABA), a FATF-style regional body (FSRB). The mutual evaluation report for Sierra Leone was conducted by the World Bank and discussed at the GIABA Plenary in June 2007. The GOSL is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Sierra Leone is number 150 of 180 countries listed in Transparency International's 2007 Corruption Perception Index.

President Ernest Bai Koroma was elected in September 2007 and came into office pledging to fight corruption. If the President succeeds in creating an environment and legal framework to combat corruption, there will be a positive impact on the enforcement of laws against money laundering. Although the Government of Sierra Leone has passed anti-money laundering legislation, it remains to be effectively harmonized with other legislation relating to anti-money laundering and combating financing of terrorism, including the Anti-Corruption Act, National Drug Control Act, and Anti-Terrorism Act. The GOSL must increase the level of awareness of money laundering issues throughout the country and allocate the necessary resources to facilitate the development of its anti-money laundering and counter-terrorist financing regime. Sierra Leone needs to develop implementing regulations for its legislation, institute a reporting regime, and strengthen its FIU through both training and technical assistance. The Sierra Leonean FIU should work toward membership in the Egmont Group. The GOSL should ensure that its counter-terrorist financing measures adhere to international standards. The GOSL should work to ensure that the UNSCR 1267 Sanctions Committee's consolidated list is distributed to financial institutions regularly. It needs to ratify the UN Convention against Transnational Organized Crime. Sierra Leone should also continue its efforts to counter the smuggling of diamonds and take steps to combat corruption at all levels of commerce and government.

Singapore

As a significant international financial and investment center and, in particular, as a major offshore financial center, Singapore is vulnerable to money launderers. Stringent bank secrecy laws and the lack of routine currency reporting requirements make Singapore a potentially attractive destination for drug traffickers, transnational criminals, terrorist organizations and their supporters seeking to launder money, as well as for flight capital. Structural gaps remain in financial regulations that may hamper efforts to control these crimes. To address some of these deficiencies, Singapore is implementing legal and regulatory changes to better align itself with the Financial Action Task Force's (FATF) revised recommendations on anti-money laundering (AML) and counter-terrorist financing (CTF). FATF will conclude a Mutual Evaluation of Singapore's AML/CTF regime in February 2008.

Singapore amended the Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) in May 2006 to add 108 new categories to its "Schedule of Serious Offenses." The CDSA criminalizes the laundering of proceeds from narcotics transactions and other predicate offenses, including ones committed overseas that would be serious offenses if committed in Singapore. Included among the new offenses are crimes associated with terrorist financing, illicit arms trafficking, counterfeiting and piracy of products, environmental crime, computer crime, insider trading, and rigging commodities and securities markets. With an eye on Singapore's two new multibillion-dollar casinos slated to be operational in 2009, the list also addresses a number of gambling-related crimes. However, tax and fiscal offenses are still absent from the expanded list.

Singapore has a sizeable offshore financial sector. As of October 2007, there were 112 commercial banks in operation, including six local and 24 foreign-owned full banks, 42 offshore banks, and 40 wholesale banks. All offshore and wholesale banks are foreign-owned. Singapore does not permit shell banks in either the domestic or offshore sectors. The Monetary Authority of Singapore (MAS), a semi-autonomous entity under the Prime Minister's Office, serves as Singapore's central bank and financial sector regulator, particularly with respect to Singapore's AML/CTF efforts. MAS performs extensive prudential and regulatory checks on all applications for banking licenses, including whether banks are under adequate home country banking supervision. Banks must have clearly identified directors. Unlicensed banking transactions are illegal.

Singapore has increasingly become a center for offshore private banking and asset management. Total assets under management in Singapore grew 24 percent between 2005 and 2006 to Singapore $891 billion (U.S. $581 billion), according to MAS. Private wealth managers estimate that total private banking and asset management funds increased nearly 300 percent between 1998 and 2004.

Beginning in 2000, MAS began issuing a series of regulatory guidelines ("Notices") requiring banks to apply "know your customer" standards, adopt internal policies for staff compliance and cooperate with Singapore enforcement agencies on money laundering cases. Similar guidelines exist for securities dealers and other financial service providers. Banks must obtain documentation such as passports or identity cards from all individual customers to verify names, permanent contact addresses, dates of births and nationalities. Banks must also check the bona fides of company customers. The regulations specifically require that financial institutions obtain evidence of the identity of the beneficial owners of offshore companies or trusts. They also mandate specific record-keeping and reporting requirements, outline examples of suspicious transactions that should prompt reporting, and establish mandatory intra-company point-of-contact and staff training requirements. Similar guidelines and notices exist for finance companies, merchant banks, life insurers, brokers, securities dealers, investment advisors, futures brokers and advisors, trust companies, approved trustees, and money changers and remitters.

Singapore is in the process of revising its AML/CTF regulations for banks and other financial institutions. MAS issued new or revised AML/CTF regulations (in the form of "Notices" and "Guidelines") for banks and other financial institutions, most of which took effect March 1, 2007.

Affected institutions include banks, finance companies, merchant banks, moneychangers and remitters, life insurers, capital market intermediaries, and financial advisers. New reporting requirements for originator information on cross-border wire transfers took effect July 1. The relevant regulations further align certain parts of Singapore's AML/CTF regime more closely with FATF recommendations and specifically address CTF concerns for the first time. Among the recently implemented regulations are new provisions that would proscribe banks from entering into, or continuing, correspondent banking relationships with shell banks; clarify and strengthen procedures for customer due diligence (CDD), including adoption of a risk-based approach; mandate enhanced CDD for foreign politically exposed persons; and additional suspicious transaction reporting requirements. Effective November 1, 2007, Singapore increased the maximum penalty for financial institutions that fail to comply with AML/CTF regulations from Singapore $100,000 (U.S. $71,000) to Singapore $1 million (U.S. $714,000). The Act also empowers MAS to prosecute financial institution managers in cases where noncompliance is attributable to their consent, connivance or neglect. MAS is considering new regulations for holders of stored value facilities (SVF) to limit the risk of their use for illicit purposes.

In addition to banks that offer trust, nominee, and fiduciary accounts, Singapore has 12 trust companies. All banks and trust companies, whether domestic or offshore, are subject to the same regulation, record-keeping, and reporting requirements, including for money laundering and suspicious transactions. In August 2005, Singapore introduced regulations under the new Trust Companies Act (enacted in January 2005 to replace the Singapore Trustees Act) that mandated licensing of trust companies and MAS approval for appointments of managers and directors. MAS issued revised regulations that took effect April 1, 2007 that require approved trustees and trust companies to complete all mandated CDD procedures before they can establish relations with customers. Other financial institutions are allowed to establish relations with customers before completing all CDD-related measures.

Singapore amended its Moneylenders Act in April 2006 to require moneylenders under investigation to provide relevant information or documents. The Act imposes new penalties for giving false or misleading information and for obstructing entry and inspection of suspected premises. Singapore is considering further amendments to strengthen the Act's AML/CTF provisions.

Singapore has issued additional regulations and guidelines governing designated nonfinancial businesses and professions. The Internal Revenue Authority of Singapore issued AML/CTF guidelines for real estate agents in July 2007. The Law Society of Singapore in August 2007 amended its Legal Profession (Professional Conduct) Rules to strengthen its AML guidelines. Among its provisions, the new rules prohibit attorneys from acting on the behalf of anonymous clients to open or maintain bank accounts or to hold cash or cash instruments.

In April 2005, Singapore lifted its ban on casinos, paving the way for development of two integrated resorts scheduled to open in 2009. Combined total investment in the resorts is estimated to exceed U.S. $5 billion. In June 2006, Singapore implemented the Casino Control Act. The Act establishes the Casino Regulatory Authority of Singapore, which will administer the system of controls and procedures for casino operators, including certain cash reporting requirements. Internet gaming sites are illegal in Singapore.

A person who wishes to engage in for-profit business in Singapore, whether local or foreign, must register under the Companies Act. Every Singapore-incorporated company is required to have at least two directors, one of whom must be resident in Singapore, and one or more company secretaries who must be resident in Singapore. There is no nationality requirement. A company incorporated in Singapore has the same status and powers as a natural person. Bearer shares are not permitted.

Financial institutions must report suspicious transactions and positively identify customers engaging in large currency transactions and are required to maintain adequate records. Since November 1, 2007,

Singapore has begun requiring in-bound and out-bound travelers to report cash and bearer-negotiable instruments in excess of Singapore $30,000 (U.S. $20,675), in accordance with FATF Special Recommendation Nine. Violators are subject to a fine of up to Singapore $50,000 (U.S. $34,459) and/or a maximum prison sentence of three years.

The Singapore Police's Suspicious Transaction Reporting Office (STRO) has served as the country's Financial Intelligence Unit (FIU) since January 2000. Procedural regulations and bank secrecy laws limit STRO's ability to provide information relating to financial crimes. In December 2004, STRO concluded a Memorandum of Understanding (MOU) concerning the exchange of financial intelligence with its U.S. counterpart, FinCEN. STRO has also signed MOUs with counterparts in Australia, Belgium, Brazil, Canada, Greece, Hong Kong, Italy, Japan, and Mexico. To improve its suspicious transaction reporting, STRO has developed a computerized system to allow electronic online submission of STRs, as well as the dissemination of AML/CTF material. It plans to encourage all financial institutions and relevant professions to participate in this system.

Singapore is an important participant in the regional effort to stop terrorist financing in Southeast Asia. The Terrorism (Suppression of Financing) Act that took effect in January 2003 criminalizes terrorist financing, although the provisions of the Act are actually much broader. In addition to making it a criminal offense to deal with terrorist property (including financial assets), the Act criminalizes the provision or collection of any property (including financial assets) with the intention that the property be used (or having reasonable grounds to believe that the property will be used) to commit any terrorist act or for various terrorist purposes. The Act also provides that any person in Singapore, and every citizen of Singapore outside Singapore, who has information about any transaction or proposed transaction in respect of terrorist property, or who has information that he/she believes might be of material assistance in preventing a terrorist financing offense, must immediately inform the police. The Act gives the authorities the power to freeze and seize terrorist assets.

The International Monetary Fund/World Bank assessment of Singapore's financial sector published in April 2004 concluded that, because Singapore is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the country imposes few restrictions on intergovernmental terrorist financing-related mutual legal assistance, even in the absence of a Mutual Legal Assistance Treaty. However, the IMF urged Singapore to improve its mutual legal assistance for other offenses, noting serious limitations on assistance through the provision of bank records, search and seizure of evidence, restraints on the proceeds of crime, and the enforcement of foreign confiscation orders.

Based on regulations issued in 2002, MAS has broad powers to direct financial institutions to comply with international obligations related to terrorist financing. The regulations bar banks and financial institutions from providing resources and services of any kind that will benefit terrorists or terrorist financing. Financial institutions must notify the MAS immediately if they have in their possession, custody or control any property belonging to designated terrorists or any information on transactions involving terrorists' funds. The regulations apply to all branches and offices of any financial institutions incorporated in Singapore or incorporated outside of Singapore, but located in Singapore. The regulations are periodically updated to include names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

Singapore's approximately 757,000 foreign guest workers are the main users of alternative remittance systems. As of October 2007, there were 380 moneychangers and 92 remittance agents. All must be licensed and are subject to the Money-Changing and Remittance Businesses Act (MCRBA), which includes requirements for record keeping and the filing of suspicious transaction reports. Firms must submit a financial statement every three months and report the largest amount transmitted on a single day. They must also provide information concerning their business and overseas partners. Unlicensed informal networks, such as hawala, are illegal. In August 2005, Singapore amended the MCRBA to apply certain AML/CTF regulations to remittance licensees and moneychangers engaged in inward

remittance transactions. The Act eliminated sole proprietorships and required all remittance agents to incorporate under the Companies Act with a minimum paid-up capital of Singapore $100,000 (approximately U.S. $60,000). In July 2007, MAS issued regulations that require licensees to establish the identity of all customers. MAS must approve any non face-to-face transactions.

Singapore has five free trade zones (FTZs), four for seaborne cargo and one for airfreight, regulated under the Free Trade Zone Act. The FTZs may be used for storage, repackaging of import and export cargo, assembly and other manufacturing activities approved by the Director General of Customs in conjunction with the Ministry of Finance.

Charities in Singapore are subject to extensive government regulation, including close oversight and reporting requirements, and restrictions that limit the amount of funding that can be transferred out of Singapore. Singapore had a total of 1,900 registered charities as at end 2006. All charities must register with the Commissioner of Charities that reports to the Minister for Community Development, Youth and Sports. Charities must submit governing documents outlining their objectives and particulars of all trustees. The Commissioner of Charities has the power to investigate charities, search and seize records, restrict the transactions into which the charity can enter, suspend staff or trustees, and/or establish a scheme for the administration of the charity. Charities must keep detailed accounting records and retain them for at least seven years.

Changes to the Charities (Registration of Charities) Regulations that came into effect in May 2007 authorize the Commissioner to deregister charities deemed to be engaged in activities that run counter to the public interest. Singapore has also implemented tighter rules under the Charities Act that govern public fund-raising by charities, effective May 1, 2007. Charities authorized to receive tax-deductible donations are required to disclose the amount of funds raised in excess of Singapore $1 million (approximately U.S. $690,000), expenses incurred, and planned use of funds. Under the Charities (Fund-raising Appeals for Foreign Charitable Purposes) Regulations (1994), any charity or person that wishes to conduct or participate in any fund-raising for any foreign charitable purpose must apply for a permit. The applicant must demonstrate that at least 80 percent of the funds raised will be used in Singapore, although the Commissioner of Charities has discretion to allow for a lower percentage. Permit holders are subject to additional record-keeping and reporting requirements, including details on every item of expenditure, amounts transferred to persons outside Singapore, and names of recipients. The government issued 26 permits in 2006 and 18 permits as of November 2007 related to fundraising for foreign charitable purposes. There are no restrictions or direct reporting requirements on foreign donations to charities in Singapore.

To regulate law enforcement cooperation and facilitate information exchange, Singapore enacted the Mutual Assistance in Criminal Matters Act (MACMA) in March 2000. Parliament amended the MACMA in February 2006 to allow the government to respond to requests for assistance even in the absence of a bilateral treaty, MOU or other agreement with Singapore. The MACMA provides for international cooperation on any of the 292 predicate “serious offenses” listed under the CDSA. In November 2000, Singapore and the United States signed the Agreement Concerning the Investigation of Drug Trafficking Offenses and Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking (Drug Designation Agreement or DDA). This was the first agreement concluded pursuant to the MACMA. The DDA, which came into force in early 2001, facilitates the exchange of banking and corporate information on drug money laundering suspects and targets, including access to bank records. It also entails reciprocal honoring of seizure/forfeiture warrants. This agreement applies only to narcotics cases, and does not cover nonnarcotics-related money laundering, terrorist financing, or financial fraud.

In May 2003, Singapore issued a regulation pursuant to the MACMA and the Terrorism Act that enables the government to provide legal assistance to the United States and the United Kingdom in matters related to terrorist financing offenses. Singapore concluded mutual legal assistance agreements

with Hong Kong in 2003, India in 2005, and Laos in 2007. Singapore is a party to the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters along with Malaysia, Vietnam, Brunei, Cambodia, Indonesia, Laos, the Philippines, Thailand, and Burma. The treaty will come into effect after ratification by the respective governments. Singapore, Malaysia, Laos, Vietnam and Brunei have ratified thus far.

In addition to the UN International Convention for the Suppression of the Financing of Terrorism, Singapore is also party to the 1988 UN Drug Convention. In August 2007, Singapore also ratified the UN Convention against Transnational Organized Crime. Singapore has signed, but has not yet ratified, the UN Convention against Corruption. In addition to FATF, Singapore is a member of the Asia/Pacific Group (APG) on Money Laundering, the Egmont Group, and the Offshore Group of Banking Supervisors.

Singapore should continue close monitoring of its domestic and offshore financial sectors. The government should add tax and fiscal offenses to its schedule of serious offenses. The conclusion of broad mutual legal assistance agreements is also important to further Singapore's ability to work internationally to counter money laundering and terrorist financing. Singapore should lift its rigid bank secrecy restrictions to enhance its law enforcement cooperation in areas such as information sharing and to conform to international standards and best practices. Singapore should ratify the UN Convention against Corruption.

Slovak Republic

The geographic, economic, and legal conditions related to money laundering in Slovakia are typical of Central European economies in transition. While not a regional financial center, Slovakia's location makes it an attractive transit country for smuggling and trafficking in narcotics, mineral oils, and people. Organized criminal activity and opportunities to use gray market channels also lead to a favorable money laundering environment. According to the Financial Police, auto theft is the most commonly prosecuted predicate offense to money laundering.

Since 2000, Slovakia has strengthened the financial provisions of its criminal and civil codes through a series of amendments, which have resulted in an increased number of money laundering prosecutions. Slovakia replaced its original anti-money laundering (AML) legislation, Act No. 249/1994, with Act No. 367/2000, On Protection against the Legalization of Proceeds from Criminal Activities, which entered into force in January 2001. The Act defines money laundering, stating that "legalization of incomes derived from illegal activities," is "the use or other disposal of income or other property acquired or reasonably suspected of being acquired from illegal activity with the knowledge or suspicion that it was acquired through criminal activity in Slovakia or a third country." The Act defines "Use or disposal of property" as "ownership, possession or use of real estate, movable property, securities, monies or other liquid assets," and "disposal of income" as a "transfer of ownership, possession or use of such property with the purpose of concealing or disguising ownership." One of the most significant concepts defined in the Act is "unusual transaction" which the Act defines as "a legal action or other action which suggests that execution may enable legalization or the financing of terrorism." In practice, both unusual and suspicious transactions need to be reported, and Slovak authorities use the terms interchangeably. The Act sets forth the powers of the financial police and defines basic responsibilities of obliged entities, imposing customer identification, record keeping, and suspicious transaction reporting requirements on financial institutions.

Act No. 367/2000 expanded the list of entities subject to reporting requirements from banks and depository institutions to include foreign bank subsidiaries, the Slovak Export-Import Bank, nonbank financial institutions such as casinos, post offices, brokers, stock exchanges, commodity exchanges, securities markets, asset management companies, insurance companies, real estate companies, tax

advisors, auditors, credit unions, leasing firms, auctioneers, foreign exchange houses, and pawnshops. Nonprofit organizations are generally exempt from reporting requirements.

The Government of Slovakia (GOS) amended Act No. 367/2000 to address deficiencies in the original legislation and to harmonize Slovak legislation with the Second European Union (EU) Money Laundering Directive. Amendments to Act No. 367/2000 in 2002 extend reporting requirements to include dealers of antiques, art and collectibles; precious metals and stones, and other high-value goods; legal advisors; consultants; securities dealers; foundations; financial managers and consultants; and accounting services. The failure to report an unusual transaction is a criminal offense, punishable by 2-8 years imprisonment. Tipping off is also a criminal offense. The 2005 Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) evaluation report (MER) reported a lack of reporting on the part of designated nonfinancial business and professions (DNFBPs), and that casinos and exchange houses had not reported at all. The Slovak financial intelligence unit (FIU) estimated that of approximately 100,000 obliged entities, only banks and insurance companies had reported regularly, and the securities sector infrequently. It is unclear whether the obliged entities understand their reporting obligations. Slovakia has no requirement to give special attention to business relationships or transactions with legal or actual persons from countries not applying, or insufficiently applying, FATF recommendations.

Obliged entities must identify all customers, including legal entities, if they find the customers prepared or conducted suspect transactions, or if a sum of multiple transactions exceeding 15,000 euros (approximately U.S. $19,000) within a 12-month period is involved. Insurance brokers must identify all clients whose premiums exceed approximately 1,000 euros (approximately U.S. $1,400) in a year or whose one-time premium exceeds approximately 2,500 euros (approximately U.S. $3,600). Casinos have enhanced customer identification requirements.

Each competent authority has the discretion to delay a suspect transaction for up to 48 hours. The entity may, upon request, further delay a transaction for an additional 24 hours if the financial police notify the institution that the case has been submitted to law enforcement authorities. If the suspicion turns out to be unfounded, the state assumes the burden of compensation for losses stemming from the delay.

Article 233 of the Criminal Code defines "Legalization of Proceeds from Criminal Activity" as a criminal offense. A money laundering conviction does not require a conviction for the predicate offense, and a predicate offense need not occur within the Slovak Republic to be considered as such. Slovakia amended its Criminal Procedure Code and Criminal Code in 2003 and 2005. The amendments enhance law enforcement powers by granting investigators the authority to conduct sting operations, and introduce limited provisions regarding corporate criminal liability. The revised codes contain sentencing guidelines, including 2 to 20 years for laundering illicit proceeds. Corporate liability for money laundering still does not exist in Slovakia.

As a result of amendments to the Slovak Civil Code in 2001, the Government of Slovakia (GOS) ordered all banks to stop offering passbook, or anonymous, accounts. All existing owners of anonymous accounts were required to disclose their identity to the bank and close the anonymous account by December 31, 2003. Owners of accounts that were still open could withdraw money for a three-year noninterest bearing grace period. The GOS confiscated all funds from accounts remaining after January 1, 2007, and deposited them in a fund administered by the Ministry of Finance, where they will be available for collection by the account holder until January 1, 2012. As of January 1, 2007, bearer passbook accounts ceased to exist.

Slovak law reportedly lacks effectiveness with regard to the beneficial ownership of legal persons. According to the 2005 MONEYVAL MER, "Slovakian law does not require adequate transparency concerning beneficial ownership and control of legal persons." The law does not mandate

identification on the Commercial Register for beneficial owners of a company purchasing or holding shares in another registered company.

Slovak authorities have been preparing to implement the Third EU Money Laundering Directive. After consultations with the Ministry of Finance, the Ministry of Interior, and the National Bank of Slovakia, the FIU drafted new legislation to comply with the Third Directive. The new Anti-Money Laundering Act, which will fully implement the Third Money Laundering Directive and upgrade many requirements regarding money laundering and terrorist financing, will come into force in February 2008. The new AML Act, when enacted, will replace Act No. 367/2000.

The Bureau of Organized Crime (BOC) focuses on all forms of organized crime, including narcotics, money laundering, human trafficking, and prostitution. The BOC has four regional units, each responsible for a different part of Slovakia (Bratislava, Eastern Slovakia, Western Slovakia, and Central Slovakia). The FIU is a fifth unit of this agency, but works at a national level.

Established in November 1996 as a department within the Financial Police, Slovakia's FIU, "Spravodajská Jednotka Financnej Policie" in Slovak,was downgraded in 2005 to one of eight divisions of the BOC. The FIU has four departments: the Unusual Transactions Department, the Obliged Entities Supervision Department, the International Cooperation Department, and the Property Checks Department. The FIU receives unusual transaction reports. Despite a slight decline in staff and resources, the FIU and regional financial police increased filings, inspections, and the number of cases forwarded for prosecution.

As the organization responsible for combating money laundering, the FIU receives and evaluates unusual (suspicious) transaction reports (STRs) and collects additional information pursuant to suspicions of money laundering. If justified, the unit forwards the case to one of the regional financial police units. All supervisory authorities must inform the FIU of any violation immediately upon discovery. Once enough information has been obtained to warrant suspicion that a criminal offense has occurred, the FIU may take appropriate measures, including asking the obliged entity to delay business or financial transactions for 48 hours. The FIU then submits cases of reasonable suspicion of a criminal offence to police investigators.

In 2006, the FIU received 1,571 STRs with a total value of U.S. $568 million. The FIU submitted fourteen cases for prosecution, including two cases outstanding from 2005. The regional units of the Financial Police submitted an additional 177 cases for prosecution. A growing number of these cases involve organized crime groups transferring funds from neighboring countries (primarily Ukraine and Hungary) to Slovakia. Most criminal prosecutions involved credit fraud. Most tax prosecutions and on-site inspections violations related to abuses of Slovakia's value added tax system. Money laundering convictions (under Article 252 of the previous Criminal Code) have gradually increased. Detailed statistics on money laundering convictions are not available. However, there were no autonomous cases of money laundering convictions, since the FIU and regional financial police tend to forward for prosecution only money laundering cases that are tied to broader organized criminal activities. No information for 2007 is available.
Section 10 of Act No. 367/2000 assigns the FIU a supervisory role, embodied by the Obliged Entities Supervision Department, over the implementation of AML measures in financial institutions. In this capacity, the FIU inspects these institutions. It also has sole supervisory authority over DNFBPs. The seven officers in the supervision department carried out 92 on-site inspections in 2006, resulting in fines with a total value of U.S. $62,000.

Slovak law mandates forfeiture of the proceeds of crime. It does not, however, allow for forfeiture from third-party beneficiaries. The Public Prosecutor Service may order the seizure of accounts during the pre-trial proceedings stage, and can order the use of information technology for enhanced investigations under Articles 79c, 88 and 88e of the Criminal Procedure Code. In 2006, a new

Confiscation Law became effective, strengthening the government's ability to seize assets gained through criminal activity.

The Law on Proving the Origin of Property came into force on September 1, 2005. According to the law, an undocumented increase in property exceeding an amount 200 times the minimum monthly wage must be scrutinized and could be considered illegal. The police must investigate allegations of illegally acquired property, and report their findings to the Office of the Public Prosecutor. The Public Prosecutor's Office may then order the property confiscated. However, the new law was controversial, and a provisional decision of the Constitutional Court froze its implementation on October 6, 2005. A year later, the Constitutional Court suspended the Act. The Constitutional Court has not yet reached a final decision on this law.

Supporting a terrorist group is an offense under the Criminal Code. Act No. 445/2002 amended the money laundering law to criminalize terrorist financing and require obliged entities to report transactions possibly linked to terrorist financing. Although authorities have acknowledged the ability to prosecute "aiding and abetting an offense of terrorism or the establishment of a terrorist group," no case has gone before the courts.

As Slovakia itself reported in its 2004 self-assessment questionnaire on its AML efforts, its counter-terrorist financing (CTF) regime is not fully compliant with the FATF's Special Recommendations on Terrorist Financing. MONEYVAL gave Slovakia a rating of "partial compliance" in 2004 with regard to Special Recommendation I (Implementation of UNSCR 1373), as the criminalization of terrorist financing solely based on aiding and abetting does not meet the FATF standard; and Special Recommendation VII (enhanced scrutiny of transfers lacking originator information). The MER also stated that Slovakia's provisions are not broad enough to clearly criminalize the collection of funds with the intent to carry out terrorist acts, support terrorist organizations regardless of whether the donation is for the commission of a terrorist act, or for the use of any individual terrorist.

All competent authorities in the Slovak Republic have full authority to freeze or confiscate terrorist assets consistent with UNSCR 1373. The GOS has agreed to immediately freeze all accounts owned by entities listed by the UNSCR 1267 Sanctions Committee Consolidated List of terrorist entities, the EU's consolidated lists, and those provided by the United States under Executive Order 13224. The GOS posts the lists online, but does not distribute them. Obliged entities must check the website and report any matches they find. In the event an obliged entity were to identify a terrorism-related account, the financial police could suspend any related financial transaction for up to 48 hours, and then gather evidence to freeze the account and seize assets. However, the reporting obligation with respect to terrorist financing remains insufficiently clear. Obliged entities and other covered institutions have not received any guidance and no reports involving terrorist financing have been filed. Guidance and communication with financial intermediaries and DNFBPs is reportedly weak. No terrorist finance-related accounts have been frozen or seized in Slovakia.

Slovakia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism. Slovakia is also a party to the European Convention on Mutual Assistance in Criminal Matters and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

Slovakia is a member of the MONEYVAL Committee. Its FIU is a member of the Egmont Group and has signed memoranda of understanding (MOUs) with seven counterpart FIUs and with the Royal Canadian Mounted Police (RCMP).

The Government of Slovakia should continue to improve its AML/CTF regime. Authorities should ensure that property and proceeds are equivalent in Article 252 and that this definition is codified to avoid confusion on this issue. Slovakia should also provide guidance and outreach to, and improve

supervision of, its DNFBPs to ensure that they follow their AML and CTF reporting requirements. Slovakia should implement formal AML supervision for exchange houses. Slovak authorities should encourage and enable police to pursue money laundering and financial crime even when it does not involve organized crime activities. Slovakia should provide adequate resources to ensure that the FIU, law enforcement, and prosecutorial agencies receive adequate funding and training, as well as maintain adequate staff, to effectively perform their various responsibilities. The FIU in particular needs staffing commensurate with its responsibilities. The GOS should work to enhance cooperation and coordination among these agencies and other competent authorities. Slovakia should take steps to include in its legislative framework the international standard for definition and treatment of beneficial owners. Authorities should also consider requiring enhanced due diligence or reporting requirements for transactions involving countries not in conformance with FATF standards, and consider adopting criminal, civil or administrative sanctions for money laundering in relation to legal persons. The GOS should consider amending its confiscation and forfeiture regime to provide for asset forfeiture from third-party beneficiaries.

The Government of Slovakia should hone its legal framework to clarify the reporting obligation with respect to terrorist financing and issue formal guidance to covered institutions. The GOS should ensure proactive circulation of the UN, EU and U.S. lists of terrorist entities to obliged entities, thus tightening the CTF regime. The GOS should also codify reporting requirements for charitable and nonprofit organizations. Authorities should amend the Criminal Code to ensure that the criminalization of terrorist financing parallels international standards, including broad parameters that criminalize the collection of funds for carrying out terrorist acts, for any activities undertaken by terrorist organizations, and for use by any individual terrorist.

South Africa

South Africa's position as the major financial center in the region, its relatively sophisticated banking and financial sector, and its large cash-based market, make it a very vulnerable target for transnational and domestic crime syndicates. Nigerian, Pakistani, and Indian drug traffickers, Chinese triads, Taiwanese groups, Lebanese trading syndicates, and the Russian mafia have all been identified as operating in South Africa, along with South African criminal groups. The fact that a high number of international crime groups operate in South Africa and that there are few reported money laundering prosecutions indicate that South Africa remains vulnerable to all-source money laundering. Although the links between different types of crime have been observed throughout the region, money laundering is primarily related to the illicit narcotics trade. Other common types of crimes related to money laundering are: fraud, theft, corruption, currency speculation, illicit dealings and theft of precious metals and diamonds, human trafficking, stolen cars, and smuggling. Most criminal organizations are also involved in legitimate business operations. There is a significant black market for smuggled goods.

South Africa is not an offshore financial center, nor does it have free trade zones. It does, however, operate Industrial Development Zones (IDZs). The South African Revenue Service (SARS) monitors the customs control of these zones. Imports and exports that are involved in manufacturing or processing in the zone are duty-free, provided that the finished product is exported. South Africa maintains IDZs in Port Elizabeth, East London, Richards Bay, and Johannesburg International Airport.

The Proceeds of Crime Act (No. 76 of 1996) criminalized money laundering for all serious crimes. This act was repealed and replaced by the Prevention of Organized Crime Act (no. 121 of 1998), which confirms the criminal character of money laundering, mandates the reporting of suspicious transactions, and provides a "safe harbor" for good faith compliance. Violation of this act carries a fine of up to 100 million rand (approximately U.S. $14.8 million) or imprisonment for up to 30 years.

The Financial Intelligence Centre Act (FICA) requires a wide range of financial institutions and businesses to identify customers, maintain records of transactions for at least five years, appoint compliance officers to train employees to comply with the law, and report transactions of a suspicious or unusual nature. Regulated businesses include companies and firms considered particularly vulnerable to money laundering activities, such as banks, life insurance companies, foreign exchange dealers, casinos, and real estate agents. If the FIC has reasonable grounds to suspect that a transaction involves the proceeds of criminal activities, it forwards this information to the investigative and prosecutorial authorities. If there is suspicion of terrorist financing, that information is to be forwarded to the National Intelligence Service. There are no bank secrecy laws in effect that prevent the disclosure of ownership information to bank supervisors and law enforcement authorities. Regulations require suspicious transaction reports to be sent to the South African financial intelligence unit (FIU), the Financial Intelligence Centre (FIC). Both the Prevention of Organized Crime Act and the FICA contain criminal and civil forfeiture provisions.

The FIC began operating in February 2003. The mandate of the FIC is to gather and analyze financial intelligence for use against money laundering and other financial crimes; to coordinate policy and efforts to counter money laundering activities; and to act as a centralized repository of information and statistics on money laundering. The FIC is a member of the Egmont Group of financial intelligence units. In addition to the FIC, South Africa has a Money Laundering Advisory Council (MLAC) to advise the Minister of Finance on policies and measures to combat money laundering.

From March 2006 through March 2007, the FIC received 21,466 suspicious transaction reports (STRs), an increase of nine percent from the previous year's 19,793 STRs. Eighty-eight percent of the reports came from financial institutions, with the balance coming from casinos, coin dealers, accountants, attorneys, and other reporting entities. FIC referred 549 STRs to law enforcement and/or intelligence agencies for further investigation, with a value in excess of 1.4 billion rand (approximately U.S. $200 million). FIC and banking officials report that the quality of STRs is steadily improving, as bank personnel receive AML training and as AML software and other detection systems are installed and refined.

Precise information is not available on how many of the STRs led to criminal investigations. However, the number of money laundering and terrorist finance investigations, prosecutions, and convictions is thought to be very low. Two of the corporate defendants in the high-profile 2005 Schabir Shaik corruption trial were convicted of money laundering. However, the small number of actual cases prosecuted in South Africa indicates problems in reporting, analysis, and investigations. Many investigators and prosecutors seem to focus on the underlying "predicate" crimes, and may be unfamiliar with money laundering offenses or see no reason to add money laundering charges to cases.

In 2005, the Protection of Constitutional Democracy Against Terrorist and Related Activities Act came into effect. The Act criminalizes terrorist activity and terrorist financing and gave the government investigative and asset seizure powers in cases of suspected terrorist activity. The Act is applicable to charitable and nonprofit organizations operating in South Africa. The Act requires financial institutions to report suspected terrorist activity to the FIC. The FIC distributes the list of individuals and entities included on the United Nations (UN) 1267 Sanctions Committee's consolidated list.

Conforming to the new money laundering regime has been expensive for banks, which have re-registered customers, given AML training to thousands of employees, expanded their internal compliance offices, and taken other steps to meet global best practices and comply with the law. Many banks state that the reporting requirements hamper their efforts to attract new customers. For example, if the customer has never traveled outside the country, they may not have supporting documentation (no driver's license or passport) to properly satisfy the due diligence laws. Also, retroactive due diligence requirements mean those account holders who do not present identifying documents in

person risk having their accounts frozen. These requirements were fully implemented in September 2006, after which date transactions with accounts owned by still-unidentified persons were blocked. Reporting requirements were specifically waived for brokers assisting clients with a one-time amnesty offer according to the Exchange Control and Amnesty and Amendment of Taxation Laws of 2003.

Because of the cash-driven nature of the South African economy, alternative remittance systems that bypass the formal financial sector exist and are used largely by the Islamic and Indian communities. Hawala networks in South Africa have direct ties to South Asia and the Middle East. Currently, there is no legal obligation requiring alternative remittance systems to report cash transactions within the country.

SARS requires all visitors with cash in their possession to declare the amount upon arrival in South Africa. In addition, all South Africans and residents leaving the country with cash must declare amounts in excess of 175,000 rand (approximately U.S. $24,600) for individuals, or 250,000 rand (approximately U.S. $35,280) for families. Although bulk-cashing smuggling is not illegal per se, failure to make the required declarations carries a penalty. Smuggling and border enforcement are major problems in South Africa. The Financial Action Task Force (FATF) conducted a mutual evaluation of South Africa in 2003 and made several recommendations regarding controls on cross-border currency movement, thresholds, and amendments to the Exchange Control Act. While legislation has been adopted in response to the recommendations, full implementation has yet to take place.

South Africa has cooperated with the United States in exchanging information related to money laundering and terrorist financing. The two nations have a mutual legal assistance treaty and a bilateral extradition treaty. In June 2003, South Africa became the first African nation to be admitted into the Financial Action Task Force (FATF), and it held the FATF Presidency for the period June 2005-June 2006. South Africa is also an active member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. South Africa is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

The South African Government should fully implement FATF Special Recommendation Nine and establish control over cross-border currency movement. South Africa should increase steps to bolster border enforcement and should examine forms of trade-based money laundering and informal value transfer systems. It should also regulate and investigate the country's alternative remittance systems. There is an over-reliance on STR reporting to initiate money laundering investigations. Law enforcement and customs officials should follow the money and value trails during the course of their investigations. South Africa should continue to enforce anti-money laundering regulations within the casino industry. It should fully implement the new law (Protection of Constitutional Democracy against Terrorist and Related Activities Act) against terrorist activity and terrorist financing. South Africa should publish the annual number of money laundering and terrorist financing investigations, prosecutions, and convictions.

Spain

Spain is a major European center of money laundering activities as well as a major gateway for illicit narcotics. Drug proceeds from other regions enter Spain as well, particularly proceeds from hashish entering from Morocco and heroin entering from Turkey. There are no known currency transactions of significance involving large amounts of U.S. currency and/or direct narcotics proceeds from U.S. sales.

Tax evasion in internal markets and the smuggling of goods along the coastline also continue to be sources of illicit funds in Spain. The smuggling of electronics and tobacco from Gibraltar remains an ongoing problem. Airline personnel traveling from Spain to Latin America reportedly smuggle sizeable sums of bulk cash. Additional money laundering activities found in Spain include Colombian companies purchasing goods in Asia and selling them legally at stores run by drug cartels in Europe. Credit card balances are paid in Spanish banks for charges made in Latin America, and money deposited in Spanish banks is withdrawn in Colombia through ATM networks.

An unknown percentage of drug-trafficking proceeds are invested in Spanish real estate, particularly in the booming coastal areas in the south and east of the country. Up to thirty percent of the 500 euros notes in use in Europe are reported to be in circulation in Spain, directly linked to the purchase of real estate to launder money. Given the burgeoning profitability of the construction sector over the past several years, many coastal municipalities have ignored the illegality of various construction projects in their localities. In 2006, the prosecutor's office in the southern province of Malaga processed more than 200 reports of abuse and systemic corruption related to the real estate and construction industries, resulting in judicial action against 20 out of 100 mayors in that province.

Throughout 2007, Spanish authorities conducted numerous anti-money laundering (AML) and counter-terrorist financing (CTF) operations that resulted in arrests. On July 25, Spanish authorities arrested two Syrian nationals accused of funneling donations from Muslim extremists living in Spain to foreign Islamic terrorist organizations. The network reportedly also funneled donations into the booming Spanish real estate market, selling the properties at a later date for profit. On July 27, Spanish police in cooperation with Colombian authorities dismantled a drug trafficking and money laundering network. The operation led to nine arrests in Barcelona and 18 in Colombia, along with the seizure of funds and illicit narcotics. There was little legislative activity regarding anti-money laundering and terrorism finance in 2007, though regulations clarifying financial reporting requirements were passed.

The most recent mutual evaluation of Spain was conducted by the Financial Action Task Force (FATF) in 2005, with the mutual evaluation report (MER) released in June 2006. The MER noted areas where Spain is not in full compliance with the 40 Recommendations and Nine Special Recommendations. Of the 49 recommendations, of which 47 were applicable, Spain was rated "largely compliant" or better in 32 and compliant in the five core FATF recommendations (Recommendations 1, 5, 10, 13, and Special Recommendations II and IV).

Spanish authorities recognize the presence of alternative remittance systems. Informal nonbank outlets such as "locutorios" (communication centers that often offer wire transfer services) are used to move money in and out of Spain by making small international transfers for members of the immigrant community. Spanish regulators also note the presence of hawala networks in the Islamic community.

Spain is not considered to be an offshore financial center and does not operate any free trade zones. Spanish law states that an entity can perform banking activity if its registered office, administration, and management reside within Spanish territory. Spanish law does not prohibit financial institutions from entering into banking relationships with shell banks, but there are no shell banks in Spain. Financial institutions have no requirement to determine whether a correspondent financial institution in a foreign country allows accounts used by shell banks. The Government of Spain (GOS) has no accurate estimate of the numbers of offshore banks, offshore international business companies, exempt companies, or shell companies. Spanish law does not recognize trusts, including those created in foreign countries. Offshore casinos and Internet gaming sites are forbidden, but online casinos often run from servers located outside of Spanish territory. Spanish politicians have been critical of Gibraltar's role in this regard. In this instance, regulation can only occur through mutual judicial assistance or international agreements.

Money laundering is criminalized by Article 301 of the Penal Code, added in 1988 when laundering the proceeds from narcotics trafficking was made a criminal offense. Individuals in fiduciary

institutions can be held liable if their institutions have been used to commit financial crimes; a 1991 amendment made such persons culpable for both fraudulent acts and negligence connected with money laundering. The law was expanded in 1995 to cover all serious crimes that required a prison sentence greater than three years. Amendments to the code on November 25, 2003, which took effect on October 1, 2004, made all forms of money laundering financial crimes. Any property, of any value, can form the basis for a money laundering offense, and a conviction or a prosecution for a predicate offense is not necessary to prosecute or obtain a conviction for money laundering. Spanish authorities can also prosecute money laundering based on a predicate offense in another country, if the predicate offense would be illegal in Spain.

Law 19/2003 obliges financial institutions to make monthly reports on large transactions. Banks are required to report all international transfers greater than 30,000 euros (approximately $43,800). The law also requires the declaration and reporting of internal transfers of funds greater than 80,500 euros (approximately U.S. $117,520). Individuals traveling internationally are required to report the importation or exportation of currency greater than 6,000 euros (approximately U.S. $8,760). Foreign exchange and money remittance entities must report on transactions above 3,000 euros (approximately U.S. $4,380). Authorities also require reporting transactions exceeding 30,000 euros (approximately U.S. $43,800) from or with persons in countries or territories considered to be tax havens. Law 19/2003 allows the seizure of up to 100 percent of the currency if illegal activity under financial crimes ordinances can be proven. Spanish authorities claim they have seen a drop in cash couriers since the law's enactment in July 2003. When the money has not been declared and cannot be connected to criminal activity, authorities may seize it until the origin of the funds is proven. On October 26, 2005, the European Parliament and the Council passed Regulation 1889/2005 on Controls of Cash Entering or Leaving the Community, which requires all travelers entering or leaving the EU with €10000 or more in cash to declare the sum to Customs. As of June 15, 2007, all Member States were required to implement the regulation.

The financial sector is required to identify customers, keep records of transactions, and report suspicious financial transactions. Spanish financial institutions are required by law to maintain fiscal information for five years and mercantile records for six years.

Money laundering controls apply to most entities active in the financial system, including banks, mutual savings associations, credit companies, insurance companies, financial advisers, brokerage and securities firms, postal services, currency exchange outlets, and individuals and unofficial financial institutions exchanging or transmitting money. Most categories of designated nonfinancial businesses and professions (DNFBPs) are subject to the same core obligations as the financial sector. The list of DNFBPs includes realty agents, dealers in precious metals and stones, as well as in antiques and art, legal advisors, accountants, auditors, lawyers, notaries and casinos

Reporting entities are required to examine and commit to writing the results of an examination of any transaction, irrespective of amount, which by its nature may be linked to laundering of proceeds. Law 12/2003 reaffirms the obligation of reporting suspicious activities. Reporting entities are required to report each suspicious transaction to the financial intelligence unit (FIU). Financial institutions also have an obligation to undertake systematic reporting of unusual transactions and those exceeding the currency threshold, including physical movements of cash, travelers' checks, and other bearer instruments/checks drawn on credit institutions above 30,000 euros (approximately U.S. $43,795). The reporting obligation applies to the laundering of proceeds of all illicit activity punishable by a minimum of three years imprisonment, including terrorism or terrorist financing. Nonbank financial institutions (NBFIs) such as insurers, investment services firms, collective investment schemes, pension fund managers, and others are subject to these requirements.

Article 4 of Law 19/1993 and Article 15 of Royal Decree (RD) 925/1995 contain safe harbor provisions. Financial institutions and their staff are legally protected from any breach of restrictions on

disclosure of information when reporting suspicious transactions. Reporting units must also take appropriate steps to conceal the identity of employees or managers making suspicious transaction reports (STRs).

The FATF MER noted shortcomings in the areas of customer due diligence, beneficial ownership of legal persons, and bearer shares. Anonymous accounts and accounts in fictitious names are precluded by Spanish legislation. Bearer shares are permitted in Spain, although they are not as prevalent as they have been in the past. Spanish authorities have taken steps to neutralize them since 1998, ensuring that mere possession cannot serve as proof of ownership. However, they still exist, and the MER cited the requirements to determine the beneficial owner as "inadequate."

Law 19/1993 and RD 925/1995 established the Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC) as Spain's FIU. Its primary mission is to receive, analyze, and disseminate suspicious and unusual transaction reports from financial institutions and DNFBPs. SEPBLAC coordinates the fight against money laundering in Spain and has primary responsibility for any investigation in money laundering cases. SEPBLAC also has supervisory and inspection functions and is directly responsible for the supervision of a large number of regulated institutions; for example, it directly supervises the AML procedures of banks and financial institutions. SEPBLAC thus has memoranda of understanding with the Bank of Spain, the National Securities Market Commission, and the Director General of Insurance and Pension Funds, to coordinate with the regulators that supervise their respective sectors. SEPBLAC is an interdepartmental body chaired by the Secretary for Economic Affairs, and all of the agencies involved in the prevention of money laundering participate. The representatives include the National Drug Plan Office, the Ministry of Economy, Federal Prosecutors (Fiscalia), Customs, Spanish National Police, Civil Guard, CNMV (equivalent to the U.S. Securities and Exchange Commission), Treasury, Bank of Spain, and the Director General of Insurance and Pension Funds.

The FATF MER described the FIU's supervisory capabilities as ineffective because of its limited resources; the MER also expressed concern regarding SEPBLAC's independence from the Bank of Spain. In SEPBLAC's annual report, the organization acknowledged the weaknesses highlighted by the FATF report and expressed a desire to work to address these issues.

SEPBLAC has access to the records and databases of other government entities and financial institutions. It also has formal mechanisms in place to share information domestically and with other FIUs. SEPBLAC has been a member of the Egmont Group since 1995. In 2006, SEPBLAC received 2,251 STRs, down from 2,502 in 2005. SEPBLAC received 539 requests for information from other FIUs in 2006 and made 231 requests to Egmont members.

Any member of the Commission may request an investigation. However, the FATF MER noted some concerns about the effectiveness of SEPBLAC's investigations, stating that at certain stages of the investigative process, obtaining account files can be time-consuming. The National Police and Anticorruption Police informed the evaluation team that they receive too many reports, and the reports they do receive are not adequate to serve as the basis for an investigation. SEPBLAC delegates responsibility to a secretariat in the Treasury to carry out penalties following investigation and a guilty verdict by a court. Sanctions can include closure, fines, account freezes, or seizures of assets. Law 19/2003 allows seizures of assets of third parties in criminal transactions and a seizure of real estate in an amount equivalent to the illegal profit.

Under Spain's currency control system, individuals and companies must declare the amount, origin, and destination of incoming and outgoing funds. Cash smuggling reports are shared between host government agencies. Provisional measures and confiscation provisions apply to persons smuggling cash or monetary instruments that are related to money laundering or terrorist financing. Gold, precious metals, and precious stones are considered to be merchandise and are subject to customs

legislation. Failing to file a declaration for such goods may constitute a case of smuggling and would fall under the responsibility of the customs authorities.

All legal charities are placed on a register maintained by the Ministry of Justice. Responsibility for policing registered charities lies with the Ministry of Public Administration. If a charity fails to comply with the requirements, sanctions or other criminal charges may be levied.

The Penal Code provides for two types of confiscation: generic (Article 127) and specific, for drug-trafficking offenses (Article 374). Article 127 of the Penal Code allows for broad confiscation authority by applying it to all crimes or summary offenses under the Code. The effects and instruments used to commit the offense, and the profits derived from the offense can all be confiscated. Article 127 also provides for the confiscation of property intended for use in the commission of any crime or offense. It also applies to property that is derived directly or indirectly from proceeds of crime, regardless of whether the property is held or owned by a criminal defendant or by a third party. Article 374 of the Penal Code calls for the confiscation of goods acquired through drug trafficking-related crimes and of any profit obtained. This allows for the confiscation of instruments and effects used for illegal drug dealing, as well as the goods or proceeds obtained from the illicit traffic. Consequently, all assets held by a person convicted of drug trafficking may be confiscated if those assets are the result of unlawful conduct.

A judge may impose provisional measures concerning seizures from any type of offense by virtue of the code of criminal procedure. Effects may be seized and stored by the judicial authorities at the beginning of an investigation. The Fund of Seized Goods of Narcotics Traffickers, established under the National Drug Plan, receives seized assets. The proceeds from the funds are divided, with equal amounts going to drug treatment programs and to a foundation that supports officers fighting narcotics trafficking. The division of assets from seizures involving more than one country depends on the relationship with the country in question. EU working groups determine how to divide the proceeds for member countries. Outside of the EU, bilateral commissions are formed with countries that are members of FATF, FATF-style regional bodies, and the Egmont Group, to coordinate the division of seized assets. With other countries, negotiations are conducted on an ad hoc basis.

The banking community cooperates with enforcement efforts to trace funds and seize or freeze bank accounts. The law is unclear as to whether or not civil forfeitures are allowed. The GOS enforces existing drug-related seizure and forfeiture laws. Spain has adequate police powers and resources to trace, seize, and freeze assets. Spain disseminates limited statistics on money laundering and terrorist financing investigations, prosecutions and convictions as well as on property frozen, seized and confiscated.

A small percentage of the money laundered in Spain is believed to be used for terrorist financing. It is primarily money from the extortion of businesses in the Basque region that is moved through the financial system and used to finance the Basque terrorist group ETA. After ETA announced the end of its cease-fire in June of 2007, reports of extortion against businesses located in the Basque and Navarra regions increased greatly. The FATF MER gives Spain a favorable review with regard to countering terrorist financing. Spain has long been dedicated to fighting terrorist organizations, including ETA, GRAPO, and more recently, Al-Qaida. Spanish law enforcement entities have identified several methods of terrorist financing: donations to finance nonprofit organizations (including ETA and Islamic groups); establishment of publishing companies that print and distribute books or periodicals for the purposes of propaganda, which then serve as a means for depositing funds obtained through kidnapping or extortion; fraudulent tax and subvention collections; the establishment of “cultural associations” used to facilitate the opening of accounts and provide a cover for terrorist finance activity; and alternate remittance system transfers.

Spain complies with all EU regulations concerning the freezing of terrorist assets. Crimes of terrorism are defined in Article 571 of the Penal Code, and penalties are set forth in Articles 572 and 574.

Sanctions range from ten to thirty years' imprisonment with longer terms if the terrorist actions were directed against government officials. On March 6, 2001, Spain's Council of Ministers adopted a decision requesting the implementation of UNSCR 1373 in the Spanish legal framework. EU Council Regulation (EC) 881/2002, which obliges covered countries such as Spain to execute UNSCR 1373, is implemented through EC No. 2580/of 27 December 2001. Terrorist financing issues are governed by a separate code of law and commission, the Commission of Vigilance of Terrorist Finance Activities (CVAFT). This commission was created under Law 12/2003 on the Prevention and Blocking of the Financing of Terrorism. In addition to the EU Council Regulations, Law 12/2003, when implemented, will allow the freezing of any type of financial flow so as to prevent the funds from being used to commit terrorist acts. Spanish authorities' ability to freeze accounts granted in the most recent law is more aggressive than that of most of their European counterparts. Though many laws are transposed from EU directives, Law 12/2003 on the prevention and freezing of terrorist financing surpasses EU Council requirements. However, the implementing regulations have yet to be announced, meaning that Spanish authorities have not yet established and implemented a clear, efficient procedure to ensure the freezing of funds or other assets without delay.

As with all European Union countries, the obligation to freeze assets under UNSCR 1267 has also been implemented through the Council. Spain regularly circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee consolidated list. There were six actions taken against individuals or entities in 2005 under 1267 and/or 1373, for a total value of 83.75 euros ($106). The CVAFT is charged with issuing freezing orders.

Spain is a member of the FATF and co-chairs the FATF Terrorist Finance Working Group. Spain is also involved with FSRBs as an observer to the South American Financial Action Task Force (GAFISUD) and a cooperating and supporting nation to the Caribbean Financial Action Task Force (CFATF). Spain is a major provider of counterterrorism assistance. SEPBLAC is a member of the Egmont Group and currently chairs the Outreach Committee Working Group. Spain provides AML/CTF assistance, particularly to Spanish speaking countries in Latin America.

Spain actively collaborates with Europol, supplying and exchanging information on terrorist groups. In 2007, U.S. law enforcement agencies also reported excellent cooperation with their Spanish counterparts. Spanish media gave prominent coverage to the cooperation between the U.S. Drug Enforcement Administration (DEA) and Spanish law enforcement authorities that led to the August 10, 2007 Spanish arrest of an accused prominent drug trafficker. This was one of many cases that U.S. law enforcement is working in collaboration with various Spanish authorities to resolve. In September 2007, Spanish police arrested two Pakistani men who were indicted in the U.S. on money laundering charges following a joint counter-terrorism investigation with the FBI. The investigation found evidence that more than 1 million euros (U.S. $1.46 million) flowed from the drug trade and other criminal actions to terrorist groups.

The GOS has signed criminal mutual legal assistance agreements with Argentina, Australia, Canada, Chile, the Dominican Republic, Mexico, Morocco, Uruguay, and the United States. Spain's mutual legal assistance treaty with the United States has been in effect since 1993 and provides for sharing of seized assets "to the extent permitted by [domestic] laws." Spain has also entered into bilateral agreements for cooperation and information exchange on money laundering issues with 14 countries around the world, as well as with the United States. SEPBLAC has bilateral agreements for cooperation and information exchange on money laundering issues with 21 FIUs around the world.

Spain is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism.

The scale of money laundering and the sophisticated methods used by criminals represent a major threat to Spain. The GOS has passed and enacted legislation designed to help eliminate and prosecute

financial crimes. Spain should also review the resources available for industry supervision, and ensure that SEPBLAC has the resources it needs to effectively discharge the supervisory duties entrusted to it. The GOS should work to close the loopholes that FATF identified, including those in the areas of customer due diligence, beneficial ownership of legal persons, and bearer shares. Spain should also work to implement Law 12/2003, which will greatly enhance Spain's capabilities to combat terrorist financing. Spain should maintain and disseminate statistics on investigations, prosecutions and convictions, including the amounts and values of assets frozen or confiscated.

St. Kitts and Nevis

St. Kitts and Nevis is a federation composed of two islands in the Eastern Caribbean. The federation is at major risk for corruption and money laundering due to the high volume of narcotics trafficking activity through and around the island, and the presence of known traffickers on the islands. The growth of its offshore sector and an inadequately regulated economic citizenship program further contribute to the federation's money laundering vulnerabilities.

The Ministry of Finance oversees St. Kitts and Nevis' Citizenship by Investment Program. An individual may qualify for citizenship with a U.S. $350,000 minimum investment in real estate. In addition, the Government of St. Kitts and Nevis (GOSKN) created the Sugar Industry Diversification Foundation (SIDF) after the closure of the federation's sugar industry as a special approved project for the purposes of citizenship by investment. To be eligible, an applicant must make a contribution between U.S. $200,000 to $400,000 (based on the number of the applicant's dependents). The GOSKN requires applicants to make a source of funds declaration and provide evidence supporting the declaration. According to the GOSKN, the Ministry of Finance oversees the Citizenship Investment Program and has established a Citizenship Processing Unit to manage the screening and application process.

As a federation, there is anti-money laundering, counter-terrorist financing, and offshore legislation governing both St. Kitts and Nevis. However, each island has the authority to organize its own financial structure. With most of the offshore financial activity concentrated in Nevis, it has developed its own offshore legislation independently. As of October 2007, Nevis has one offshore bank, 90 licensed insurance companies, 33,165 international business companies (IBCs), 9,840 limited liability companies (LLCs), 3,684 international trusts, 47 multiform foundations (utilized for estate planning, charity financing, and special investment holding arrangements), and 3,684 trusts. Figures from 2007 indicate that the St. Kitts has 1,201 exempt companies, 257 exempt foundations, nine exempt partnerships, 23 exempt trusts, 51 captive insurance companies, one insurance manager, five trust service providers, 25 corporate service providers, two investment companies, and three licensed Internet gaming sites. Internet gaming entities must apply for a license as an IBC.

Bearer shares are permitted provided that bearer share certificates are retained in the safe custody of authorized persons or financial institutions authorized by the Minister of Finance as approved custodians. Legislation requires certain identifying information to be maintained about bearer certificates, including the name and address of the bearer of the certificate, as well as its beneficial owner. All authorized custodians are required by law to obtain proper documents on shareholders or beneficial owners before incorporating exempt or other offshore companies. This information is not publicly available and only available to the regulator and other authorized persons who have access to the information.

The GOSKN licenses offshore banks and businesses. The GOSKN states that extensive background checks on all proposed licensees are conducted by a third party on behalf of the GOSKN before a license is granted. By law, all offshore bank licensees are required to have a physical presence in the federation; shell banks are not permitted. The Eastern Caribbean Central Bank (ECCB) has direct responsibility for regulating and supervising the offshore bank in Nevis, as it does for the entire

domestic sector of St. Kitts and Nevis, and for making recommendations regarding approval of offshore bank licenses. Under Section 10(8) of the Nevis Offshore Banking Ordinance, 1996 as amended in 2002, the ECCB is required to review all applications for licenses and report its findings to the Minister of Finance prior to consideration of the application.

The St. Kitts and Nevis Gaming Board is responsible for ensuring compliance of casinos. The Financial Services Commission (FSC) is the primary regulatory body for financial services in the federation and has the authority to cooperate with foreign counterparts on supervisory issues. Separate regulators for St. Kitts and Nevis carry out the actual supervision of institutions on behalf of the FSC including anti-money laundering examinations. Nevis seeks to consolidate its regulatory regime to a single unit as of January 2009, which would regulate all financial services businesses in Nevis. This would expand supervision to credit unions, local insurance companies, and money transfer agencies. Nevis also seeks to establish a risk-based supervision program and will conduct risk assessments on all licensees, as well as establish a risk based supervision schedule for onsite and offsite monitoring.

The Proceeds of Crime Act (POCA) No. 16 of 2000 criminalizes money laundering for serious offenses (defined to include more than drug offenses), and imposes penalties ranging from imprisonment to monetary fines. The POCA also overrides secrecy provisions that may have constituted obstacles to administrative and judicial authorities' ability to access information with respect to account holders or beneficial owners. The POCA limits and monitors the international transportation of currency and monetary instruments. Any person importing into or exporting from St. Kitts and Nevis a value exceeding $10,000 or its equivalent in Eastern Caribbean Currency needs to declare it through Customs. In addition, the Customs Control and Management Act criminalizes bulk cash smuggling. Customs and police share cash smuggling reports.

The FSC has issued guidance notes on the prevention of money laundering, pursuant to the Anti-Money Laundering Regulations. Regulations require financial institutions to identify their customers, maintain a record of transactions for up to five years, report suspicious transactions, and establish anti-money laundering training programs. The Anti-Money Laundering (Amendment) Regulations No. 36, 2001 and relevant Guidance Notes are presently under revision to include institutions' reporting obligations related to combating terrorist financing.

The Financial Intelligence Unit Act (FIUA) No. 15 of 2000 authorized the creation of a financial intelligence unit (FIU). The FIU began operations in 2001 and receives, collects, and investigates suspicious activity reports (SARs). All financial institutions, including nonbank financial institutions, are required by law to report suspicious transactions. Anti-money laundering regulations and the FIUA provide protection to reporting entities and employees, officers, owners, or representatives who forward suspicious reports to the FIU. The FIU has direct and indirect access to the records of other government entities via memorandums of understanding with domestic agencies. There is also indirect access to the records at financial institutions. The FIUA contains provisions for sharing information both domestically and with other foreign law enforcement agencies.

In 2007, the FIU received 96 SARs, almost double the number received in 2006. The FIU attributes this increase to efforts to increase awareness and educate entities of their reporting obligations. Of the 96 SARs, 40 were referred to law enforcement for appropriate action. The GOSKN did not report any action taken on these referrals. The Royal St. Kitts and Nevis Police Force is responsible for investigating financial crimes, but does not have adequate staff or training to effectively execute its mandate.

The Anti-Terrorism Act (ATA) No. 21 of 2002 provides the FIU and Director of Public Prosecutions with the authority to identify, freeze, and/or forfeit terrorist finance-related assets. However, the law only allows for criminal forfeiture. Civil forfeiture is considered unconstitutional. Under the POCA, legitimate businesses can be seized by the FIU if proven to be connected to money laundering activities. The FIU and the Director of Public Prosecutions are responsible for tracing, seizing, and

freezing assets. The FIU can freeze an individual's bank account for a period not exceeding five days in the absence of a court order. The freeze orders obtained via the court at times ascribe an expiration of six months or more. Also under the POCA, there is a forfeiture fund under the administration and control of the Financial Secretary in St. Kitts and the Permanent Secretary in the Ministry of Finance in Nevis. All monies and proceeds from the sale of property forfeited or confiscated are placed in the fund to be used for the purpose of anti-money laundering activities in both St. Kitts and Nevis. Between 2001 and 2006, the GOSKN froze approximately $2 million in assets, of which $1 million was forfeited. No assets were seized in 2007.

The ATA criminalizes terrorist financing. The ATA also implements various UN conventions against terrorism. The GOSKN circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 sanctions committee's lists. The GOSKN has some existing controls that apply to alternative remittance systems, but has undertaken no initiatives that apply directly to the potential terrorist misuse of charitable and nonprofit entities. To date, no terrorist related funds have been identified.

St. Kitts and Nevis is a member of the Caribbean Financial Action Task Force (CFATF) and is expected to undergo a mutual evaluation in 2008. St. Kitts and Nevis' Anti-Money Laundering/Combating Terrorist Financing Task Force will review the federation's legal and administrative structures and seek to address weaknesses in the regime in preparation for the upcoming mutual evaluation. St. Kitts and Nevis is also a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). The FIU is a member of the Egmont Group. The GOSKN is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. St. Kitts and Nevis is not a party to the UN Convention against Corruption, and has signed, but not ratified, the Inter-American Convention against Terrorism. A Mutual Legal Assistance Treaty (MLAT) between the GOSKN and the United States entered into force in 2000.

St. Kitts and Nevis should devote sufficient resources to effectively implement its anti-money laundering regime, giving particular attention to its offshore financial sector. St. Kitts and Nevis should determine the exact number of Internet gaming companies present on the islands and provide the necessary oversight of these entities. St. Kitts and Nevis should provide adequate resources and training to law enforcement agencies to effectively investigate money laundering cases. The GOSKN should also become a party to the UN Convention against Corruption.

St. Lucia

St. Lucia has developed an offshore financial service center that is vulnerable to money laundering. Transshipment of narcotics (cocaine and marijuana), unregulated money remittance businesses, cash smuggling, and bank fraud, such as counterfeit U.S. checks and identity theft, are among the other primary vulnerabilities for money laundering in St. Lucia.

Currently, St. Lucia has six offshore banks, 2,851 international business companies (a 49 percent increase from 2006), six private mutual funds, two public mutual funds, 24 international insurance companies, 66 trust companies, three mutual fund administrators, 25 registered agents and five registered trustees (service providers),and 30 domestic financial institutions. Shell companies are not permitted. The Government of St. Lucia (GOSL) also has one free trade zone where investors may establish businesses and conduct trade and commerce within the free trade zone or between the free trade zone and foreign countries. There are no casinos or Internet gaming sites in St. Lucia and the GOSL does not plan to consider the establishment of gaming enterprises.

Money laundering in St. Lucia is a crime under the 1993 Proceeds of Crime Act and the Money Laundering (Prevention) Act (MLPA) of 2003, which superseded the Money Laundering (Prevention) Act of 1999 and the Financial Intelligence Authority Act of 2002. The MLPA criminalizes the laundering of proceeds with respect to numerous predicate offenses, including narcotics, abduction, blackmail, counterfeiting, extortion, firearms and narcotics trafficking, forgery, corruption, fraud, prostitution, trafficking in persons, tax evasion, terrorism, gambling and robbery. The MLPA mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the MLPA imposes a duty on financial institutions (which include banks, credit unions, building societies, trust companies, and financial services providers) to take reasonable measures to establish the identity of customers, and requires accounts to be maintained in the true name of the holder. It also requires an institution to take reasonable measures to identify the underlying beneficial owner when an agent, trustee or nominee operates an account. These obligations apply to domestic and offshore financial institutions, including credit unions, trust companies, and insurance companies. The Financial Services Supervision Unit has issued detailed guidance notes to implement the MLPA. Currently, steps are also being taken to implement legislation to regulate money remitters.

In 1999, the GOSL enacted a comprehensive inventory of offshore legislation, consisting of the International Business Companies (IBC) Act, the Registered Agent and Trustee Licensing Act, the International Trusts Act, the International Insurance Act, the Mutual Funds Act, and the International Banks Act. An IBC may be incorporated under the IBC Act. Only a person licensed under the Registered Agent and Trustee Licensing Act as a licensee may apply to the Registrar of IBCs to incorporate and register a company as an IBC. IBCs intending to engage in banking, insurance or mutual funds business may not be registered without the approval of the Minister responsible for international financial services. An IBC may be struck off the register on the grounds of carrying on business against the public interest.

The Committee on Financial Services, established in 2001, is designed to safeguard St. Lucia's financial services sector. The Committee is composed of the Minister of Finance, the Attorney General, the Solicitor General, the Director of Public Prosecutions, the Director of Financial Services, the Registrar of Business Companies, the Commissioner of Police, the Deputy Permanent Secretary of the Ministry of Commerce, the police officer in charge of the Special Branch, the Comptroller of Inland Revenue, and others. The GOSL has implemented administrative procedures for an integrated regulatory unit to supervise the onshore and offshore financial institutions the GOSL currently regulates; however, the unit is not yet fully functional. The Eastern Caribbean Central Bank regulates St. Lucia's domestic banking sector.

The MLPA authorizes the establishment of St. Lucia's financial intelligence unit (FIU), which became operational in October 2003. The FIU is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs) from obligated financial institutions, and has regulatory authority to monitor compliance with anti-money laundering requirements. The FIU is also able to compel the production of information necessary to investigate possible offenses under the 1993 Proceeds of Crime Act and the MLPA. Failure to provide information to the FIU is a crime punishable by a fine or up to ten years imprisonment. The FIU has access to relevant records and databases of all St. Lucian government entities and financial institutions, and is permitted by law to share information with foreign FIUs. However, no formal agreement exists for sharing information domestically and with other FIUs. In 2007, the FIU received 39 suspicious transaction reports, two of which were referred to law enforcement agencies for further investigation. There are no recorded cases of money laundering within St. Lucia's banking sector for 2007.

Customs laws criminalize cash smuggling, and customs officials are aware of cash courier problems. Cash smuggling reports are shared with the FIU, Police, Director of Public Prosecutions and the Attorney General.

Under current legislation, instruments of crime, such as conveyances, farms, and bank accounts, can be seized by the FIU. Substitute assets can also be seized. The legislation also applies to legitimate businesses if used to launder drug money, support terrorist activity, or are otherwise used in a crime. There is no legislation for civil forfeiture or shared narcotics assets. If the individual or business is not charged, then assets must be released within seven days. No assets were frozen in 2007.

The GOSL has not criminalized the financing of terrorism. However, St. Lucia circulates lists to financial institutions of terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O 13224. The GOSL has the legislative power to freeze, seize and forfeit terrorist finance related assets. To date, no accounts associated with terrorists or terrorist entities have been found in St. Lucia. The GOSL has not taken any specific initiatives focused on the misuse of charitable and nonprofit entities.

The GOSL has been cooperative with the USG in financial crimes investigations. In February 2000, St. Lucia and the United States brought into force a Mutual Legal Assistance Treaty.

The GOSL is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime or the Inter-American Convention against Terrorism. The GOSL has not signed the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Corruption. St. Lucia is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. St. Lucia's FIU is not a member of the Egmont Group.

In accordance with international standards, the Government of St. Lucia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

The GOSL should criminalize the financing of terrorism. It should also enhance and implement its anti-money laundering legislation and programs, including adopting civil forfeiture legislation and ensuring that its FIU meets the Egmont Group standards. The rapid expansion of the island's offshore financial services sector should be counterbalanced by efforts that increase transparency. The GOSL also needs to improve its record of investigating, prosecuting, and sentencing money launderers and those involved in other financial crimes, as well as improving and implementing its asset seizure and forfeiture regime.

St. Vincent and the Grenadines

St. Vincent and the Grenadines (SVG) remains vulnerable to money laundering and other financial crimes as a result of the rapid expansion and limited regulation of its offshore sector. Money laundering is principally affiliated with the production and trafficking of marijuana in SVG, as well as the trafficking of other narcotics from South America. Money laundering occurs in various financial institutions such as banks (domestic and offshore) and money remitters. There has been a slight increase in fraud and the use of counterfeit instruments over the last year, such as tendering counterfeit checks or cash.

The domestic financial sector includes two commercial banks, a development bank, two savings and loan banks, a building society, 16 insurance companies, 10 credit unions, and two money remitters. The offshore sector includes six offshore banks, 8,573 international business corporations (an increase of 918 from the previous year), 13 offshore insurance companies, 55 mutual funds, 27 registered agents, and 154 international trusts. There are no offshore casinos and no Internet gaming licenses have been issued. There are no free trade zones in SVG. The Government of St. Vincent and the Grenadines (GOSVG) eliminated its economic citizenship program in 2001.

No physical presence is required for offshore sector entities and businesses, with the exception of offshore banks. Nominee directors are not mandatory except when an international business corporation (IBC) is formed to carry on banking business. Bearer shares are permitted for IBCs but not for banks. The International Business Companies (Amendment) Act No.26 and 44 of 2002 was enacted to immobilize bearer shares and requires registration and custody of bearer share certificates by a registered agent who must also keep a record of each bearer certificate issued or deposited in its custody. The record must contain pertinent information relating to the company issuing the shares, the number of the share certificate, and identity of the beneficial owner. The Offshore Finance Inspector has the ability to access the name or title of a customer account and confidential information about the customer that is in the possession of a license.

The Eastern Caribbean Central Bank (ECCB) supervises SVG's domestic banks. The International Banks (Amendment) Act No. 30 of 2002 provided the ECCB with enhanced authority to review and make recommendations regarding approval of offshore bank license applications, and to directly supervise the offshore banks in conjunction with the International Financial Services Authority (IFSA). The agreement includes provisions for joint on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore banks. The IFSA continues independently to supervise and regulate other offshore sector entities; however, its staff exercises only rudimentary controls over these institutions. The GOSVG has strengthened the structure and staffing of the IFSA to regulate offshore insurance and mutual funds. The Exchange of Information Act No. 29 of 2002 authorizes and facilitates the exchange of information among regulatory bodies.

The Proceeds of Crime and Money Laundering (Prevention) Act (PCMLPA) 2001 criminalizes money laundering, and requires financial institutions and other regulated businesses to report suspicious transactions. Reporting is required for all suspicious activities regardless of the transaction amount. In 2005, the PCMLPA was amended to expand the definition to include an all offences approach and extended the scope of sections relating to the seizure, detention, and forfeiture of cash. The Proceeds of Crime (Money Laundering) Regulations establish mandatory record-keeping rules and customer identification requirements. Financial institutions are required to maintain all records relating to transactions for a minimum of seven years.

Customers are required to complete a source of funds declaration for any cash transaction over 10,000 East Caribbean dollars (XCD) (approximately U.S. $3,800). It is not mandatory to report other noncash transactions exceeding 10,000 XCD. In 2003, the GOSVG reintroduced a customs declaration form to be completed by incoming travelers. Incoming travelers are required to declare currency over 10,000 XCD.

The Financial Intelligence Unit Act No. 38 of 2001 (FIU Act) establishes the GOSVG's financial intelligence unit (FIU). Operational as of 2002, the FIU has the mandate to receive, analyze, and investigate financial intelligence, and prosecute money laundering cases. Suspicious activity related to drug trafficking is forwarded to the Narcotics Unit for further investigation, and activity related to fraud is forwarded to the Criminal Investigation Division. The FIU also has the ability to obtain production orders and stop/freeze orders. The FIU staff includes the Director, financial investigators, legal officers, and administrative officers. As of November 2007, the FIU received 159 suspicious activity reports for the year, and more than 750 since its inception. There was one conviction for money laundering in 2007.

The FIU is the main entity responsible for supervising and examining financial institutions for compliance with anti-money laundering and counter-terrorist financing laws and regulations. The function is also performed by the International Financial Services Authority (IFSA) and the ECCB. Money laundering controls also apply to nonbanking financial institutions and intermediaries, which the FIU monitors for compliance. Reporting entities are protected by law if fully cooperative with the FIU. An amendment to the FIU Act permits the sharing of information even at the investigative or

intelligence stage. The FIU does not have direct access to the records or databases of other government entities. Generally, records are still kept in physical form and must be retrieved manually.

Existing anti-money laundering legislation allows for the criminal forfeiture of intangible as well as tangible property. Drug trafficking offenses may also be liable to forfeiture pursuant to the Drug (Prevention and Misuse) Act and the Criminal Code. There is no period of time during which the assets must be released. Frozen assets are confiscated by the FIU upon conviction of the defendant. Proceeds from asset seizures and forfeitures are placed by the FIU into the Confiscated Assets Fund established by the PCMLPA. Legitimate businesses can also be seized if used to launder drug money, support terrorist activity, or are otherwise used in a crime. A civil forfeiture bill has been drafted and is currently before the National Anti-Money Laundering Committee (NAMLC) for its approval. In 2007, approximately $304,380 was frozen or seized. Of this amount, approximately U.S. $69,889 was forfeited.

In 2006, the GOSVG enacted the United Nations (Anti-Terrorism Measures) (Amendment) (UNATMA) Act 2006, Act. No.13. The UNATMA criminalizes terrorist financing and imposes a legal obligation on financial institutions and relevant business to report suspicious transactions relating to terrorism and terrorist financing to the FIU. The GOSVG circulates lists of terrorists and terrorist entities to all financial institutions in SVG. To date, no accounts associated with terrorists have been found. The GOSVG has not undertaken any specific initiatives focused on the misuse of charitable and nonprofit entities.

An updated extradition treaty and a Mutual Legal Assistance Treaty between the United States and the GOSVG entered into force in 1999. The FIU executes the Mutual Legal Assistance Treaty requests. A member of the Caribbean Financial Action Task Force (CFATF), the GOSVG is scheduled to undergo its second mutual evaluation in early 2008. The GOSVG is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering, and the FIU is a member of the Egmont Group. The GOSVG is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GOSVG has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOSVG has not signed the UN Convention against Corruption.

The Government of St. Vincent and the Grenadines has strengthened its anti-money laundering and counter-terrorist financing regime through legislation and the establishment of an effective FIU. The GOSVG should continue to ensure that this legislation is fully implemented, and that the FIU has access to all necessary information. The GOSVG should insist that the beneficial owners of IBCs are known and listed in a registry available to law enforcement, immobilize all bearer shares, and properly supervise and regulate all aspects of its offshore sector. The GOSVG should continue to provide training and devote resources to increase the cooperation among its regulatory, law enforcement, and FIU personnel in anti-money laundering and counter-terrorist financing operations and investigations. In addition, the GOSVG should consider computerizing its record keeping systems to ensure timely and effective information sharing. The GOSVG should pass civil forfeiture legislation and consider the utility of special investigative techniques. The GOSVG should also become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Suriname

Suriname is not a regional financial center. Narcotics-related money laundering is closely linked to transnational criminal activity related to the transshipment of Colombian cocaine. Domestic drug trafficking organizations and organized crime are thought to control much of the money laundering proceeds, which are “invested” in casinos, real estate, and private sector businesses. Additionally, money laundering occurs as a result of poorly regulated private sector activities, such as casinos and

car dealerships, the nonbanking financial system (including money exchange businesses or "cambios"), and a variety of other means, including construction, the sale of gold purchased with illicit money, and the manipulation of commercial bank accounts.

Suriname is not an offshore financial center and has no free trade zones. There is a gold economy in the interior mining regions of the country. Suriname has a significant informal economy, the majority of which is not linked to money laundering proceeds.
A package of legislation passed in 2002 included the criminalization of money laundering. The legislation, "Reporting of Unusual Transactions in the Provision of Services," addresses multiple issues related to all types of money laundering, including criminalizing money laundering, reporting of unusual transactions, and requiring service providers to request identification from each customer making a transaction. The legislation applies to both banking and nonbanking financial institutions. The law also provides for the establishment of a financial intelligence unit (FIU) and requires financial institutions, nonbank financial institutions, and natural legal persons who provide financial services to report unusual transactions to the FIU. In total, approximately 130 entities in Suriname are required to report to the FIU. While the FIU has informed all entities of their reporting requirements, to date only the banking sector is in full compliance.

In accordance with international standards, objective and subjective indicators have been approved to identify unusual transactions. An unusual transaction is defined as any transaction that deviates from the usual account as well as any customer activities that are not "normal" daily banking business. Reporting is mandatory if financial transactions are above a certain threshold; however, sanctions for noncompliance are currently not enforced. The thresholds for financial institutions range from U.S. $5,000 for money-transfer offices to U.S. $10,000 for banks, insurance companies, money exchange offices, and savings and credit unions. Thresholds for nonbanking financial institutions and "natural legal persons" are U.S. $5,000 for casinos, U.S. $10,000 for dealers of precious metals and stones, and U.S. $25,000 for notaries, accountants, lawyers, and car dealerships. In addition, service providers are required to confirm the identities of individual or corporate clients before completing requested services and to retain photocopies of identity documents and all other relevant documents pertaining to national and international transactions for a period of seven years. The legislation includes a due diligence section that holds individual bankers responsible if their institution launders money and ensures confidentiality to bankers and others with respect to their cooperation with law enforcement officials.

Statutory requirements limit the international transportation of currency and monetary instruments; amounts in excess of $10,000 must be reported to authorities before entering or leaving Suriname. In addition, any person who wishes to take money in excess of U.S. $10,000 out of the country must notify the Military Police. The Central Bank of Suriname also requires that all transactions in excess of U.S. $10,000 be reported. Suriname does not recognize indigenous alternative remittance systems.

The FIU, which falls under the auspices of the Attorney General's Office, is an administrative body that performs analytical duties. Its responsibilities entail requesting, analyzing, and reporting to the Attorney General's office information on transactions that may constitute money laundering. If necessary, the FIU may request access to the records of other government entities. To facilitate interagency coordination, Suriname has an Anti-Money Laundering Project Team, which consists of representatives from the FIU, Judicial Police, the Attorney General's Office, and the judiciary. Bureaucracy and the lack of financial and human resources have made it difficult for the FIU to perform to its best capabilities. On the basis of a Memorandum of Understanding (MOU), Suriname shares information regarding money laundering with the FIU in the Netherlands. Another MOU was concluded with the Netherlands Antilles in October 2007. The number of unusual transaction reports received by the FIU was not available for 2007.

Suriname's anti-money laundering regime also includes a Financial Investigation Team (FOT) under the authority of the Judicial Police. The FOT is the body responsible for investigating all suspicious transactions identified by the FIU. Upon making a determination that an unusual activity report is indeed suspicious and sufficient to initiate an investigation, the FIU refers the matter to the Attorney General's Office. If the Attorney General's office concurs with the determination, it directs the FOT to conduct an investigation. Prosecutors use evidence collected from FOT investigations to build legal cases. However, the FOT suffers from a lack of personnel and resources that have rendered it largely ineffective over the past year. The 2004 sentencing of an individual to seven years imprisonment for intentional money laundering and for attempting to export a small amount of cocaine remains the most significant and longest money laundering sentence to date. Resource constraints and a severe shortage of judges are proving to be a limiting factor in expanding this success. A new class of seven judges could partially redress the problem, but they will not complete their judicial training until 2008.

While the number of prosecutions in 2007 related to money laundering was not public information, there were several significant convictions in 2007 related to illegal transfers of money. In August 2007, De Surinaamse Bank President Siegmund Proeve and former Bank President Edward Muller were sentenced to six months imprisonment for the illegal transfer of approximately U.S. $14.5 million in casino profits to foreign countries between 1998 and 2003. The defendants were charged with transferring funds without the permission of the Foreign Exchange Commission and for the transfer of amounts over U.S. $10,000 without reporting it to the Central Bank. Other defendants in the case were Procurement Officer Patrick Bagwandin, who was sentenced to a conditional three-month imprisonment, and Canadian Dorsett Group staffer Jeffrey Claque, who was sentenced to six months. The bank was fined U.S. $358,000. The defendants are appealing the case and are serving their sentences while the case is under appeal.

In July 2007, a judge handed down the verdict for a 2006 case in which three people were arrested with a large sum of money and charged with money laundering. Two of the defendants were arrested after police put up a roadblock between Paramaribo and the country's most western district, Nickerie. The police seized the money and the vehicle the two were driving. The three were sentenced to 12 weeks imprisonment and each paid an additional fine of U.S. $3,600. The prosecution filed an appeal in this case, as is possible under Suriname law, to seek a stricter sentence.

Close cooperation between Suriname and the Netherlands led to the 2005 arrest of three persons in a high profile money laundering scandal. In January 2006, one of the three was sentenced by a Dutch court to two-and-a-half years imprisonment for money laundering. In August 2006, the second suspect was convicted in Suriname, also on money laundering charges, and sentenced to one and a half years in prison. The third suspect was former Minister of Trade and Industry Siegfried Gilds, who resigned his position after the Attorney General announced he was under investigation for laundering money and membership in a criminal organization. The former Minister is alleged to have laundered close to $1.27 million between 2003 and 2005. His trial is ongoing.

An amendment to the criminal code enacted in 2003 allows authorities to confiscate illegally obtained proceeds and assets obtained partly or completely through criminal offenses; however, assets cannot be converted to cash or disposed of until the case is settled. New assets forfeiture legislation, which would make this possible, is under consideration in Parliament. There are no provisions for civil forfeiture, and there is no legal mechanism that designates the proceeds gained by the sale of forfeited goods to be used directly for law enforcement efforts. There is no entity for the management and disposition of assets seized and forfeited for narcotics-related money laundering offenses.

The financing of terrorism is not a crime in Suriname. Suriname does have legislation that allows the authorities to freeze assets of those suspected of money laundering. The Central Bank of Suriname circulates to commercial banks the names of individuals/entities that are designated by the United Nations 1267 Sanctions Committee list as associates of Al-Qaeda, the Taliban, or Usama bin Laden.

There are no known cases of charitable or nonprofit entities serving as conduits for financing terrorism in Suriname.

Upon its independence in 1975, Suriname automatically adopted an extradition treaty held between the United States and the Kingdom of the Netherlands into its own legislation, which serves as the extradition treaty between the United States and the Republic of Suriname. The GOS has an agreement with the Netherlands on extradition of nonnationals and mutual legal assistance with regard to criminal matters; but, under Surinamese law, citizens of Suriname "will not be extradited." Money laundering is an extraditable offense. Suriname has bilateral treaties and cooperation agreements with the United States on narcotics trafficking, and with Colombia, France and the Netherlands Antilles on transnational organized crime. In January 2006, Suriname, the Netherlands Antilles, and Aruba signed a Mutual Legal Assistance Agreement allowing for direct law enforcement and judicial cooperation between the countries, making it no longer necessary for the process to be first routed through The Hague. Parties to the Agreement, which covers cooperation with regard to drug trafficking, trafficking in persons, and organized crime, had a follow-up meeting in March 2007 and expanded the cooperation to include information sharing on transnational crime and financial crimes.

Suriname is party to the 1988 UN Drug Convention and, in May 2007, acceded to the UN Convention against Transnational Organized Crime. The GOS is not a party to the UN Convention against Corruption or the Inter-American Convention against Terrorism. Draft legislation to become a party to the UN International Convention for the Suppression of the Financing of Terrorism has been prepared by the Ministry of Justice and Police, and is awaiting the Council of Ministers' approval. Suriname is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Suriname's FIU is not a member of the Egmont Group. In 2006, a joint team from the FIUs of Canada and the United States visited Suriname and agreed to sponsor Suriname's FIU in the Egmont membership process. The two organizations proposed steps to be taken by Suriname to qualify for the Egmont application process. A crucial step recommended is the formal criminalization of terrorist financing, which is a requirement for all new members of the Egmont Group.

The GOS should pass legislation to criminalize terrorist financing. Recent convictions have demonstrated the ability and willingness of the Government of Suriname to combat money laundering. However, the GOS should take steps to further enhance its anti-money laundering regime to conform to international standards. Suriname should devote the necessary resources to effectively investigate and prosecute money laundering cases. The GOS should consider implementing provisions for civil forfeiture, and create a program for the management and disposition of seized and forfeited assets. The GOS should bolster the capacity of the FIU with the necessary personnel and financial resources, and implement reforms to permit the FIU to qualify as a member of the Egmont Group.

Switzerland

Switzerland is a major international financial center. There are 331 banks and a large number of nonbank financial intermediaries. Swiss authorities suspect that Switzerland is vulnerable at the layering and integration stages of the money laundering process. Switzerland's central geographic location, relative political, social, and monetary stability, wide range and sophistication of financial services and long tradition of bank secrecy—first codified in 1934—are all factors that make Switzerland a major international financial center. These same factors also make Switzerland vulnerable to potential money launderers. However, Swiss authorities are aware of these factors and are sensitive to the size of the Swiss banking industry (14.5 percent of GDP) relative to the size of the economy. Moreover, client confidentiality laws, also called bank secrecy, are waived automatically in cases of suspected money laundering and fraud.

Reporting indicates that criminals attempt to launder criminal proceeds in Switzerland via a wide range of illegal activities conducted worldwide. These illegal activities include, but are not limited to, financial crimes, narcotics trafficking, arms trafficking, organized crime, terrorist financing and corruption. Although both Swiss and foreign individuals or entities launder money in Switzerland, foreign narcotics trafficking organizations, often based in the Balkans, Eastern Europe, or South America, dominate the narcotics-related money laundering operations in Switzerland.

Swiss bank accounts also figure in fraud and corruption of foreign government officials and heads-of-state. Recent examples of public figures that have been the subject of Swiss money laundering allegations or investigations include a former Kyrgyzstan President, a former Russian Minister of Atomic Energy, the Nigerian dictator Sani Abacha, former Pakistani Prime Minister Benazir Bhutto, and former Haiti President Jean-Claude Duvalier. These individuals have Swiss bank accounts and have moved national funds to Switzerland for personal use. Swiss bank routinely screen PEPs (Politically Exposed Persons) accounts for illicit money transfers.

Switzerland has significant anti-money laundering (AML) legislation in place, making banks and other financial intermediaries subject to strict know-your-customer (KYC) and reporting requirements. Switzerland has also implemented legislation for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets. Legislation that aligns the Swiss supervisory arrangements with the Basel Committee's "Core Principles for Effective Banking Supervision" is contained in the Swiss Money Laundering Act. Money laundering is a criminal offense in Switzerland. However, Swiss law, does not recognize certain types of criminal offenses as predicate offenses for money laundering, including illegal trafficking in migrants, counterfeiting and pirating of products, smuggling, insider trading, and market manipulation.

Swiss money laundering laws and regulations apply to both banks and nonbank financial institutions. The Federal Banking Commission, the Federal Office of Private Insurance, and the Swiss Federal Gaming Board serve as primary oversight authorities for a number of financial intermediaries, including banks, securities dealers, insurance institutions, and casinos. Other financial intermediaries are required to either come under the direct supervision of the Money Laundering Control Authority (MLCA) of the Federal Finance Department or join an accredited self-regulatory organization (SRO). SROs are nongovernmental self-regulating organizations authorized by the Swiss government to oversee implementation of AML measures by their members. The SROs must be independent of the management of the intermediaries they supervise and must enforce compliance with due diligence obligations. Noncompliance can result in a fine or a revoked license. About 6,000 financial intermediaries are associated with SROs; the majority of these are financial management companies.

The Swiss Federal Banking Commission's AML regulations were revised in 2002 and became effective in 2003. These regulations, aimed at the banking and securities industries, codify a risk-based approach to suspicious transaction and client identification and install a global know-your-customer risk management program for all banks, including those with branches and subsidiaries abroad. In the case of higher-risk business relationships, additional investigations by the financial intermediary are required. The regulations require increased due diligence in the cases of politically exposed persons (PEPs) by ensuring that decisions to commence relationships with such persons be undertaken by at least one member of the senior executive body of a financial institution. All provisions apply to correspondent banking relationships as well. Swiss banks may not maintain business relationships with shell banks (banks with no physical presence at their place of incorporation), but there is no requirement that banks ensure that foreign clients do not authorize shell banks to access their accounts in Swiss banks.

The 2002 Banking Commission regulations mandate that all cross-border wire transfers must contain identifying details about the funds' remitters, though banks and other covered entities may omit such information for "legitimate reasons." The Swiss Federal Banking Commission has said that there are

no plans at the moment to follow EU regulations aimed at registering names, addresses, and account numbers of everyone making even small money transfers between EU member states.

Revisions to the Swiss Penal Code regarding terrorist financing entered into force on October 1, 2003. Article 260 of the Penal Code provides for a maximum sentence of five years' imprisonment for terrorist financing. Article 100 of the Penal Code, also added in 2003, extends criminal liability for terrorist financing to include companies. The Financial Action Task Force's 2005 mutual evaluation of Switzerland found it "largely compliant" with FATF Special Recommendation II regarding the criminalization of terrorist financing; however, it noted that the Swiss Penal Code criminalizes the financing of an act of criminal violence, not the financing of an individual, independent of a particular act. The evaluation also noted that Switzerland wasn't compliant with respect to correspondent banking, beneficial ownership of legal persons, and cash couriers. On 29 September 2006 the Federal Council decided on the next steps regarding the implementation of the revised FATF recommendations to combat money laundering and terrorist financing, and on extending the scope of the Money Laundering Act to cover terrorist financing. The adoption of anti-money laundering (AML) regulations planned for 2008-2009 will make these crimes predicate offenses.

In June 2007, the Swiss Parliament approved a new financial market regulation bill aimed at creating a new regulator to boost the image of Switzerland's financial workplace by combining the activities of three existing watchdog groups. But the Federal Financial Market Supervisory Authority (FINMA) will be delayed for a year and has been criticized in some quarters for lacking full autonomy from the government. FINMA will finally group together the regulatory work of the Federal Banking Commission, the Federal Office of Private Insurance and the Money Laundering Control Authority at the beginning of 2009. It will investigate suspected cases of money laundering and corruption. The FINMA is scheduled to become operational in early 2009.

The Swiss do not have laws comparable to those in the U.S. to report large cash transactions, cross-border currency declarations, and large cash purchases. As a result, the Swiss are unable to effectively initiate bulk cash investigations because they have no legal reporting requirement for cash into or out of Switzerland. Switzerland does have suspicious transaction reports (STRs), which are referred to law enforcement through the Money Laundering Reporting Office (MROS)—the Swiss financial intelligence unit (FIU).

Switzerland's banking industry offers the same account services for both residents and nonresidents. These can be opened through various intermediaries who advertise their services. As part of Switzerland's international financial services, banks offer certain well-regulated offshore services, including permitting nonresidents to form offshore companies to conduct business, which can be used for tax reduction purposes. Pursuant to an agreement signed between the EU and Switzerland in 2004, EU residents have tax withheld on interest payments from savings accounts based in Switzerland. This measure, enacted in concert with the EU's Savings Directive (2003/48/EC), was implemented on July 1, 2005.

Swiss commercial law does not recognize any offshore mechanism per se and its provisions apply equally to residents and nonresidents. The stock company and the limited liability company are two standard forms of incorporation offered by Swiss commercial law. The financial intermediary is required to verify the identity of the beneficial owner of the stock company and must also be informed of any change regarding the beneficial owner. Bearer shares may be issued by stock companies but not by limited liability companies.

Switzerland has duty free zones. Customs authorities supervise the admission into and the removal of goods from customs warehouses. Warehoused goods may only undergo manipulations necessary for their maintenance, such as repacking, splitting, sorting, mixing, sampling and removal of the external packaging. Any further manipulation is subject to authorization. Goods may not be manufactured in the duty free zones. Swiss law has full force in the duty free zones; for example, export laws on

strategic goods, war material, and medicinal products, as well as laws relating to anti-money laundering prohibitions, all apply.

Switzerland ranks fifth in the highly profitable artwork trading market, exporting SFr. 1,592 million (approximately U.S. $1,460,000) worth of artwork in 2004. Because of the size of the Swiss art market organized crime has attempted to transfer stolen art or to use art to launder criminal funds via Switzerland. The United States is by far Switzerland's most important trading partner in this area, having purchased U.S. $578 million worth (or 36 percent) of works of art in 2006. The 2003 Cultural Property Transfer Act, implemented in June 2005, codifies in Swiss law elements of the 1970 United Nations Educational, Scientific, and Cultural Organization (UNESCO) Convention. This measure increases from five to thirty years the time period during which stolen pieces of art may be confiscated from those who purchased them in good faith. The law also allows police forces to search bonded warehouses and art galleries.

The MROS or FIU is charged with receiving and processing suspicious transaction reports (STRs). MROS does not have any investigative powers of its own nor can it obtain additional information from reporting entities after receiving a STR. Last year, banks submitted the highest number of reports in relative terms (over 58 percent.) The payment services sector followed with 26.5 percent of all STRs filed. By canton, Zurich is on the top of the list of filing STRs with 18 percent, followed by Tessin with 14 percent and Geneva with 10 percent.

In 2006, eight reports were received by the MROS regarding terrorist finance; 20 reports were received in 2005. Out of the total number (154) of STRs submitted since 2001 in connection with suspected terrorist financing, 149 or 97 percent have been forwarded to law enforcement agencies. Suspicious activity reports were often prompted by press reports. If one compares the figures for the categories with those for 2005, it is apparent that outside information was an increasingly important factor in 2006. More than 56 percent of STRs were prompted by outside information in 2006 as opposed to 41 percent in 2005. Of these 149, 44 cases have been dropped, 5 cases have been temporarily suspended and 100 cases are still pending.

Under the 2002 Efficiency Bill, the Swiss Attorney General is vested with the power to prosecute crimes addressed by Article 340 of the Swiss Penal Code, which also covers money laundering offenses. In the past, the individual cantons (administrative components of the Swiss Confederation) were charged with investigating money laundering offences. Additional legislation increased the effectiveness of the prosecution of organized crime, money laundering, corruption, and other white-collar crime, by increasing the personnel and financing of the criminal police section of the federal police office. The law confers on the Federal Police and Attorney General's office the authority to take over cases that have international dimensions, involve several cantons, or which deal with money laundering, organized crime, corruption, and white collar crime.

If financial institutions determine that assets were derived from criminal activity, the assets must be frozen immediately until a prosecutor decides on further action. Under Swiss law, suspect assets may be frozen for up to five days while a prosecutor investigates the suspicious activity. Switzerland cooperates with the United States to trace and seize assets, and has shared a large amount of funds seized with the U.S. Government (USG) and other governments. The Government of Switzerland (GOS) has worked closely with the USG on numerous money laundering cases. Swiss legislation permits "spontaneous transmittal," a process allowing the Swiss investigating magistrate to signal to foreign law enforcement authorities the existence of evidence in Switzerland. Eight percent of the 1,693 foreign judicial assistance requests originated from the U.S. However, Swiss privacy laws make it extremely difficult for bank officials and Swiss police to divulge financial crime information to U.S. authorities absent a Mutual Legal Assistance Treaty (MLAT) request or Letters Rogatory.

Since September 11, 2001, Swiss authorities regularly alert banks and nonbank financial intermediaries to check their records and accounts against lists of persons and entities with links to

terrorism. The accounts of these individuals and entities are to be reported to the Ministry of Justice as suspicious transactions. Based on the "state security" clause of the Swiss Constitution, the authorities have ordered banks and other financial institutions to freeze the assets of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list.

Along with the U.S. and UN lists, the Swiss Economic and Finance Ministries have drawn up their own list of individuals and entities connected with international terrorism or it's financing. Swiss authorities have thus far blocked about 48 accounts totaling SFr. 25.5 million (approximately U.S. $20,648,360) from individuals or companies linked to individuals or entities listed pursuant to relevant UN resolutions. The Swiss Attorney General also separately froze 41 accounts representing about SFr. 25 million (approximately U.S. $22,943,800) on the grounds that they were related to terrorist financing, but the extent to which these funds overlap with the UN consolidated list has yet to be determined.

Switzerland has ratified the Council of Europe's Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Switzerland is a party to the 1988 UN Drug Convention. Switzerland ratified the UN Convention against Transnational Organized Crime on October 27, 2006. Swiss ratification of the UN Convention against Corruption is still pending.

Swiss authorities cooperate with counterpart bodies from other countries. Switzerland has a mutual legal assistance treaty in place with the United States, and Swiss law allows authorities to furnish information to U.S. regulatory agencies, provided it is kept confidential and used for supervisory purposes. Switzerland is a member of the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision, and its FIU is a member of the Egmont Group.

The Government of Switzerland hopes to correct the country's image as a haven for illicit banking services. The Swiss believe that their system of self-regulation, which incorporates a "culture of cooperation" between regulators and banks, equals or exceeds that of other countries. The primary interest of the Swiss system is to avert bad risks by countering them at the account-opening phase, where due diligence and know-your-customer procedures address the issues, rather than relying on an early-warning system on all filed transactions. The GOS believes that because of the due diligence approach the Swiss have taken, there are fewer STRs filed than in some other countries. At the same time, 82 percent of the STRs that are filed lead to the opening of criminal investigations. While generally positive, Switzerland's FATF mutual evaluation report nonetheless identified weaknesses in the Swiss anti-money laundering and counter-terrorist financing regime, including problems with correspondent banking and the identification of beneficial owners. Per FATF Special Recommendation IX, the GOS should implement cross-border currency reporting requirements. Switzerland should also put forward effective AML legislation and rules that monitor and regulate money service businesses.

Syria

Syria is not an important regional or offshore financial center, due primarily to its still underdeveloped private banking sector and the fact that the Syrian pound is not a fully convertible currency. Despite rapid growth in the banking sector since 2004, industry experts estimate that only eight percent of Syria's population of nearly 20 million people actually uses banking services. Consequently, some 70 percent of all business transactions are still conducted in cash. Additionally, there continue to be significant money laundering and terrorist financing vulnerabilities in Syria's financial and nonbank financial sectors that have not been addressed by necessary legislation or other government action. Syria's black market moneychangers are not adequately regulated, and the country's borders remain porous. Regional hawala networks are intertwined with smuggling and trade-based money laundering and raise significant concerns, including involvement in the financing of terrorism. The most obvious

indigenous money laundering threat involves Syria's political and business elite, whose corruption and extra-legal activities continue unabated. The U.S. Department of State has designated Syria as a State Sponsor of Terrorism.

The Syrian banking sector is dominated by the Commercial Bank of Syria (CBS), which holds approximately 75 percent of all deposits and controls most of the country's foreign currency reserves. With growing competition from private banks, CBS and the country's four other specialized public banks—the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank—have begun offering a broader range of retail services to private customers. However, these state-owned banks still retain a monopoly on all government banking business, and account for some 80 percent of all bank branches nationwide. Furthermore, as a state-owned bank, CBS has no bottom-line incentive to stop financing Syria's many poor-performing public enterprises.

In May 2004, the U.S. Department of Treasury designated CBS, along with its subsidiary, the Syrian Lebanese Commercial Bank, as a financial institution of "primary money laundering concern," pursuant to Section 311 of the USA PATRIOT Act. This designation resulted from information that CBS has been used by terrorists or persons associated with terrorist organizations, as a conduit for the laundering of proceeds generated from the illicit sale of Iraqi oil, and continued concerns that CBS is vulnerable to exploitation by criminal and/or terrorist enterprises. In April 2006, Treasury promulgated a final rule, based on the 2004 designation, prohibiting U.S. financial institutions from maintaining or opening correspondent accounts with CBS or its Syrian Lebanese Commercial Bank subsidiary.

The Syrian Arab Republic Government (GOS) began taking steps to develop a private banking sector in April 2001, with Law No. 28, which legalized private banking, and Law No. 29, which established rules on bank secrecy. Under Law No. 28, subsidiary branches of private foreign banks are required to have 51 percent Syrian ownership to be licensed in Syria. Bank of Syria and Overseas, a subsidiary of Lebanon's BLOM Bank, was the first private bank to open in Syria in January 2004. There are now seven private banks in Syria, including Bank of Syria and Overseas (BSOM), Banque BEMO Saudi Fransi, the International Bank for Trade and Finance, Bank Audi, Arab Bank, Byblos Bank, and Syria Gulf Bank. Three more private banks, the Bank of Jordan, Fransa Bank and Qatar National Bank have obtained the necessary licenses and are expected to begin operations in Syria in 2008. A new law was enacted in May 2005 that allows for the establishment of Islamic banks and the first such bank, al-Sham Islamic Bank, began operations in August 2007. Shortly thereafter, Syria International Islamic Bank (IIB) opened its doors in September. Al-Baraka Islamic Bank was also officially licensed in 2007 and is expected to begin operations in early 2008.

By mid-2007, the Syrian banking sector reported assets totaling U.S. $29.5 billion and held deposits totaling $17.2 billion. Syrian banks are playing an increasing role in providing the business sector with foreign currency to finance imports and as a source of credit for businesses and individuals. However, the sector's development is hampered by the continuing lack of human expertise in finance, insufficient automation and communication infrastructure, regulations that limit Syrian banks' ability to make money on their liquidity, and restrictions on foreign currency transactions.

Syria's free trade zones also may provide an easy entry or transit point for the proceeds of criminal activities. There are seven free zones in Syria, serviced mostly by subsidiaries of Lebanese banks, including BLOM (Bank du Liban et d'Autre Mer), BEMO (Banque Europeenne Pour le Moyen-Orient Sal), BBAC (Bank of Beirut and Arab Countries), Bank Societee Generale, Fransa Bank, SBA (Societee du Banks Arabe) and Basra International Bank. Four additional public free zones are planned to be established in Homs, Dayr al Zur, Idleb, and the Port of Tartous. The Al-Ya'rubiyeh free zone in al-Hasakeh province, near the northeastern Syrian-Iraqi border, is scheduled to be opened in early 2008.

In recent years, both China and Iran announced plans to build free zones in Syria, although Iran later dropped this idea in favor of pursuing a regular Free Trade Agreement with Syria. China's free zone in

Adra, however, is on-schedule to provide roughly 200 Chinese companies with a regional gateway for their goods. Recently, a Syrian investor, in cooperation with partners from the Gulf, obtained preliminary approval for the establishment of a private free zone near the al-Tanf border crossing with Iraq. The volume of goods entering the free zones is estimated to be in the billions of dollars and is growing, especially with increasing demand for automobiles and automotive parts, which enter the zones free of customs tariffs before being imported into Syria. While all industries and financial institutions in the free zones must be registered with the General Organization for Free Zones, which is part of the Ministry of Economy and Trade, the Syrian General Directorate of Customs continues to lack strong procedures to check country of origin certification or the resources to adequately monitor goods that enter Syria through the zones. There are also continuing reports of Syrians using the free zones to import arms and other goods into Syria in violation of USG sanctions under the Syrian Accountability and Lebanese Sovereignty Act.

Legislation approved in the last few years provides the Central Bank of Syria with new authority to supervise the banking sector and investigate financial crimes. In September 2003, the GOS passed Decree 59; this criminalized money laundering and created an Anti-Money Laundering Commission (Commission) in May 2004. In response to international pressure to improve its anti-money laundering and counter-terrorist financing (AML/CTF) regulations, the GOS passed Decree 33 in May 2005, which strengthened the Commission and empowered it to act as a Financial Intelligence Unit (FIU). The Decree finalized the Commission's composition to include the Governor of the Central Bank, a Supreme Court Judge, the Deputy Minister of Finance, the Deputy Governor for Banking Affairs, and the GOS's Legal Advisor, and will include the Chairman of the Syrian Stock Market once the market is operational.

Under Decree 33, all banks and nonbank financial institutions are required to file reports with the Commission for transactions over $10,000, as well as Suspicious Transaction Reports (STRs) regardless of amount. They are also required to use "know your customer" (KYC) procedures to follow up on their customers every three years and maintain records on closed accounts for five years. The chairmen of Syria's private banks continue to report that they are employing internationally recognized KYC procedures to screen transactions and also employ their own investigators to check suspicious accounts. Nonbank financial institutions must also file STRs with the Commission, but many of them continue to be unfamiliar with the requirements of the law. The Commission has organized workshops for these institutions over the past two years, but more time is needed for the information to penetrate the market.

Once a STR has been filed, the Commission has the authority to conduct an investigation, waive bank secrecy on specific accounts to gather additional information, share information with the police and judicial authorities, and direct the police to carry out a criminal investigation. In addition, Decree 33 empowers the Governor of the Central Bank, who is the chairman of the Commission, to share information and sign Memoranda of Understanding (MOUs) with foreign FIUs. In November 2005, the Prime Minister announced that the Commission had completed an internal reorganization, creating four specialized units to: oversee financial investigations; share information with other GOS entities including customs, police and the judiciary; produce AML/CTF guidelines and verify their implementation; and develop a financial crimes database.

Decree 33 provides the Commission with a relatively broad definition of what constitutes a crime of money laundering, but one that does not fully meet international standards. The definition includes acts that attempt to conceal the proceeds of criminal activities, the act of knowingly helping a criminal launder funds, and the possession of money or property that resulted from the laundering of criminal proceeds. In addition, the law specifically lists thirteen crimes that are covered under the AML legislation, including narcotics offenses, fraud, and the theft of material for weapons of mass destruction. It is unclear whether terrorist financing is a predicate offense for money laundering or otherwise punishable under Decree 33.

While a STR is being investigated, the Commission can freeze accounts of suspected money launderers for a nonrenewable period of up to eighteen days. The law also stipulates the sanctions for convicted money launderers, including a three to six-year jail sentence and a fine that is equal to or double the amount of money laundered. Further, the law allows the GOS to confiscate the money and assets of the convicted money launderer. The Commission circulates among its private and public banks the names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanction Committee's consolidated list. has taken action to freeze the assets of designated individuals, but has not frozen the assets of any Syrian citizens in 2007.

In 2007, the Commission investigated 130 suspicious transaction cases, 15 of which were forwarded by foreign countries, including Qatar, Croatia and Ukraine. Eleven of these cases were referred to the criminal court system for prosecution. Over the past two years, the Commission investigated 263 cases and referred 34 of them to the criminal court system. At the end of 2007, all criminal cases are pending, and there have been no convictions. Most Syrian judges are not yet familiar with the evidentiary requirements of the law. Furthermore, the slow pace of the Syrian legal system and political sensitivities delay quick adjudication of these issues. The Commission itself continues to be seriously hampered by human resource constraints, although it has increased its staff from six in 2005 to ten in 2007, and hopes to expand to 30 by the end of 2008. However, the lack of expertise further undermined by a lack of political will continues to impede effective implementation of existing AML/CTF regulations.

The GOS has not updated its laws regarding charitable organizations to include strong AML/CTF language. A promised updated draft law is still pending. The GOS decided at the end of 2004 to restrict charitable organizations to only distributing nonfinancial assistance, but the current laws do not require organizations to submit detailed financial information or information on their donors. While the Commission says that it is seeking to increase cooperation with the Ministry of Social Affairs and Labor, which is supposed to approve all charitable transactions, this remains a largely unregulated area.

Although Decree 33 provides the Central Bank with the legal basis to combat money laundering, most Syrians still do not maintain bank accounts or use checks, credit cards, or ATM machines. The Syrian economy remains primarily cash-based, and Syrians use moneychangers, some of whom also act as hawaladars, for many financial transactions. Estimates of the volume of business conducted in the black market by Syrian moneychangers range between $15-70 million per day. Even the GOS admits that it does not have visibility into the amount of money that currently is in circulation. The GOS has begun issuing new regulations to entice people to use the banking sector, including offering high interest certificates of deposit and allowing Syrians to access more foreign currency from banks when they are traveling abroad. The GOS also passed a Moneychangers Law in 2006 to try to regulate the sector, requiring moneychangers to receive a license. However, it is unlikely that black market currency transactions will enter the formal sector because the GOS has still not offered adequate incentives; there is a 25 percent tax on these transactions, inadequate enforcement mechanisms, and continuing restrictions on foreign currency transfers. Although moneychangers had until the end of 2006 to license their operations, to date, only nine moneychangers applied for licensing and just two money exchange offices have begun operating legally. The Commission does have the authority to monitor the sector under Decree 33, but the GOS has not yet begun investigating illegal money-changing operations. Consequently, hawaladars in Syria's black market remain a source of concern for money laundering and terrorist financing.

While the GOS maintains strict controls on the amount of money that individuals can take with them out of the country, there is a high incidence of cash smuggling across the Lebanese, Iraqi, and Jordanian borders. Most of the smuggling involves the Syrian pound, as a market for Syrian currency exists among expatriate workers and tourists in Lebanon, Jordan, and the Gulf countries. U.S. dollars are also commonly smuggled in the region. Some of the smuggling may involve the proceeds of

narcotics and other criminal activity. In addition to cash smuggling, there also is a high rate of commodity smuggling out of Syria, particularly of diesel fuel, prompted by individuals buying diesel domestically at the low subsidized rate and selling it for much higher prices in neighboring countries. There are reports that some smuggling is occurring with the knowledge of or perhaps even under the authority of the Syrian security services.

The General Directorate of Customs lacks the necessary staff and financial resources to effectively handle the problem of smuggling. And while it has started to enact some limited reforms, including the computerization of border outposts and government agencies, problems of information-sharing remain. In September 2006, the Minister of Finance issued a decision stipulating the establishment of a unit specializing at combating money laundering and terrorist financing in the General Directorate of Customs. Additionally, Customs currently lacks the infrastructure to effectively monitor or control even the legitimate movement of currency across its borders. The Commission and Customs have reportedly implemented a form asking individuals to voluntarily declare currency when entering or exiting the country, although consistency of implementation and any action resulting from enforcement remain unknown.

Syria is one of the fourteen founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body. In 2006, Syria underwent a mutual evaluation by its peers in MENAFATF and the released evaluation report found Syria to be fully compliant with five of the 49 recommendations, largely compliant on eight, partially compliant on 26 and noncompliant on eight, although two of those eight recommendations were not applicable to Syria. In 2007, the Syrian FIU became a fully accepted member of the Egmont Group.

Syria is a party to the 1988 UN Drug Convention. In April 2005, it became a party to the International Convention on the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Syria has signed, but not ratified the UN Convention against Corruption. Syria is ranked 138 out of 180 countries on Transparency International's 2007 Corruption Perception Index

While Syria has made modest progress in implementing AML/CTF regulations that govern its formal financial sector, the continuing lack of transparency of the state-owned banks and their vulnerability to political influence reveals the absence of political will to address AML/CTF in the largest part of the banking sector. In addition, nonbank financial institutions and the black market will continue to be vulnerable to money laundering and terrorist financiers. To build confidence in Syria's intentions, the Central Bank should be granted independence and supervisory authority over the entire sector. Additionally, Syria should continue to modify its AML/CTF legislation and enabling regulations so that they adhere to global standards. The General Directorate of Customs, the Central Bank, and the judicial system in particular continue to lack the resources and the political will to effectively implement AML/CTF measures. Although the GOS has stated its intention to create the technical foundation through which different government agencies could share information about financial crimes, this does not exist. In addition, it remains doubtful that the GOS has the political will to punish terrorist financing, by classifying what it sees as legitimate resistance groups as terrorist organizations, or to address the corruption that exists at the highest levels of government and business. All of these issues remain obstacles to developing a comprehensive and effective AML/CTF regime in Syria. The GOS should become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Taiwan

Taiwan's modern financial sector and its role as a hub for international trade make it susceptible to money laundering. Its location astride international shipping lanes makes it vulnerable to transnational crimes, such as narcotics trafficking, trade fraud, and smuggling. There has traditionally been a

significant volume of informal financial activity through unregulated nonbank channels, but in recent years Taiwan has taken steps to shift much of this activity into official, regulated financial channels. Most illegal or unregulated financial activities are related to tax evasion, fraud, or intellectual property violations. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes most commonly linked to SAR reporting include financial crimes, corruption, and other general crimes.

Taiwan's anti-money laundering legislation is embodied in the Money Laundering Control Act (MLCA) of April 23, 1997, which was amended in 2003 and in 2007. Its major provisions include a list of predicate offenses for money laundering, customer identification and record keeping requirements, disclosure of suspicious transactions, international cooperation, and the creation of a financial intelligence unit (FIU), the Money Laundering Prevention Center (MLPC).

The MLPC, a law enforcement-style FIU, is located within the Ministry of Justice Investigation Bureau (MJIB). The FIU is tasked to receive, analyze, and disseminate suspicious transaction reports, currency transaction reports and cross-border currency movement declaration reports. The MLPC also assists other law enforcement authorities to investigate money laundering and terrorist financing cases. MLPC staff has law enforcement status.

The 2003 amendment expanded the list of predicate crimes for money laundering, widened the range of institutions subject to suspicious transaction reporting, and mandated compulsory reporting to the MLPC of significant currency transactions in excess of New Taiwan dollars (NT $) 1 million (approximately U.S. $30,980). As of November 2007, the MLPC received 1,065,879 currency transaction reports and in 2006 it received 1,089,768. The amendments further expanded the scope of reporting entities beyond traditional financial institutions to include: automobile dealers, jewelers, boat and aviation dealers, real estate brokers, credit cooperatives, consulting companies, insurance companies, and securities dealers.

In July 2007, the MLCA was amended to expand its coverage to include a new agricultural bank, trust companies, and newly licensed currency exchanges as well as hotels, jewelry stores, postal offices, temples, and bus/railway stations. The list of predicate offenses was expanded to include offenses against the Public Procurement Law, Bills Finance Management Law, Insurance Law, Financial Holding Company Law, Trust Law, Credit Cooperative Association Law, and Agriculture Financing Law. The number of agencies with money laundering responsibilities was expanded from the Ministry of Justice, Ministry of Transportation and Communication, and Ministry of Finance to include also the Financial Supervisory Commission (established in July 2004), Ministry of Economic Affairs, Council of Agriculture (supervising a new agriculture bank and the credit departments of farmers' and fisherman's associations), and Taiwan's Central Bank (monitoring currency exchanges). The amended law also authorized Taiwan agencies to share information obtained from the MLCA with law enforcement agencies in countries that have signed a mutual legal assistance agreement (MLAA) with Taiwan and on a reciprocal basis with other countries.

Taiwan set up a single financial regulator, the Financial Supervisory Commission (FSC) on July 1, 2004. The FSC consolidates the functions of regulatory monitoring for the banking, securities, futures and insurance industries, and also conducts financial examinations across these sectors. In mid-December 2005, the FSC began an incentive program for the public to provide information on financial crimes. The reward for information on a financial case with fines of NT $10 million (approximately U.S. $309,000) or at least a one-year sentence is up to NT $500,000 (approximately U.S. $15,500). The reward for information on a case with a fine of between NT $2 and $10 million (approximately U.S. $61,500 and $308,000) or less than a one-year sentence is up to NT $200,000 (approximately U.S. $6,200).

Two new articles added to the 2003 amendments to the MLCA grant prosecutors and judges the power to freeze assets related to suspicious transactions and give law enforcement more powers related to

asset forfeiture and the sharing of confiscated assets. The 2007 amendment to the MLCA permits the freezing of proceeds of money laundering for up to one year. In terms of reporting requirements, financial institutions are required to identify, record, and report the identities of customers engaging in significant or suspicious transactions. There is no threshold amount specified for filing suspicious transaction reports. The time limit for reporting cash transactions of over NT $1 million is five business days. Banks are barred from informing customers that a suspicious transaction report has been filed. Reports of suspicious transactions must be submitted to the MLPC within 10 business days. In 2006, the MLPC received 1,281 suspicious transaction reports and 689 of them resulted in prosecutions. As of November 2007, the MLPC received 2,953 reports. Thirty of them involved an amount exceeding NT $5 million (approximately U.S. $154,600), which resulted in prosecutions based on the MCLA. Of these 30 cases, 19 relate to financial crimes, four to corruption, one to narcotics, and six to other miscellaneous crimes.

Institutions are also required to maintain records necessary to reconstruct significant transactions. Bank secrecy laws are overridden by anti-money laundering legislation, allowing the MPLC to access all relevant financial account information. Financial institutions are held responsible if they do not report suspicious transactions. In May 2004, the Ministry of Finance issued instructions requiring banks to demand two types of identification and to retain photocopies of the identification cards when bank accounts are opened on behalf of a third party, to prove the true identity of the account holder. Individual bankers can be fined NT $200,000 to $1 million (approximately U.S. $6,200 to $30,900) for not following the provisions of the MLPA. Starting in August 2006, the Financial Supervisory Commission required banking institutions to collect, verify and store information about any banking customer that makes any single cash or electronic remittance above NT $30,000 (approximately $927). The requirement was adopted in response to suggestions submitted to Taiwan in 2004 by the FATF.

All foreign financial institutions and offshore banking units follow the same regulations as domestic financial entities. Offshore banks, international businesses, and shell companies must comply with the disclosure regulations from the Central Bank, the Banking Bureau of the Financial Supervisory Commission, and MLPC. These supervisory agencies conduct background checks on applicants for banking and business licenses. Offshore casinos and Internet gambling sites are illegal. According to the Central Bank, as of September 2007, Taiwan hosted 32 local branches of foreign banks, two trust and investment companies, and 65 offshore banking units.

On January 5, 2006, legislation was ratified to allow expansion of offshore banking unit (OBU) operations to the same scope as Domestic Business Units (DBU). This was done to assist China-based Taiwan businesspeople in financing their business operations. DBUs engaging in cross-strait financial business must follow the regulations of the "Act Governing Relations between Peoples of the Taiwan Area and the Mainland Area" and "Regulations Governing Approval of Banks to Engage in Financial Activities between the Taiwan Area and the Mainland Area." The Competent Authority, as referred to in these Regulations, is the Financial Supervisory Commission (FSC).

Taiwan prosecuted 689 cases involving money laundering in 2006, compared with 947 cases involving financial crimes during the same period of 2005. Among the 689 cases, 631 involved unregistered stock trading, credit card theft, currency counterfeiting or fraud. Among the 58 other money laundering cases, 11 were corruption-related and one was drug-related. In July 2007, the MCLA was amended so that only cases involving amounts exceeding NT $5 million (U.S. $154,578) were covered under the MLCA, while the rest were handled in accordance with other laws. Figures for the full year are not available yet, but the number of MLCA-based prosecution cases in the first 11 months dropped to 30. Using the most current figures available, between January and October 2007, the number of drug-related investigations reached 73,411, an increase of 13.4 percent when compared to the same period in 2006. Only 10 percent of these cases were related to drug trafficking. The number of subjects investigated in 2007 increased 10.9 percent to 71,202 from January-October 2006. The number of

indicted subjects grew 36 percent to 31,614 from January-October 2007 and the number of subjects cleared further declined 5.6 percent to 16,657.

To comply with Financial Action Task Force (FATF) Special Recommendation Nine on bulk cash smuggling, the July 2007 legislation required individuals to report currency transported into or out of Taiwan in excess of NT $60,000 (approximately U.S. $1,850), U.S. $10,000 in foreign currency, 20,000 Chinese Yuan (approximately U.S. $2,700), or gold worth more than U.S. $20,000. When foreign currency in excess of NT $500,000 (approximately U.S. $15,400) is brought into or out of Taiwan, the bank customer is required to report the transfer to the Central Bank, though there is no requirement for Central Bank approval prior to the transaction. Prior approval is required, however, for exchanges between New Taiwan dollars and foreign currency when the amount exceeds U.S. $5 million for an individual resident and U.S. $50 million for a corporate entity. Starting August 1, 2006, those who transfer funds over NT $30,000 (approximately U.S. $900) at any bank in Taiwan must produce a photo ID, and the bank must record the name, ID number and telephone number of the client.

The authorities on Taiwan are actively involved in countering the financing of terrorism. A new "Counter-Terrorism Action Law" (CTAL) has been under review by the Legislative Yuan since 2003. The new law would explicitly designate the financing of terrorism as a major crime. Under the proposed CTAL, the National Police Administration, the MJIB, and the Coast Guard would be able to seize terrorist assets even without a criminal case in Taiwan. Also, in emergency situations, law enforcement agencies would be able to freeze assets for three days without a court order.

Assets and income obtained from terrorist-related crimes could also be permanently confiscated under the proposed CTAL, unless the assets could be identified as belonging to victims of the crimes. Under the MLCA Taiwan officials currently have the authority to freeze and/or seize terrorist-related financial assets. Under the Act, the prosecutor in a criminal case can initiate freezing assets, or without criminal charges, the freezing/seizure can be done in response to a request made under a treaty or international agreement.

The Banking Bureau of the FSC circulates the names of individuals and entities included on the UN 1267 Sanctions Committee's consolidated list, as well as names designated by the U.S. Treasury, to all domestic and foreign financial institutions and relevant government agencies. Banks are required to file a report on cash remittances if either of the parties involved are on a terrorist list. Although, as noted above, Taiwan does not yet have the authority to confiscate the assets, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism.

Alternative remittance systems, or underground banks, are considered to be operating in violation of Banking Law Article 29. Authorities in Taiwan consider these entities to be unregulated financial institutions. Foreign labor employment brokers, after obtaining approval from the Central Bank, are authorized to use banks to remit income earned by foreign workers to their home countries. These brokers may not start the remittance services before they obtain the guaranty of their correspondent banks. They are required to sign and retain a standard remittance service contract with foreign workers and establish remittance records for each contracting foreign worker. There were 25 foreign labor employment brokers as of December 2007. If brokers accept money in Taiwan dollars for delivery overseas in another currency, they are violating Taiwan law. It is illegal for retail outlets to accept money in Taiwan dollars and remit it overseas. Violators are subject to a maximum of three years in prison, and/or forfeiture of the remittance, and/or a fine equal to the remittance amount.

In April 2007, the Ministry of Justice Investigation Bureau (MJIB) uncovered a 13-office network engaged in cross-Strait underground remittances and money laundering. The network's accounting records showed that cross-Strait underground remittances through the network exceeded NT $2.1 billion (U.S. $63 million). The MJIB arrested eight persons. Over the past five years, the MJIB has

uncovered 43 cross-Strait underground remittance channels involving capital flows totaling NT $136.2 billion (U.S. $4.2 billion).

Authorities in Taiwan do not believe that charitable and nonprofit organizations in Taiwan are being used as conduits for the financing of terrorism. Such organizations are required to register with the government and, like any other individual or corporate entity, are checked against list of names designated by the United Nations or the U.S. Treasury as being involved in terrorist financing activities. The Ministry of Interior (MOI) is in charge of overseeing foundations and charities. In 2004 and in 2006, the MOI assigned public accountants to audit the financial management of nationwide foundations.

Article 3 of Taiwan's Free Trade Zone Establishment and Management Act defines a Free Trade Zone (FTZ) as a controlled district of an international airport or an international seaport approved by the Executive Yuan. The FTZ coordination committee, formed by the Executive Yuan, has the responsibility of reviewing and examining the development policy of the FTZ, the demarcation and designation of FTZs, and inter-FTZ coordination.

There are five FTZs in Taiwan, all of which have opened since 2004, including the Taipei Free Trade Zone, the Taichung Free Trade Zone, the Keelung Free Trade Zone, the Kaohsiung Free Trade Zone, and the Taoyuan Air Cargo Free Trade Zone. These FTZs were designated with different functions, so that Keelung and Taipei FTZs focus on international logistics; Taoyuan FTZ on adding value to high value added industries; Taichung FTZ on warehousing, transshipment and processing of cargo; and Kaohsiung FTZ on mature industrial clusters. According to the Center for Economic Deregulation and Innovation (CEDI) under the Council for Economic Planning & Development, as of November 2007 there were 17 shipping and logistics companies listed in the Kaohsiung Free Trade Zone, 19 logistics companies in Taichung Free Trade Zone, 11 logistics and shipping companies in Keelung Free Trade Zone, one logistics company in Taipei Free Trade Zone, and 81 manufacturers and enterprises in Taoyuan Air Cargo Free Trade Zone. Shipments through these FTZs in the first ten months of 2007 was valued at NTD 43.7 billion ($1.3 billion), equivalent to 0.3 percent of Taiwan's two-way trade in the same period. There is no indication that FTZs in Taiwan are being used in trade-based money laundering schemes or by the financiers of terrorism. According to Article 14 of the Free Trade Establishment and Management Act, any enterprise applying to operate within an FTZ shall apply to the management authorities of the particular FTZ by submitting a business operation plan, the written operational procedures for good control, customs clearance, and accounting operations, together with relevant required documents. Financial institutions may apply to establish a branch office inside the FTZ and conduct foreign exchange business, in accordance with the Banking Law of the ROC, Securities and Exchange Law, Statute Governing Foreign Exchange, and the Central Bank of China Act.

According to Taiwan's Banking Law and Securities Trading Law, in order for a financial institution to conduct foreign currency operations, Taiwan's Central Bank must first grant approval. The financial institution must then submit an application to port authorities to establish an offshore banking unit (OBU) in the free-trade zone. No financial entity has yet applied to establish such an OBU in any of the five free trade zones. An offshore banking unit may operate a related business under the Offshore Banking Act, but cannot conduct any domestic financial, economic, or commercial transaction in New Taiwan Dollars.

Taiwan has promulgated drug-related asset seizure and forfeiture regulations that provide—in accordance with treaties or international agreements—Taiwan's Ministry of Justice shall share seized assets with foreign official agencies, private institutions, or international parties that provide Taiwan with assistance in investigations or enforcement. Assets of drug traffickers, including instruments of crime and intangible property, can be seized along with legitimate businesses used to launder money. The injured parties can be compensated with seized assets. The Ministry of Justice distributes other

seized assets to the prosecutor's office, police or other anti-money laundering agencies. The law does not allow for civil forfeiture. A mutual legal assistance agreement between the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO) entered into force in March 2002. It provides a basis for Taiwan and U.S. law enforcement agencies to cooperate in investigations and prosecutions for narcotics trafficking, money laundering (including the financing of terrorism), and other financial crimes.

Although Taiwan is not a UN member and cannot be a party to the 1988 UN Drug Convention, the authorities in Taiwan have passed and implemented laws in compliance with the goals and objectives of the Convention. Similarly, Taiwan cannot be a party to the UN International Convention for the Suppression of the Financing of Terrorism, as a nonmember of the United Nations, but it has agreed unilaterally to abide by its provisions. Taiwan is a founding member of the Asia/Pacific Group on Money Laundering (APG) and in 2005, was elected to the APG steering committee. In 2007, Taiwan underwent its second round mutual evaluation by the APG.

The MLPC is a member of the Egmont Group of financial intelligence units. The Investigation Bureau of the Ministry of Justice has actively engaged in international cooperation, and the number of cooperation cases in the first 11 months of 2007 reached 74. The MOJ has signed mutual legal assistance memoranda with four jurisdictions.

Over the past five years, Taiwan has created and implemented an anti-money laundering regime that comports with international standards. The MLCA amendments of 2003 address a number of vulnerabilities, especially in the area of asset forfeiture. The authorities on Taiwan should continue to strengthen the existing anti-money laundering regime as they implement the new measures. Taiwan should endeavor to pass the proposed Counter-Terrorism Action Law to better address terrorist financing issues. The authorities on Taiwan should investigate underground finance and its links to trade and also enact legislation regarding alternate remittance systems.

Tanzania

While not an important regional financial center, Tanzania is vulnerable to money laundering and has weaknesses in its anti-money laundering/counter-terrorist financing (AML/CTF) regime, specifically in its financial institutions and law enforcement capabilities. However, with the enactment of the Anti-Money Laundering (AML) Act, 2006 and the creation of a financial intelligence unit (FIU), the Government of Tanzania (GOT) is improving its capability to track and prosecute money laundering. Money laundering is more likely to occur in the informal nonbank financial sector, as opposed to the formal sector, which is largely undeveloped. Real estate and used car businesses appear to be vulnerable trade industries involved in money laundering. Front companies are used to launder funds including hawaladars and bureaux de change, especially on the island of Zanzibar, where few federal regulations apply. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash smuggling. The likely sources of illicit funds are from Asia and the Middle East and, to a lesser extent, Europe. Such transactions rarely include significant amounts of U.S. currency. There are no indications Tanzania's two free trade zones are being used in trade-based money laundering schemes or by financiers of terrorism.

The 2002 Prevention of Terrorism Act criminalizes terrorist financing. It requires all financial institutions to inform the government each quarter in a calendar year of any assets or transactions that may be associated with a terrorist group. The implementing regulations for this provision have not yet been drafted. Under the Act, the government may seize assets associated with terrorist groups. The Bank of Tanzania (BOT) circulates to Tanzanian financial institutions the names of suspected terrorists and terrorist organizations on the United Nations Security Council Resolution (UNSCR) 1267 Sanction Committee's consolidated list, but to date no assets have been frozen under this provision. In 2004, the Government of Tanzania took action against one charitable organization on the

list by closing its offices and deporting its foreign directors. However, it is not clear whether Tanzania has the investigative capacity to identify and seize related assets. Tanzania has cooperated with the U.S. in investigating and combating terrorism and exchanges counterterrorism information. There are no specific laws in place allowing Tanzania to exchange records with the U.S. on narcotics transactions or narcotics-related money laundering.

Tanzania made progress in 2007 with its anti-money laundering legislation. The national multi-disciplinary committee, established with the help of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), finalized the AML bill in 2005 after gaining input from a wide range of stakeholders. The Anti-Money Laundering Act, which creates a financial intelligence unit as an extra-ministerial department of the Ministry of Finance, was passed by the Parliament in December 2006 and signed into law in July 2007. The AML regulations implementing the Act were published in September 2007. The AML Act empowers the FIU to receive and share information with foreign FIUs and other comparable bodies. At present, the FIU has a small core staff-a Commissioner, an analyst, and an information technology expert. Current plans call for the recruitment of three additional staff members. The FIU has not yet set up its office and has not yet begun the analysis of suspicious transactions. It is working toward building capacity to become operational, and has applied for membership in the Egmont Group.

The AML Act criminalizes cash smuggling in and out of Tanzania. The AML Act and regulations require all "reporting persons"-banks and financial institutions, cash dealers, accountants, real estate agents, dealers in precious stones, customs officers, auctioneers, and legal professionals handling real estate or funds-to obtain specific information from citizen and noncitizen customers, maintaining specific identification procedures, and to report suspicious and unusual transactions to the FIU within 24 hours. The AML Act governs all serious crimes, including narcotics and terrorism. The FIU is developing a sensitization and outreach program to ensure that financial and nonfinancial institutions are aware of their reporting obligations under the AML Act.

The GOT is a party to the 1988 UN Drug Convention; the UN International Convention for the Suppression of the Financing of Terrorism; the UN Convention Against Corruption; and the UN Convention against Transnational Organized Crime. Tanzania is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG). The Government of Tanzania has detailed personnel to the ESAAMLG Secretariat. In 2007, Tanzania was listed 94 out of 179 countries in Transparency International's Corruption Perceptions Index.

Tanzania has made many improvements in its compliance with international AML standards. The GOT should focus on the practical implementation of its new AML Act, including dedicating the resources necessary to build an effective FIU. The FIU should work towards attaining international standards and membership in the Egmont Group.

Thailand

Thailand has introduced a number of measures in recent years to strengthen its AML/CTF framework. Illicit proceeds are generated from drug trafficking, illegal gambling, theft, corruption, prostitution, human trafficking, illegal logging, production and distribution of counterfeit consumer goods, production and sale of counterfeit travel documents, and from crime in bordering countries. Thailand remains a transit point for heroin en route to the international drug markets from Burma and Laos, and a drug money laundering center for transnational organized crime groups in Thailand. Authorities believe Thailand's major narcotics problem now is the trafficking of large quantities of methamphetamine produced in Burma. The illegal economy in Thailand is estimated as much as 13 percent of gross domestic product (GDP) and money laundering predicate offenses are estimated to generate illicit proceeds as much as five percent of Thailand's GDP. The widespread use of cash and a large informal sector provide many avenues for illicit proceeds to be laundered in Thailand.

Thailand's 1999 anti-money laundering legislation, the Anti-Money Laundering Act (AMLA) B.E. 2542 criminalizes money laundering for the following predicate offenses: narcotics trafficking, trafficking in women or children for sexual purposes, fraud, financial institution fraud, public corruption, customs evasion, extortion, public fraud, blackmail, and terrorist activity. On August 11, 2003, as permitted by the Thai constitution, the Royal Thai Government (RTG) issued two Emergency Decrees to enact measures related to terrorist financing that had been under consideration by the Executive Branch and Parliament for more than a year and a half. The first of these Decrees amended Section 135 of the Penal Code to establish terrorism as a criminal offense. The second Decree amended Section 3 of the AMLA to add the newly established offense of terrorism and terrorist financing as an eighth predicate offense for money laundering. The Decrees took effect when they were published. Parliament endorsed their status as legal acts in April 2004. No cases of terrorist financing have been prosecuted.

The current list of predicate offenses in the AMLA does not meet international best practices standards consistent with the first and second recommendations of the Financial Action Task Force (FATF) 40 Recommendations, which apply the crime of money laundering to all serious offenses or with the minimum list of acceptable designated categories of offenses. Additionally, the definition of "property involved in an offense" in the AMLA is limited to proceeds of predicate offenses and does not extend to instrumentalities of a predicate offense or a money laundering offense.

The AMLA created the Anti-Money Laundering Office (AMLO). Among other functions it serves as Thailand's financial intelligence unit (FIU), which became fully operational in 2001. When first established, AMLO reported directly to the Prime Minister. In October 2002, pursuant to a reorganization of the executive branch following criticisms that AMLO had been politicized, AMLO was designated as an independent agency under the Minister of Justice.

AMLO receives, analyzes, and processes suspicious and large transaction reports, as required by the AMLA. In addition, AMLO is responsible for investigating money laundering cases for civil forfeiture and for the custody, management, and disposal of seized and forfeited property. AMLO is also tasked with providing training to the public and private sectors concerning the AMLA. The law also created the Transaction Committee, which operates within AMLO to review and approve disclosure requests to financial institutions and asset restraint/seizure requests. The AMLA also established the Anti-Money Laundering Board, which is comprised of ministerial-level officials and agency heads and serves as an advisory board that meets periodically to set national policy on money laundering issues and to propose relevant ministerial regulations.

AMLO, the Bank of Thailand, the Securities and Exchange Commission, and the Department of Special Investigation (DSI) are responsible for investigating financial crimes. During the 2007 fiscal year, AMLO forwarded 83 cases for civil asset forfeiture to the Attorney General's office for prosecution totaling 309 million baht in Thai currency (approximately U.S. $10.5 million); fifteen other cases remain under investigation. AMLO has a memorandum of understanding with the Royal Thai Customs, which shares information and evidence of smuggling and customs evasion involving goods or cash exceeding one million baht (approximately U.S. $34,000) with AMLO. In criminal narcotics cases, the forfeiture and seizure of assets is governed by the 1991 Act on Measures for the Suppression of Offenders in an Offense relating to Narcotics (Assets Forfeiture Law). The Assets Examination Committee, which is separate from AMLO and was created by the post coup government to deal with corruption, has filed 1,865 cases with assets valued at 1.64 billion baht (approximately U.S. $56.6 million) and 1,644 cases are on trial.

The Ministry of Justice also houses a criminal investigative agency, the Department of Special Investigations (DSI), which is separate from the Royal Thai Police (RTP). DSI has responsibility for investigating the criminal offense of money laundering (as distinct from civil asset forfeiture actions carried out by AMLO) and for several of the money laundering predicates defined by the AMLA,

including terrorism. The DSI, AMLO, and the RTP all have authority to identify, freeze, and/or forfeit terrorist finance-related assets.

Article 13 of the Anti-Money Laundering Act, B.E. 2542 requires financial institutions to submit three categories of cash transactions. For example, transactions that are worth two million baht (approximately U.S. $68,300) or more; transactions involving assets worth five million baht (approximately U.S. $170,000) or more; and suspicious transactions, on reasonable grounds, must be reported to the financial intelligence unit (FIU).

In addition to reporting large and suspicious transactions, financial institutions are also required to keep customer identification and specific transaction records for a period of five years from the date the account was closed, or from the date the transaction occurred, whichever is longer. Reporting individuals (banks and others) who cooperate with law enforcement entities are protected from liability. In January 2007, the Bank of Thailand issued notification to financial institutions (which includes Thai and foreign commercial banks, finance companies, as well as assessment management companies) to adopt "know your customer" and customer due diligence procedures to comply with international standards and practices. The requirement was made effective immediately. However, there is no penalty for noncompliance. Thailand does not have stand-alone secrecy laws but the Commercial Bank Act B.E. 2505 (1962), regulated by Bank of Thailand, has a provision providing for bank secrecy to prevent disclosure of client financial information. However, AMLA overrides this provision, and financial institutions must disclose their client and ownership information to AMLO if requested.

The Bank of Thailand (BOT), Securities and Exchange Commission (SEC), and AMLO are empowered to supervise and examine financial institutions for compliance with anti-money laundering/counter-terrorist financing laws and regulations. Although the Bank of Thailand regulates financial institutions in Thailand, bank examiners are prohibited, except under limited circumstances, from examining the financial transactions of a private individual. This prohibition acts as an impediment to the BOT's auditing of a financial institution's compliance with the AMLA or BOT regulations. Lacking power to conduct transactional testing, BOT does not currently examine its financial institutions for anti-money laundering compliance. Legislation to eliminate the impediments is under review.

Anti-money laundering controls are also enforced by other Royal Thai Government (RTG) regulatory agencies, including the Board of Trade and the Department of Insurance. Financial institutions that are required to report suspicious activities are broadly defined by the AMLA as any business or juristic person undertaking banking or nonbanking business. The land registration offices are also required to report on any transaction involving property of five million baht or greater (approximately U.S. $170,000), or a cash payment of two million baht or greater (approximately U.S. $68,300) for the purchase of real property.

The Exchange Control Act of B.E. 2485 (1942), amended in 1984, states that foreign currencies can be brought into Thailand without limit. The Ministry of Finance issued a regulation, effective October 28, 2007, that requires any person who transports foreign currencies in or out of the country exceeding U.S. $15,000, to declare such to the Customs office, which, in turn, reports the information directly to the Ministry. There is no restriction on the amount of Thai currency that may be brought into the country. However, absent authorization to exceed the limits, a person traveling to Thailand's bordering countries including Vietnam is allowed to take out no more than 500,000 baht (approximately U.S. $17,000) and to other countries no more than 50,000 baht (approximately U.S. $1,700).

Thailand is not an offshore financial center nor does it host offshore banks, shell companies, or trusts. Licenses were first granted to Thai and foreign financial institutions to establish Bangkok International Banking Facilities (BIBFs) in March 1993. BIBFs may perform a number of financial and investment banking services, but can only raise funds offshore (through deposits and borrowing) for lending in

Thailand or offshore. The United Nations Drug Control Program and the World Bank listed BIBFs as potentially vulnerable to money laundering activities, because they serve as transit points for funds. BIBFs are subject to the AMLA. However, in mid October 2006, the last BIBF license was returned to the Bank of Thailand due to the BOT's "one presence" policy for all financial institutions. Some of these qualified "stand-alone" BIBFs have upgraded to either full branches or subsidiaries, while Thai commercial banks with BIBF licenses had to surrender their licenses to the BOT. Most BIBFs simply exited the market.

The Stock Exchange of Thailand (SET) requires securities dealers to have "know your customer" procedures; however, the SET does not check anti-money laundering compliance during its reviews. The Department of Insurance (DOI), under the Ministry of Commerce, is responsible for the supervision of insurance companies, which are covered under the AMLA definition of a financial institution, but there are no anti-money laundering regulations for the insurance industry. Similarly, the Cooperative Promotion Department (CPD) is responsible for supervision of credit cooperatives, which are required under the Cooperatives Act to register with the CPD. Approximately 6,000 cooperatives are registered, with approximately 1,348 thrift and credit cooperatives engaged in financial business. Thrift and credit cooperatives are engaged in deposit taking and providing loans to the members and are covered under the definition of a financial institution, but, as with the securities and insurance sectors, there are no anti-money laundering compliance mechanisms currently in place. These deficiencies have been recognized and are currently being addressed by the relevant government agencies.

Financial institutions (such as banks, finance companies, savings cooperatives, etc.), land registration offices, and persons that act as solicitors for investors are required to report significant cash, property, and suspicious transactions. Reporting requirements for most financial transactions (including purchases of securities and insurance) exceeding two million baht (approximately U.S. $68,300), and property transactions exceeding five million baht (approximately U.S. $170,000), have been in place since October 2000. The AMLO Board is considering the issuance of an announcement or regulation to subject gold shops, jewelry stores, and car dealers to either mandatory transactional reporting requirements and/or suspicious transactions reporting requirements. Thailand has more than 6,000 gold shops and 1,000 gem traders that would be subject to these reporting requirements.

Thailand acknowledges the existence and use of alternative remittance systems (hawala, the Chinese underground banking system) that attempt to circumvent financial institutions. There is a general provision in the AMLA that makes it a crime to transfer, or to receive a transfer, that represents the proceeds of a specified criminal offense (including terrorism). Remittance and money transfer agents, including informal remittance businesses, require a license from the Ministry of Finance. Guidelines issued in August 2004 by the Ministry of Finance and the BOT prescribe that before they are granted a license, both money changers and money transfer agents are subject to onsite examination by the BOT, which also consults with AMLO on the applicant's criminal history and anti-money laundering prevention record. At present, moneychangers have to report financial transactions to the Anti-Money Laundering Office while remittance agents do not. Licensed agents are subject to monthly transaction reporting and a five-year record maintenance requirement for onsite inspections. At present, there are approximately 560 authorized moneychangers and 28 remittance agents. In 2004, the Bank of Thailand limited the maximum amount to $5000 or equivalent for authorized moneychangers to sell foreign currencies and requires customers to present a passport or other traveling document. There are no limitations for buying currencies or no annual transaction volume. However, for remittance agents, the BOT limits the annual transaction volume for agents to U.S. $60,000 for offices in the Bangkok area, and U.S. $30,000 for offices located outside of Bangkok. Moneychangers frequently act as illegal remittance agents.

Money and property may be seized under Section 3 of the AMLA if derived from commission of a predicate offense, from aiding or abetting commission of a predicate offense, or if derived from the

sale, distribution, or transfer of such money or asset. AMLO is responsible for tracing, freezing, and seizing assets. Instruments that are used to facilitate crime such as vehicles or farms (when not proceeds) cannot be forfeited under AMLA and are subject to seizure under the Criminal Asset Forfeiture Act of 1991, and unlike the AMLA, require a criminal conviction as a pre-requisite to a final forfeiture. The AMLA makes no provision for substitute seizures if authorities cannot prove a relationship between the asset and the predicate offense. Overall, the banking community in Thailand provides good cooperation to AMLO's efforts to trace funds and seize/freeze bank accounts.

The Bank of Thailand (BOT) does not have any regulations that give it explicit authorization to control charitable donations, but it is working with AMLO to monitor these transactions under the Exchange Control Act of 1942.

The Thai Prime Minister endorsed a cabinet decision in October 2007 to abolish an incentives system that went into effect three years earlier under the "Office of the Prime Minister's Regulation on Payment of Incentives and Rewards in Proceedings against Assets under the Anti-Money Laundering Act." Under this now largely defunct rewards system, AMLO investigators and their supervisors, as well as other investigative agencies were eligible to receive personal commissions on the property that they seized if it was ultimately forfeited. The United States, other countries, and international organizations, including UNODC, criticized this system on the grounds that it threatened the integrity of its AML regime and created a conflict of interest by giving law enforcement officers a direct financial stake in the outcome of forfeiture cases. The USG ceased providing technical assistance to the AMLO until the reward system was abolished,

Thailand is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed (December 2000), but not yet ratified, the UN Convention against Transnational Organized Crime. It has also signed (December 2003), but not yet ratified the UN Convention against Corruption.

The RTG has issued instructions to all authorities to comply with UNSCR 1267. To date, Thailand has not identified, frozen, and/or seized any assets linked to individuals or entities included on the UNSCR 1267 Sanctions Committee's consolidated list. However, AMLO has identified some suspicious transaction reports derived from financial institutions as possibly terrorist-related and has initiated investigations of possible terrorist activities using nongovernmental or nonprofit organizations as a front.

Thailand has Mutual Legal Assistance Treaties (MLATs) with 10 countries, including the United States. In 2006 Thailand signed the Treaty On Mutual Legal Assistance In Criminal Matters Among Like-Minded ASEAN Member Countries but has not yet ratified the agreement. AMLO has memoranda of understanding on money laundering cooperation with 31 other financial intelligence units and also exchanges information with FIUs with which it has not entered into an MOU, including the United States. Thailand cooperates with USG and other nations' law enforcement authorities on a range of money laundering and illicit narcotics related investigations. AMLO responded to 87 requests for information from foreign FIUs in 2007. The AMLO joined the Egmont Group of financial intelligence units in June 2001.

Thailand became a member of the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body, in 1997. The most recent mutual evaluation of Thailand was conducted by the APG in 2007. The report noted that Thailand's AML/CTF regime is "not fully in line with international standards and codes; there are weaknesses in the legal framework, the pursuit of money laundering cases, the coverage of institutions and in enforcement."

AMLO has drafted amendments that will be proposed in early 2008 to deal with many of these deficiencies, including expanding the definition of property involved in an offense to include instrumentalities, creating an assets forfeiture fund, and restructuring AMLO. Additional amendments,

approved by the Thai cabinet in February 2007 but still pending, would add additional predicate offenses under Section 5 of the AMLA, including environmental crimes, foreign exchange offenses, securities fraud, illegal gambling, firearms trafficking, bid-rigging, labor fraud, and customs and excise offenses.

The Government of Thailand should continue to implement AML/CTF programs that adhere to world standards, including expanding the number of predicate crimes to adhere to the minimum list of designated categories of offenses prescribed by FATF. Predicate offenses should include trafficking in humans and migrant smuggling, counterfeiting and intellectual property offenses, as well as the "structuring" of transactions. Per some of the major findings in the 2007 APG mutual evaluation, AML/CTF obligations should be extended to nonfinancial businesses and professions such as gold shops, jewelry stores and car dealers. The insurance and securities sectors should institute AML compliance programs. Besides onsite consultation, AMLO should undertake audits of financial institutions to ensure compliance with requirements of AMLA and AMLO regulations. RTG authorities should develop and implement anti-money laundering regulations for exchange businesses and should take additional measures to address the vulnerabilities presented by its alternative remittance systems. Customs and most law enforcement agencies need to provide more training on, and dedicate specialized staff to carry out, anti-money laundering and terrorist finance investigations, especially outside of Bangkok. Authorities should give higher priority to reducing the use of cash in Thailand and to encourage more activity in the formal sector to help reduce money laundering and terrorist finance risks. Authorities should place an emphasis on prosecuting money launderers; in 2005 and 2006 there were few money laundering prosecutions and no convictions. Thailand should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Turkey

Turkey is an important regional financial center, particularly for Central Asia and the Caucasus, as well as for the Middle East and Eastern Europe. It continues to be a major transit route for Southwest Asian opiates moving to Europe. However, narcotics trafficking organizations are only one source of the total funds laundered in Turkey. Other sources of laundered funds include smuggling, counterfeit goods, fraud, forgery, robbery, and kidnapping. Money laundering takes place in banks, nonbank financial institutions, and the underground economy. Money laundering methods in Turkey include: the cross-border smuggling of currency; bank transfers into and out of the country; trade fraud, and the purchase of high-value items such as real estate, gold, and luxury automobiles. It is thought that Turkish-based traffickers transfer money and sometimes gold via couriers, the underground banking system, and bank transfers to pay narcotics suppliers in Pakistan or Afghanistan. Funds are often transferred to accounts in the United Arab Emirates, Pakistan, and other Middle Eastern countries. A substantial percentage of money laundering that takes place in Turkey involves fraud and tax evasion. Informed observers estimate that as much as 40 to 50 percent of the economy is unregistered. In 2005, the Government of Turkey (GOT) passed a tax administration reform law, with the goal of improving tax collection. The GOT is working on additional reforms to combat the unregistered economy and move these businesses onto the tax rolls.

Turkey first criminalized money laundering in 1996. Under the law whoever commits a money laundering offense faces a sentence of two to five years in prison, and is subject to a fine of double the amount of the money laundered and asset forfeiture provisions. The Council of Ministers subsequently passed a set of regulations that require the filing of suspicious transaction reports (STRs), customer identification, and the maintenance of transaction records for five years.

In 2006, the GOT enacted additional anti-money laundering legislation, a new criminal law, and a new criminal procedures law. The new Criminal Law, which took effect in June 2005, broadly defines

money laundering to include all predicate offenses for which the punishment is imprisonment for one year or more. Previously, Turkey's anti-money laundering law comprised a list of specific predicate offenses. A new Criminal Procedures Law also came into effect in June 2005.

Under a Ministry of Finance banking regulation circular all banks, including the Central Bank, securities companies, post office banks, and Islamic financial houses are required to record tax identity information for all customers opening new accounts, applying for checkbooks, or cashing checks. The circular also requires exchange offices to sign contracts with their clients. The Ministry of Finance also mandates that a tax identity number be used in all financial transactions. The requirements are intended to increase the GOT's ability to track suspicious financial transactions. Turkey has a new law, which protects the identity of those who file suspicious transaction reports, and, as of October 2007, has helped to push suspicious transaction reports above 2,000. According to anti-money laundering law Article 5, public institutions, individuals, and corporate bodies must submit information and documents as well as adequate supporting information upon the request of Turkey's Financial Crimes investigation Board (MASAK) or other authorities specified in Article 3 of the law. Individuals and corporate bodies from whom information and documents are requested may not withhold the requested items by claiming the protection provided by privacy provisions to avoid submitting the requested items. Despite the information collected for new accounts and transactions, customer due diligence (CDD) and other preventative measures have not been fully implemented and Turkey has failed to adopt a risk-based approach, as recommended by the Financial Action Task Force (FATF). There are no requirements for ongoing CDD and only limited requirements for the collection of beneficial ownership information. There is no requirement for financial institutions to exercise enhanced due diligence on business relationships or transactions with suspicious persons, including persons from or in countries which do not sufficiently apply FATF recommendations.

A new Banking Law was enacted in 2005 to strengthen bank supervision. The Banking Regulatory and Supervisory Agency (BRSA) conducts periodic anti-money laundering and compliance reviews under the authority delegated by MASAK. The number of STRs filed has been low, even taking into consideration the fact that many commercial transactions are conducted in cash. In 2006, 1140 STRs were filed. The upward trend continues as shown by the following results: in 2005, 352 STRs were filed; in 2004, 288 STRs were filed; and, in 2003, 177 STRs were filed.

Turkey does not have foreign exchange restrictions. With limited exceptions, banks and special finance institutions must inform authorities within 30 days about transfers abroad exceeding U.S. $50,000 (approximately 60,000 new Turkish liras) or its equivalent in foreign currency notes (including transfers from foreign exchange deposits). Travelers may take up to U.S. $5,000 (approximately 6,000 new Turkish liras) or its equivalent in foreign currency notes out of the country. Turkey does have cross-border currency reporting requirements. Article 16 of the recently enacted MASAK law (see below) gives customs officials the authority to sequester valuables of travelers who make false or misleading declarations and imposes fines for such declarations.

MASAK was established by the 1996 anti-money laundering law as part of the Ministry of Finance. MASAK became operational in 1997, and it serves as Turkey's Financial Intelligence Unit (FIU), receiving, analyzing, and referring STRs for investigation. MASAK has three functions: regulatory, financial intelligence, and investigative. MASAK plays a pivotal role between the financial and law enforcement communities.

In October 2006, Parliament enacted a new law reorganizing MASAK along functional lines, explicitly criminalizing the financing of terrorism, and providing safe harbor protection to the filers of STRs. The law also expands the range of entities subject to reporting requirements, to include several Designated Non-Financial Businesses and Professions (DNFBPs), such as art dealers, insurance companies, lotteries, vehicle sales outlets, antique dealers, pension funds, exchange houses, jewelry stores, notaries, sports clubs, and real estate companies. While the legislation has been improved to

require reporting from a wide range of industries and entities, almost all STRs continue to be submitted by banks, which suggests inadequate supervision or regulation of these DNFPBs. It also specifies sanctions for failure to comply. The law gives MASAK the authority to instruct a number of different inspection bodies (such as the bank examiners, the financial inspectors or the tax inspectors) to initiate an investigation if MASAK has reason to suspect financial crimes. Likewise, MASAK can refer suspicious cases to the Public Prosecutor and the Public Prosecutor can ask MASAK to conduct a preliminary investigation prior to referring a case to the police for criminal investigation. In August 2007, a regulation on money laundering crime was enacted enforcing MASAK's authority to combat these crimes. However there continues to be limited training and specialization in, or understanding of, money-laundering and terrorist financing among law enforcement units and judicial authorities, resulting in a high number of acquittals in anti-money laundering and counter-terrorist financing (AML/CTF) cases.

According to MASAK statistics, as of December 31, 2006 it had pursued 2,231 money laundering investigations since its 1996 inception, but fewer than ten cases resulted in convictions. Moreover, all of the convictions are reportedly under appeal. Most of the cases involve nonnarcotics criminal actions or tax evasion; as of December 31, 2005. 41 percent of the cases referred to prosecutors were narcotics-related.

The GOT enforces existing drug-related asset seizures and forfeiture laws. MASAK, prosecutors, Turkish National Police, and the courts are the government entities responsible for tracing, seizing and freezing assets. According to Article 9 of the anti-money laundering law, the Court of Peace-a minor arbitration court for petty offenses-has the authority to issue an order to freeze funds held in banks and nonbank financial institutions as well as other assets, and to hold the assets in custody during the preliminary investigation. During the trial phase, the presiding court has freezing authority. Public Prosecutors may freeze assets in cases where it is necessary to avoid delay. The Public Prosecutors' Office notifies the Court of Peace about the decision within 24 hours. The Court of Peace has 24 hours to decide whether to approve the action. There is no time limit on freezes. There is no specific provision in Turkish law for the sharing of seized assets with other countries; however the United States and Turkey have shared seized assets in one narcotics case.

MASAK's General Communiqué No. 3, dated February 2002, requires that a special type of STR be filed by financial institutions in cases of suspected terrorist financing. However, until the amendments to the criminal code were enacted in June 2006, terrorist financing was not explicitly defined as a criminal offense under Turkish law. Various existing laws with provisions that can be used to punish the financing of terrorism include articles 220, 314 and 315 of the Turkish penal code, which prohibit assistance in any form to a criminal organization or to any organization that acts to influence public services, media, proceedings of bids, concessions, and licenses, or to gain votes, by using or threatening violence. To commit crimes by implicitly or explicitly intimidating people is illegal under the provisions of the Law No. 4422 on the Prevention of Benefit-Oriented Criminal Organizations. The names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee consolidated list, as well as U.S.-designated names, are routinely distributed to financial institutions and appropriate Turkish agencies. However Turkey has failed to takes steps to employ an effective regime to combat terrorist financing, especially as it relates to UNSCRs 1267 and 1373. For example, while the GOT has implemented UNSCR 1267, it has failed to establish punishment or sanctions for institutions that fail to observe a freezing order, and it has not established procedures for delisting entities or unfreezing funds. Additionally, the GOT has not taken steps that would allow it to freeze the assets of entities designated by other jurisdictions, as required under UNSCR 1373.

Another area of vulnerability in the area of terrorist financing is the GOT's supervision of nonprofit organizations. The nonprofit sector is well regulated, but it is not audited on a regular basis for CTF vulnerabilities and does not receive adequate AML/CTF outreach and guidance from the GOT. The General Director of Foundations (GDF) issues licenses for charitable foundations and oversees them.

However, there are a limited number of auditors to cover more than 70,000 institutions. The Ministry of Interior regulates charitable nongovernmental associations (NGOs). The GDF, as part of the Ministry of Interior, keeps central registries of the charitable organizations they regulate and they require charities to verify and prove their funding sources and to have bylaws. Charitable organizations are required to submit periodic financial reports to the regulators. The regulators and the police closely monitor monies received from outside Turkey. The police also monitor NGOs for links to terrorist groups.

Alternative remittance systems are illegal in Turkey, and in theory only banks and authorized money transfer companies are permitted to transfer funds. Trade-based money laundering, fraud, and underground value transfer systems are also used to avoid taxes and government scrutiny. There are 21 free trade zones operating in Turkey. The GOT closely controls access to the free trade zones. Turkey is not an offshore financial center.

According to MASAK statistics, no assets linked to terrorist organizations or terrorist activities were frozen in 2006. Turkey has a system for identifying, tracing, freezing, and seizing assets that are not related to terrorism, although the law allows only for their criminal forfeiture and not their administrative forfeiture. Article 7 of the anti-money laundering law provides for the confiscation of all property and assets (including derived income or returns) that are the proceeds of a money laundering predicate offense (recently expanded to include crimes punishable by one year imprisonment), once the defendant is convicted. The law allows for the confiscation of the equivalent value of direct proceeds that could not be seized. Instrumentalities of money laundering can be confiscated under the law. In addition to the anti-money laundering law, Articles 54 and 55 of the Criminal Code provide for post-conviction seizure and confiscation of the proceeds of crimes. The defendant, however, must own the property subject to forfeiture. Legitimate businesses can be seized if used to launder drug money or support terrorist activity, or are related to other criminal proceeds. Property or its value that is confiscated is transferred to the Treasury.

In the months after 9/11, the Council of Ministers decreed (2482/2001) all funds and financial assets of individuals and organizations included on the UNSCR 1267 Sanctions Committee's consolidated list be frozen. However, the tools available at that time under Turkish law for locating, freezing, seizing, and confiscating terrorist assets were cumbersome, limited, and ineffective. In late 2001, the Council of Ministers froze the funds of one individual accused of financing terror in Turkey. This individual filed an appeal in 2001, and in June 2006 the 10th Chamber of the Turkish Administrative Court overruled the original Council of Ministers decision on technical grounds. The 10th Chamber's decision was appealed, and upon review, in February 2007 the Highest Chamber Council of the Turkish Administrative Court upheld the original decision to freeze the individual's assets on the grounds that there were no legal irregularities in the original decision. The assets of the 1267-listed individual continue to be frozen. Since then, changes in the law relating to MASAK, the Turkish criminal code, and the anti-terrorism law give more authority to seize and freeze assets quickly and make the Turkish system more compliant with international standards.

The GOT cooperates closely with the United States and with its neighbors in the Southeast Europe Cooperation Initiative (SECI). Turkey and the United States have a Mutual Legal Assistance Treaty (MLAT) and cooperate closely on narcotics and money laundering investigations. Turkey is a member of the Financial Action Task Force (FATF). Since 1998, MASAK has been a member of the Egmont Group of Financial Intelligence Units. Turkey is a party to the 1988 UN Drug Convention, the UN International Convention for Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. In January 2005, Turkey became a party to the Council of Europe (COE) Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime.

With the passage of several new pieces of legislation, the Government of Turkey took steps in 2006 and 2007 to strengthen its AML/CTF regime. The GOT now faces the challenge of aggressively implementing these laws. In 2007 the GOT established a High Coordination Council on Financial Crimes, which consists of MASAK, Finance Ministry, Capital Markets Board, and Central Bank representatives. The aim of this board is to improve coordination among the agencies to combat financial crimes and support the work of MASAK. MASAK must improve its automation to be able to access banks' and other financial institutions' data bases, so as to accelerate MASAK's process and enable it to refer cases more quickly to prosecutors. The lack of prosecutions and convictions for money laundering is troubling. Law enforcement and judicial authorities need to be given additional training and develop expertise on AML/CTF issues. There is an over-reliance on STRs to initiate money laundering investigations in Turkey. Law enforcement and customs authorities should be enabled to follow the money and value trails during the course of their investigations, and should not be required to turn that portion of the investigation over to MASAK. MASAK should second members of the Turkish National Police and prosecution offices in order fulfill its mandate to investigate preliminary indications of money laundering. As currently staffed, MASAK does not have criminal investigative experience although it is required to make such initial determinations. The GOT should also regulate and investigate remittance networks to thwart their potential misuse by terrorist organizations or their supporters. The GOT needs to fully implement the provisions of UNSCRs 1267 and 1373, and should consider expanding its narrow legal definition of terrorism, which currently is limited to acts committed by members of organizations against the Turkish Republic by pressure force and violence using terror, intimidation, oppression or threat. The GOT should also strengthen its oversight of foundations and charities, which currently receive only cursory overview and auditing. Turkey should take steps to improve the CDD procedures and other preventative measures, as well as adopt a risk-based approach to AML/CTF. Supervision and regulation of DNFBPs covered by the 2006 legislation also needs to be improved.

Turks and Caicos

The Turks and Caicos Islands (TCI) is a Caribbean overseas territory of the United Kingdom (UK). The TCI is comprised of two island groups and forms the southeastern end of the Bahamas archipelago. The U.S. dollar is the currency in use. The TCI has a significant offshore center, particularly with regard to insurance and international business companies (IBCs). Its location has made it a transshipment point for narcotics traffickers. The TCI is vulnerable to money laundering because of its large offshore financial services sector, as well as its bank and corporate secrecy laws and Internet gaming activities. As of 2006, the TCI's offshore sector has eight banks, four of which also offer offshore banking; approximately 2,500 insurance companies; 20 trusts; and 17,000 "exempt companies" that are IBCs. No updated statistics are available for 2007.

The Financial Services Commission (FSC) licenses and supervises banks, trusts, insurance companies, and company managers. It also licenses IBCs and acts as the Company Registry for the TCI. These institutions are subject to on-site examination to determine compliance with TCI laws and regulations. The Financial Services Commission has a staff of 21, including four regulators. The FSC became a statutory body under the Financial Services Commission Ordinance 2001 and became operational in 2002. It reports directly to the Governor, as well as to the Minister of Finance. The FSC is in the process of adopting a risk-based examination approach to better assess, identify, measure, monitor and control threats associated with potential money laundering and terrorist financing.

The offshore sector offers "shelf company" IBCs, and all IBCs are permitted to issue bearer shares. However, the Companies (Amendment) Ordinance 2001 requires that bearer shares be immobilized by depositing them, along with information on the share owners, with a defined licensed custodian. This applies to all shares issued after enactment and allows for a phase-in period for existing bearer shares of two years. Trust legislation allows establishment of asset protection trusts insulating assets from

civil adjudication by foreign governments; however, the Superintendent of Trustees has investigative powers and may assist overseas regulators. Currently, the FSC is rewriting the trust legislation with assistance from the UK Government.

The 1998 Proceeds of Crime Ordinance (PCO) criminalizes money laundering related to all crimes and provides "safe harbor" protection for good faith compliance with reporting requirements. The PCO allows for the criminal forfeiture of assets related to money laundering and other offenses, although civil forfeiture is not permitted. The PCO also establishes a Money Laundering Reporting Authority (MLRA), chaired by the Attorney General, to receive, analyze and disseminate financial disclosures such as suspicious activity reports (SARs). Its members also include the following individuals or their designees: Collector of Customs, the Managing Director of the FSC and the Head of its Financial Crimes Unit (FCU), the Superintendent of the FSC, the Commissioner of Police, and the Superintendent of the Criminal Investigation Department. The MLRA is authorized to disclose information it receives to domestic law enforcement and foreign governments.

The Proceeds of Crime (Money Laundering) Regulations came into force in 2000. The Money Laundering Regulations place additional requirements on the financial sector such as identification of customers, retention of records for a minimum of ten years, training staff on money laundering prevention and detection, and development of internal procedures to ensure proper reporting of suspicious transactions. The Money Laundering Regulations apply to banks, insurance companies, trusts, mutual funds, money remitters, investment dealers, and issuers of credit cards. However, there is no supervisory or regulatory authority to oversee regulatory compliance by money remitters and investment dealers. Other sectors, such as gambling, jewelers, real estate companies, and currency exchange companies, are not subject to the Money Laundering Regulations. Although the customer identification requirements only apply to accounts opened after the Regulations came into force, TCI officials have indicated that banks are required to conduct due diligence on previously existing accounts.

As with the other United Kingdom Caribbean overseas territories, the Turks and Caicos underwent an evaluation of its financial regulations in 2000, cosponsored by the local and British governments. The report noted several deficiencies and the government has moved to address most of them. The report noted the need for improved supervision, which the government acknowledged. An Amendment to the Banking Ordinance was introduced in February 2002 to remedy deficiencies outlined in the report relating to notification of the changes of beneficial owners, and increased access of bank records to the FSC. However, legislation has not been introduced to remedy the deficiencies noted in the report with respect to the Superintendent's lack of access to the client files of Company Service and Trust providers, nor is there legislation that clarifies how the Internet gaming sector is to be supervised with respect to anti-money laundering compliance.

In 1999, the FSC, acting as the secretary for the MLRA, issued nonstatutory Guidance Notes to the financial sector, to help educate the industry regarding money laundering and the TCI's anti-money laundering requirements. Additionally, it provided practical guidance on recognizing suspicious transactions. The Guidance Notes instruct institutions to send SARs to either the Royal Turks & Caicos Police Force or the FSC. Officials forward all SARs to the Financial Crimes Unit (FCU) of the Royal Turks and Caicos Islands Police Force, which analyzes and investigates financial disclosures. The FCU also acts as the TCI's financial intelligence unit (FIU). No statistics are available on the number of SARs received by the FCU in 2007, nor are there current statistics on the number of investigations, prosecutions, or convictions.

Travelers entering or leaving the TCI with more than U.S. $10,000 must make a declaration to Customs officials. In November 2007, a Bahaman citizen who entered TCI with over U.S. $14,000 in cash was arrested for making a false declaration after completing a Customs form stating that he was traveling with less than $10,000. The investigation of this incident marks the first time Customs and

the FCU have worked together on a joint investigation. In 2007, the FCU also assisted Canadian law enforcement in the investigation of two Canadian citizens, who were charged with fraud and money laundering in September.

As a UK territory, the TCI is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001. However, the Government of the TCI has not yet implemented domestic orders that would criminalize the financing of terrorism. The UK's ratification of the International Convention for the Suppression of the Financing of Terrorism has not been extended to the TCI.

The TCI cooperates with foreign governments—in particular, the United States and Canada—on law enforcement issues, including narcotics trafficking and money laundering. The FCU also shares information with other law enforcement and regulatory authorities inside and outside of the TCI. The Overseas Regulatory Authority (Assistance) Ordinance 2001, allows the TCI to further assist foreign regulatory agencies. This assistance includes search and seizure powers and the power to compel the production of documents.

The TCI is subject to the 1988 UN Drug Convention. The TCI is a member of the Caribbean Financial Action Task Force, and underwent a mutual evaluation in September 2007. The results of the mutual evaluation should be presented to the CFATF plenary in 2008. TCI's FIU is not a member of the Egmont Group of financial intelligence units. The Mutual Legal Assistance Treaty between the United States and the United Kingdom concerning the Cayman Islands was extended to the TCI in November 1990. The TCI does not have a Tax Information Exchange Agreement with the United States.

The Government of the Turks and Caicos Islands has put in place the relevant legislative framework to combat money laundering, but needs to implement relevant provisions of its anti-money laundering regime, criminalize terrorist financing, ensure that its FIU is fully functioning, and ensure that money laundering cases are investigated and prosecuted. The Government of the TCI should reform its current regulatory structure to be in full accordance with international standards by extending existing regulations to all sectors, bringing all obligated entities under the supervision of a regulatory body, and enhancing its on-site supervision program. The Turks and Caicos Islands should take the necessary steps to ensure that its FIU is eligible for membership in the Egmont Group of financial intelligence units. The Government of the TCI should criminalize the financing of terrorists and terrorism. The TCI should expand efforts to cooperate with foreign law enforcement and administrative authorities. Turks and Caicos Islands should also provide adequate resources and authorities to provide supervisory oversight of its offshore sector to further ensure criminal or terrorist organizations do not abuse the Turks and Caicos Islands' financial sector.

Ukraine

Corruption, organized crime, prostitution, smuggling, tax evasion, trafficking in persons, drugs and arms, and other organized criminal activity continue to be sources of laundered funds in Ukraine. As of October 1, 2007, Ukraine had approximately 173 active banks, two of which are state-owned. There are no offshore financial centers or facilities under Ukraine's jurisdiction.

Ukraine's 2005 budget eliminated the tax and customs duty privileges available in eleven Special Economic Zones (SEZs) and nine Priority Development Territories (PDTs) that had been associated with rampant evasion of customs duties and taxes. In late 2006, a government no longer in power registered a draft law with Parliament to restore tax and customs privileges for businesses operating in the SEZs. The law never came to a final vote, and the new government that assumed power in late 2007 has said that it will not reintroduce the privileges.

In January 2001, the Government of Ukraine (GOU) enacted the "Act on Banks and Banking Activities," which introduced some anti-money laundering (AML) requirements for banking

institutions. The Act prohibits banks from opening accounts for anonymous persons, requires the reporting of large transactions and suspicious transactions to state authorities, and provides for the lifting of bank secrecy pursuant to an order of a court, prosecutor, or specific state body. In August 2001, the President signed the "Law on Financial Services and State Regulation of the Market of Financial Services." This law establishes regulatory control over nonbank financial institutions that manage insurance, pension accounts, financial loans, or "any other financial services involving savings and money from individuals." The law provides definitions for "financial institutions" and "services," imposes record-keeping requirements on obligated entities, and identifies the responsibilities of regulatory agencies. The law established the State Commission on Regulation of Financial Services Markets, which, along with the National Bank of Ukraine (NBU) and the State Commission on Securities and the Stock Exchange, has responsibility for regulating financial services markets.

The Financial Action Task Force (FATF) placed Ukraine on the list of noncooperative countries and territories (NCCT) in September 2001. After a number of unsuccessful legislative attempts to develop an anti-money laundering (AML) regime that met international standards, the FATF called upon its members to invoke countermeasures in December 2002. At that time, the U.S. designated Ukraine as a jurisdiction of primary money laundering concern, under Section 311 of the USA PATRIOT Act. The GOU passed comprehensive AML legislation in February 2003, and promised significant institutional reform. The FATF withdrew its call for members to invoke countermeasures, after which the United States revoked its USA PATRIOT Act designation of the GOU as a jurisdiction of primary money laundering concern. The FATF removed Ukraine from the NCCT list in February 25, 2004.

Ukraine's legislation requires banks and other financial service providers to implement AML compliance programs: conduct due diligence to identify beneficial owners prior to allowing the opening of an account or conducting certain transactions; report suspicious transactions to the national financial intelligence unit (known as the State Committee for Financial Monitoring, or "SCFM") and maintain records on suspicious transactions; and, for a period of five years. The legislation includes a "safe harbor" provision that protects reporting institutions from liability for cooperating with law enforcement agencies. In August 2003, the State Commission established the State Register of financial institutions, and by March 2007, the State Register contained information on 1,956 nonbank financial institutions.

Since November 2004, the GOU has made several efforts to pass a set of amendments to the AML law to bring Ukraine's regime into compliance with FATF's revised Forty plus Nine recommendations. The Verkhovna Rada, Ukraine's Parliament, twice rejected the government's draft in 2005. The government redrafted the law, narrowing its scope to the FATF recommendations and omitting provisions introducing a new SCFM authority and other bureaucratic changes that had drawn opposition in the Parliament. Among other provisions, the new legislation would expand the sectors subject to primary monitoring to include retail traders, lawyers, accountants, and traders of precious metals. The draft law, entitled "On Amending Some Legislative Acts of Ukraine on Prevention to Legalization (Laundering) of the Proceeds from Crime and Terrorist Financing," was passed by the Parliament on June 19, 2007 but not signed into law. Because the draft law passed during a period when the authority of the Parliament was not recognized by the President, the draft law will now again need to be addressed by the Parliament.

In 2004, authorities reduced the threshold for compulsory financial monitoring from Ukrainian Hryvnias (UAH) 300,000 (approximately U.S. $59,430) for cashless payments and UAH 100,000 (approximately U.S. $19,800) for cash payments, to UAH 80,000 (approximately U.S. $15,848) for payments using either method. The compulsory reporting threshold exists only if the transaction also meets one or more suspicious activity indicators as set forth in the law. Any transaction suspected of being connected to terrorist activity must be reported to the appropriate authorities immediately.

Cash smuggling is substantial in Ukraine, although it is reportedly related more closely to unauthorized capital flight rather than to criminal proceeds or terrorist funding. In 2005, the GOU sought to combat smuggling and corruption by reducing import duties, introducing new procedures for the Customs Service, and implementing transparent procedures for the privatization of state enterprises. As of August 2005 travelers are required to declare cross-border transportation of cash sums in excess of U.S. $3,000, and declare the origin of funds exceeding U.S. $10,000.

In January 2006, Ukraine enacted Law 3163-IV, which amended the initial AML laws. Under this law, the entities obligated to conduct initial financial monitoring must be able to provide proof that they are fulfilling all Know Your Customer (KYC) identification requirements. Ukraine also granted state agencies enhanced authority to exchange information internationally, improved rules on bank organization, and implemented a screening requirement at the level of financial institutions. On September 14, 2006, Ukraine enacted amendments to the "Law on Banks and Banking" that require all banks to be formed as open joint-stock companies or as cooperatives. This measure strengthens disclosure requirements on the identity of the beneficial owners of banks. These amendments apply to all newly formed banks and provide a three-year period for existing banks to comply. As a result of these and other improvements to its legal framework, the FATF in February 2006 suspended its direct monitoring of Ukraine.

The Criminal Code of Ukraine has separate provisions criminalizing drug-related and nondrug-related money laundering. Amendments to the Code adopted in January 2003 included willful-blindness provisions and expanded the scope of predicate crimes for money laundering to include any action punishable under the Criminal Code with at least three years of imprisonment, excluding certain specified actions.

The SCFM is Ukraine's financial intelligence unit (FIU). The December 10, 2001 Presidential Decree "Concerning the Establishment of a Financial Monitoring Department" mandated the establishment of the SCFM as Ukraine's FIU. The SCFM became operational on June 12, 2003 and is the sole agency authorized to receive and analyze financial information from financial institutions. On March 18, 2004, Ukraine's Rada granted the SCFM the status of a central executive agency, subordinate to the Cabinet of Ministers. However, a draft law "On the Opposition," which was submitted to the Parliament in early 2007, specifies that the Parliament's opposition party could assign persons to certain leadership jobs in a number of state agencies, including the SCFM. Specifically, the draft law reserves the job of director and of two of the four deputy director positions to the opposition party in the Parliament. The law, if enacted, would likely contradict the November 2002, Law on Money Laundering Prevention. By year-end, the Parliament had taken no action on this draft.

The SCFM is an administrative agency with no investigative or arrest authority. It is authorized to collect suspicious transaction reports and analyze suspicious transactions, including those related to terrorist financing, and to transfer financial intelligence information to competent law enforcement authorities for investigation. As of October 1, 2007, the SCFM had established 22 local branches. The SCFM is authorized to conclude interagency agreements and exchange intelligence on financial transactions involving money laundering or terrorist financing with other FIUs. As of October 2007, the SCFM had concluded memoranda of understanding (MOUs) with thirty-three foreign FIUs, including FinCEN. It has become a regional leader with regard to the volume of case information exchanged with counterpart FIUs.

The SCFM collects and analyzes data, and identifies possible cases for prosecution to the Prosecutor General's Office (PGO). Although the SCFM is an administrative unit, it has processed, analyzed and developed some cases to the point of establishing probable cause before referring a case for further investigation. In 2006, the SCFM received 841,589 transaction reports, which include both STRs and automatic threshold reports. Banks filed the majority of the reports. The SCFM sent 446 separate cases to law enforcement agencies and the Prosecutor General's Office (PGO) for "active research". As a

result of subsequent investigation of these cases, law enforcement agencies initiated 164 criminal cases in 2006. Of these, prosecutors brought only eight cases to trial, with only one conviction. In the period 2003 through 2006, twenty of 325 cases went to trial with, with only three resulting in convictions on charges of money laundering.

Although the reporting system is effective and the SCFM has generated a substantial number of probable cases for referral, it has not led to a meaningful number of convictions. Many observers believe that the low prosecution rate is caused by a reluctance of the PGO to pursue the cases referred by the SCFM. Local prosecutors may close money laundering investigations and cases prematurely or arbitrarily, possibly because of lack of sufficient manpower or resources or because of corruption. Other possible reasons include a weak understanding of money laundering crimes (prosecutors often identify tax evasion with money laundering, for example) and a belief that other types of crimes should take priority over money laundering.

The SCFM acknowledges the existence and use of alternative remittance systems in Ukraine. In 2007, the Security Service of Ukraine published a report signaling that hawala might be on the rise in Ukraine due to a large number of Ukrainians working abroad and the growth of foreign communities in Ukraine. The SCFM and security agencies monitor charitable organizations and other nonprofit entities that might be used to finance terrorism.

Ukraine has an asset forfeiture regime. Article 59 of the Ukrainian Criminal Code provides for the forceful seizure of all or a part of the property of a person convicted for grave and particularly grave offenses as set forth in the relevant part of the code. With respect to money laundering, Article 209 allows for the forfeiture of criminally obtained money and other property.

On December 10, 2003, the Cabinet of Ministers issued Decree No. 1896, establishing a Unified State Information System of Prevention and Counteraction of Money Laundering and Terrorism Financing. The system, which became fully operational in December 2006, provides the SCFM with unobstructed access to the databases of twelve ministries and agencies, including the Ministries of Internal Affairs, Economy and, Finance, a well as the State Tax Administration, State Security Service, State Customs Administration, State Property Fund, State Statistics Administration, Border Guard Service, Securities Commission, Financial Services Commission, and Control and Revision Department.

On September 21, 2006, the Rada enacted revisions to Article 258 of the Criminal Code, adding Article 258-4 that explicitly criminalizes terrorist financing. The revised text mandates imprisonment from three to eight years for financing, material provision, or provision of arms with the aim of supporting terrorism. The revisions also amend the criminal procedure code to empower the State Security Service (SBU) with primary responsibility for investigation of terrorist financing.

Law 3163-IV enhanced Ukraine's ability to exchange information internationally and placed greater obligations on banks to combat terrorist financing. This Law requires banks to adopt procedures to screen parties to all transactions using an SCFM-issued list of beneficiaries of, or parties to, terrorist financing. Banks must freeze assets for two days and immediately inform the SCFM and law enforcement bodies whenever a party to a transaction appears on the list. The SCFM can extend the freeze to five days. On October 25, 2006, the Cabinet of Ministers approved the SCFM's list, drawn from three sources: the United Nations 1267 Sanctions Committee's consolidated list; information from the Ukrainian Security Service on individuals and entities suspected of violating article 258 of the Ukrainian Criminal Code concerning terrorism; and the lists compiled by those countries that have bilateral agreements with Ukraine on mutual recognition of terrorist designations.

The GOU has cooperated with U.S. efforts to track and freeze the financial assets of terrorists and terrorist organizations. Banks and nonbank financial services also receive these U.S. designations, and are instructed to report any transactions involving designated individuals or entities.

The U.S.-Ukraine Treaty on Mutual Legal Assistance in Criminal Matters was signed in 1998 and entered into force in February 2001. Additionally, the two countries have a bilateral taxation agreement that provides for the exchange of information in administrative, civil, and criminal matters related to taxation and tax evasion.

Ukraine is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Ukraine has signed, but has yet to ratify, to the UN Convention against Corruption (UNCAC). Ukraine is a member of MONEYVAL, a FATF-style regional body (FSRB). The SCFM is a member of the Egmont Group.

Ukraine has strengthened and clarified its newly adopted laws. With the SCFM, the NBU, and other entities in the financial and legal sectors, Ukraine has established a comprehensive AML regime. To date, however, Ukraine's ability to implement this regime through consistent successful criminal prosecutions remains unproven. Both law enforcement officers and the judiciary need a better understanding of the theoretical and practical aspects of investigating and prosecuting money laundering cases. Law enforcement agencies should give higher priority to investigating money laundering cases. The Prosecutor General's Office should address the deficiencies of that office, particularly in its organization and staff training. The GOU should establish oversight capabilities of local investigators, prosecutors, and judges to insure that cases are vigorously pursued and prosecuted. Ukraine's authorities should take steps to better understand the depth of their country's alternative remittance systems, and begin to address a monitoring and reporting regime. Likewise, Ukraine should take steps to enact a regulatory regime for charitable and nonprofit organizations that goes beyond monitoring. Ukraine should ratify the UNCAC and more aggressively address its public corruption problem by prosecuting and convicting corrupt public officials.

United Arab Emirates

The United Arab Emirates (UAE) is an important financial center in the Gulf region. Although the financial sector is modern and progressive, the UAE remains a largely cash-based society. Dubai, in particular, is a major international banking center. The country also has a growing offshore sector. The UAE's robust economic development, political stability, and liberal business environment have attracted a massive influx of people, goods, and capital. The UAE is particularly susceptible to money laundering due to its geographic location as the primary transportation and trading hub for the Gulf States, East Africa, and South Asia; its expanding trade ties with the countries of the former Soviet Union; and lack of transparency in its corporate environment.

The potential for money laundering is exacerbated by the large number of resident expatriates (roughly 80 percent of total population) who send remittances to their homelands. Given the country's proximity to Afghanistan, where most of the world's opium is produced, narcotics traffickers are increasingly reported to be attracted to the UAE's financial and trade centers. Other money laundering vulnerabilities in the UAE include hawala, trade fraud, smuggling, the real estate boom, the misuse of the international gold trade, and conflict diamonds.

The Central Bank is responsible for supervising the UAE's financial sectors, which include banks, exchange houses, and investment companies. It is authorized to issue licenses and impose administrative sanctions for compliance violations. The Central Bank also has the authority to issue instructions and recommendations to financial institutions as it deems appropriate, and to take any measures as necessary to ensure the integrity of the UAE's financial system. Following the September 11, 2001 terrorist attacks in the United States, and amid revelations that terrorists had moved funds through the UAE, the Emirates' authorities acted swiftly to address potential vulnerabilities. In close concert with the United States, the UAE imposed a freeze on the funds of groups with terrorist links, including the Al-Barakat organization, which was headquartered in Dubai. Both national and emirate-

level officials have gone on record as recognizing the threat money laundering activities in the UAE pose to the nation's reputation and security. Since 2001, the UAE Government (UAEG) has taken steps to better monitor cash flows through the UAE financial system and to cooperate with international efforts to combat terrorist financing.

The UAE has enacted the Anti-Money Laundering Law No. 4/2002, and the Anti-Terrorism Law No. 1/2004. Both pieces of legislation, in addition to the Cyber Crimes Law No. 2/2006, serve as the foundation for the country's anti-money laundering and counter-terrorist financing (AML/CTF) efforts. Law No. 4 of 2002 criminalizes all forms of money laundering activities. The law calls for stringent reporting requirements for wire transfers exceeding 2000 dirhams (approximately $545) and currency imports above 40,000 dirhams (approximately U.S. $10,900).The law imposes criminal penalties for money laundering that includes up to seven years in prison plus a fine of up to 300,000 dirhams (approximately U.S. $81,700), as well as a seizure of assets upon conviction. The law also provides safe harbor provisions for reporting officers.

Prior to the passage of the Anti-Money Laundering Law, the National Anti-Money Laundering Committee (NAMLC) was established in July 2000 to coordinate the UAE's anti-money laundering policy. The NAMLC was later codified as a legal entity by Law No. 4/2002, and is chaired by the Governor of the Central Bank. Members of the NAMLC include representatives from the Ministries of Interior, Justice, Finance, and Economy, the National Customs Board, Secretary General of the Municipalities, Federation of the Chambers of Commerce, and five major banks and money exchange houses (as observers).

Administrative Regulation No. 24/2000 provides guidelines to financial institutions for monitoring money laundering activity. This regulation requires banks, money exchange houses, finance companies, and any other financial institutions operating in the UAE to follow strict "know your customer" guidelines. Financial institutions must verify the customer's identity and maintain transaction details (i.e., name and address of originator and beneficiary) for all exchange house transactions over the equivalent of U.S. $545 and for all nonaccount holder bank transactions over U.S. $10,900. The regulation delineates the procedures to be followed for the identification of natural and juridical persons, the types of documents to be presented, and rules on what customer records must be maintained on file at the institution. Other provisions of Regulation 24/2000 call for customer records to be maintained for a minimum of five years and further require that they be periodically updated as long as the account is open.

In July 2004, the UAE government strengthened its legal authority to combat terrorism and terrorist financing by passing Federal Law Number No. 1/2004. The Law specifically criminalizes the funding of terrorist activities and terrorist organizations. It sets stiff penalties for the crimes covered, including life imprisonment and the death penalty. It also provides for asset seizure or forfeiture. Under the law, founders of terrorist organizations face up to life imprisonment. The law also penalizes the illegal manufacture, import, or transport of "nonconventional weapons" and their components that are intended for use in a terrorist activity.

Article 12 provides that raising or transferring money with the "aim or with the knowledge" that some or all of this money will be used to fund terrorist acts is punishable by "life or temporary imprisonment," regardless whether the terrorist acts occur. Law No. 1/2004 grants the Attorney General (or his deputies) the authority to order the review of information related to the accounts, assets, deposits, transfer, or property movements on which the Attorney General has "sufficient evidence to believe" are related to the funding or committing of a terror activity as defined in the law.

The law also provides for asset seizure and confiscation. Article 31 gives the Attorney General the authority to seize or freeze assets until the investigation is completed. Article 32 confirms the Central Bank's authority to freeze accounts for up to seven days if it suspects that the funds will be used to fund or commit any of the crimes listed in the law. The law also allows the right of appeal to "the

competent court" of any asset freeze under the law. The court will rule on the complaint within 14 days of receiving the complaint. Law No. 1/2004 also established the "National Anti-Terror Committee" (NATC) to serve as the government's interagency liaison with respect to implementing the United Nations Security Council Resolutions (UNSCR) on terrorism, and sharing information with its foreign counterparts as well as with the United Nations. Representatives from Ministries of Foreign Affairs, Interior, Justice, and Defense; Central Bank; State Security Department; and Federal Customs Authority comprise the NATC.

The Central Bank also ensures that it circulates an updated UNSCR 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations to all the financial institutions under its supervision. In 2007, the UAE took steps toward fulfillment of its UN nonproliferation obligations. On August 31, 2007 the UAE issued Law No. 13 of 2007 on export and import controls. With regard to the UAE's UNSCR 1737 and 1747 commitments, the UAE Central bank ordered banks and other financial institutions to freeze accounts or deposits of designated entities. It also ordered financial institutions to cease transfers on behalf of designated entities and to refrain from entering into new commitments for grants, financial assistance, and concession loans to the Iranian Government

The Anti-Money Laundering and Suspicious Case Unit (AMLSCU) was established in 2002 as the UAE's financial intelligence unit (FIU), and was housed within the Central Bank. In addition to receiving Suspicious Transaction Reports (STRs), the AMLSCU is authorized to send information requests to foreign regulatory authorities to conduct its preliminary investigations based on suspicious transaction report data. The AMLSCU joined the Egmont Group in June 2002. As of October 2007, the AMLSCU has received and investigated a total of 4392 suspicious transactions reports (STRs), for the period of December 2000 until April 2007. The AMLSCU reports that it has issued a total of 42 freeze orders in response to STRs between December 2000 (prior to the establishment of the FIU) and October 2006.

It is unclear how many money laundering prosecutions have taken place in the UAE in 2007. However, there were two high profile money laundering cases in the UAE during the 2006/2007 timeframe. In November, the Sharjah Appeals Court upheld a verdict sentencing seven men to five years in prison for money laundering. An Abu Dhabi court also sentenced two of the individuals to life imprisonment for drug trafficking and the rest to ten year sentences for drug trafficking. The individuals were arrested in 2006 for attempting to smuggle 2.5 tons of hashish from Pakistan to Holland, via Sri Lanka, the UK, and Belgium. UAE authorities worked with law enforcement officials in the respective countries to track the shipment. In October 2007, the Dubai police referred 48 suspects to the Public Prosecutors on charges of money laundering and abetting drug trafficking.

Several amendments were made to the Central Bank Regulations 24/2000 in July 2006. First, the regulations added the term "terrorist financing" to any references made to the term "money laundering." Second, the regulations required financial institutions to freeze transactions that they believe may be destined for funding terrorism, terrorist organizations, or for terrorist purposes. The regulations also require financial institutions to notify the AMLSCU in writing of such transactions "in case of any doubt". Finally, enhanced due diligence requirements for charities were promulgated, requiring banks to obtain a certificate from the Minister of Social Affairs before opening or maintaining any charitable organization-type account.

In 2006, the UAE enacted Law No. 2/2006 of the Cyber Crimes. Article 19 of the law criminalized the electronic transfer of money or property through the Internet in which the true sources of such assets are either concealed or linked to criminal proceeds. Violations are punishable by up to seven years imprisonment and fines ranging from approximately $8,170 to $54,500. Article 21 of the law outlaws the use of the Internet to finance terrorist activities, promote terrorist ideology, disseminate information on explosives, or to facilitate contact with terrorist leaders. Any violation of Article 21 is punishable by up to 5 years imprisonment.

Hawala is where money laundering activity is likely more prevalent due to the largely undocumented nature of this informal remittance system. Dubai is a regional hawala center. Hawala is an attractive mechanism for terrorist and criminal exploitation due to its nontransparency to law enforcement and regulators and the highly resilient nature of the system. In 2002, the Central Bank issued new regulations to help improve the oversight of hawala. The new regulations required hawala brokers (hawaladars) to register with the Central Bank, submit the names and addresses of all originators and beneficiaries of funds, and to file suspicious transaction reports on a monthly or quarterly basis. However, since the inception of the program, there reportedly have not been any suspicious reports filed by hawaladars.

As of October 2007, the Central Bank had registered 246 hawaladars, with an additional 70 applicants working to complete their registration requirements. Once registered, the Central Bank conducts one-on-one training sessions with each registered hawaladar to ensure that dealers understand the record-keeping and reporting obligations. The registered hawaladars are also required to use an account they open at the Central Bank to process their transactions. Currently, there is no accurate estimate of the total number of UAE-based hawala brokers, and there is no penalty for failure of hawaladars to register with the Central Bank. Officials argue that the registration program is still in the initial phase of determining the magnitude of the industry. As of August 2007, the Central Bank reported that it had received over 800 quarterly activity reports from hawaladars.

The UAE has not set any limits on the amount of cash that can be imported into or exported from the country. No reporting requirements exist for cash exports. However, the Central Bank requires that any cash imports over $10,900 must be declared to Customs; otherwise undeclared cash may be seized upon attempted entry into the country. All cash forfeiture cases are handled at the judicial level because there are no administrative procedures to handle forfeited cash. Still, enforcement mechanisms are lax. Customs officials, police, and judicial authorities tend to not regard large cash imports as potentially suspicious or criminal type activities, arguing that the UAE is a cash-based economy, and it is not unusual for people to carry significant sums of cash.

Dubai remains the center of the UAE's burgeoning diamond trade, although new facilities are springing up in the Emirates of Ajman and Ras Al Khaimah as interest spreads in the lucrative business. The UAE has been a member of the Kimberley Process Certification Scheme for Rough Diamonds since November 2002, and began certifying rough diamonds exported from the UAE on January 1, 2003. Law No. 13 of 2004 regulates supervision of Import/Export and Transit of Rough Diamonds. Article 5 of the law prohibits the import of rough diamonds, unless they are accompanied by a Kimberley Process certificate and in a sealed, tamper resistant container.

The Dubai Diamond Exchange (DDE), a subsidiary of the Dubai Multi Commodities Center (DMCC), is a quasi-governmental organization charged with issuing Kimberley Process (KP) certificates in the UAE, and employs four full-time individuals to administer the KP program. Prior to January 1, 2003, the DMCC circulated a sample UAE certificate to all KP member states and embarked on a public relations campaign to familiarize the estimated 50 diamond traders operating in Dubai with the new KP requirements. Under the KP regulations, UAE Customs is the sole point of entry for both rough and finished diamonds to the UAE. Customs officials are authorized to delay or even confiscate those diamonds entering the UAE from another KP member country that does not have the proper certificates.

In 2006, Russian customs officials reportedly apprehended an air passenger from Dubai after he tried to smuggle 2.5 kilos of diamonds into the country. There are also reports that diamonds are increasingly being used as a medium to provide counter valuation in hawala transfers, particularly between Dubai and Mumbai.

The former head of the Dubai Diamond Exchange implemented enhanced monitoring measures in compliance with the Moscow Resolution on Cote d'Ivoire of November 2005, but two suspect

diamond shipments of questionable provenance released by the DDE in 2006 and 2007 indicate continuing weaknesses in the process. The UN Group of Experts on Cote d'Ivoire, visiting Dubai in May 2007, raised with the DDE the release in September 2006 and January 2007, respectively, of two shipments of diamonds with suspect Ghanaian certificates of origin. In both cases the World Diamond Council was requested to verify the origin of the diamonds. In the first instance the WDC's Working Group Diamond Experts concluded that the assessed diamonds bore characteristics unknown in Ghanaian diamonds, but possibly consistent with stones from Guyana or Brazil. In the second case, the diamonds were released before the WDC's final report was released. The Group also reported that individuals in Dubai's Gold Land stated that they had in their possession large quantities of African diamonds without Kimberley Process certification.

The Securities and Commodities Authority (SCA) supervises the country's two stock markets. In February 2004, the SCA issued anti-money laundering guidelines to all brokers that included identity verification instructions for new customer accounts, a reporting requirement for cash transactions above U.S. $10,900, and a minimum five-year record keeping requirement for all customer account information. The SCA also instructed brokers to file suspicious transaction reports with the SCA for initial analysis before they are forwarded to the AMLSCU for further action.

The UAE's real estate market continues to grow with the various emirates following Dubai's model of opening up some property ownership to expatriates. Dubai's real estate market grew significantly in 2007, making this sector another area that is susceptible to money laundering abuse. In 2002, Dubai began to allow three real estate companies to sell "freehold" properties to noncitizens. Since then, several other emirates have followed suit. For instance, Abu Dhabi has passed a property law, which provides for a type of lease-hold ownership for noncitizens. In addition, citizens of GCC countries have the right to purchase and trade land within designated investment areas, while other expatriates are permitted to invest in real estate properties for a 99-year leasehold basis. Due to the intense interest in and reported cash purchases of such properties, the potential for money laundering has become of increased concern to the UAE Government. As a result, developers have stopped accepting cash purchases for these properties. The UAE does not have a central database to show registered property owners within the UAE, which encumbers international money laundering investigations.

Since the September 11, 2001 terrorist attacks, the UAE Government (UAEG) has been more sensitive to regulating charitable organizations and accounting for funds transfers abroad. In 2002, the UAEG mandated that all licensed charities interested in transferring funds overseas must do so via one of three umbrella organizations: the Red Crescent Authority, the Zayed Charitable Foundation, or the Muhammad Bin Rashid Charitable Trust. These three quasi-governmental bodies are in a position to ensure that overseas financial transfers go to legitimate parties. As an additional step, the UAEG has contacted the governments in numerous aid receiving countries to compile a list of recognized acceptable recipients for UAE charitable assistance.

Charities are regulated by the UAE Ministry of Social Affairs, which is responsible for licensing and monitoring registered charities in these emirates. The Ministry also requires these charities to keep records of all donations and beneficiaries, and to submit financial reports annually. Charities in Dubai are licensed and monitored by the Dubai Department of Islamic Affairs and Charitable Activities. Some charities, however, particularly those located in the Northern Emirates, are only registered with their local emirate authority and not the federal Ministry. In July 2006, Regulation 24/2000 was amended, requiring charities from all emirates to obtain a certificate from the Minister of Social Affairs before being permitted to open or maintain bank accounts in the UAE. This amendment effectively required that all charities must be registered federally and no longer at just the emirate level. In November 2006, the UAE hosted a United Kingdom/Gulf Cooperation Council conference on charities, and made a proposal to hold biannual meetings going forward with the UK and GCC on charities oversight.

The UAE has both free trade zones (FTZs) and one financial free zone (FFZ). The number of FTZs is growing, with 37 operating in the UAE. Every emirate except Abu Dhabi has at least one functioning FTZ. The free trade zones are monitored by the local emirate rather than federal authorities.

There are over 5,000 multinational companies located in the FTZs, and thousands more individual trading companies. The FTZs permit 100 percent foreign ownership, no import duties, full repatriation of capital and profits, no taxation, and easily obtainable licenses. Companies located in the free trade zones are considered offshore or foreign entities for legal purposes. However, UAE law prohibits the establishments of shell companies and trusts, and does not permit nonresidents to open bank accounts in the UAE. The larger FTZs in Dubai (such as Jebel Ali free zone) are well-regulated. Although some trade-based money laundering undoubtedly occurs in the large FTZs, a higher potential for financial crime exists in some of the smaller FTZs located in the northern emirates.

In March 2004, the UAEG passed Federal Law No. 8, regarding the Financial Free Zones (FFZs) (Law No. 8/2004). Although the new law exempts FFZs and their activities from UAE civil, and commercial laws, FFZs and their operations are still subject to federal criminal laws including the Anti-Money Laundering Law (Law No. 4/2002) and the Anti-Terror Law (Law No. 1/2004). As a result of Law 8/2004 and a subsequent federal decree, the UAE's first financial free zone (FFZ), known as the Dubai International Financial Center (DIFC), was established in September 2004. By September 2005, the DIFC had opened its securities market, the Dubai International Financial Exchange (DIFX).

Law No. 8/2004 limits the issuance of licenses for banking activities in the FFZs to branches of companies, joint companies, and wholly owned subsidiaries provided that they "enjoy a strong financial position and systems and controls, and are managed by persons with expertise and knowledge of such activity." The law prohibits companies licensed in the FFZ from dealing in UAE currency (i.e., dirham), or taking "deposits from the state's markets." Further, the law stipulates that the licensing standards of companies "shall not be less than those applicable in the state." The law empowers the Emirates Stocks and Commodities Authority to approve the listing of any company listed on any UAE stock market in the financial free zone, as well as the licensing of any UAE stock broker. Insurance activities conducted in the FFZ are limited by law to reinsurance contracts only. The law further gives competent authorities in the Federal Government the power to inspect financial free zones and submit their findings to the UAE cabinet.

In 2007 the Cabinet issued Resolution No. 28 that provided implementing regulations for financial free zones. The regulations specify that FFZs submit their semi-annual reports on activities and compliance to the UAE Cabinet. The regulations also spell out that inspections of FFZs will be carried out by cabinet resolution through a ministerial committee. These inspections will be carried out in cooperation with the FFZs. Results will be referred to the cabinet for action. The Regulation also instructs the FFZs to enter into Memorandums of Understanding (MOUs) with relevant authorities, such as the Central Bank, the Ministry of Economy, the Securities and Commodities Authority, and the Insurance Authority, for the purposes of better coordination, cooperation, and control.

DIFC regulations provide for an independent regulatory body, namely the Dubai Financial Services Authority (DFSA), to report its findings directly to the office of the Dubai ruler and an independent Commercial Court. According to DFSA regulators, the DFSA due diligence process is a risk-based assessment that examines a firm's competence, financial soundness, and integrity. Prior to the inauguration of the DIFC in 2004, several observers called into question the independence of the DFSA as a result of the high profile firings of the chief regulator and the head of the regulatory council (i.e., the supervisory authority). Subsequent to the firings, Dubai passed laws that gave the DFSA more regulatory independence from the DIFC, although these laws have not yet been tested. The DFSA, who modeled its regulatory regime after the United Kingdom, is the sole authority responsible for issuing licenses to those firms providing financial services in the DIFC.

The DFSA has licensed 156 institutions to operate within the DIFC as authorized firms licensed to carry on financial services in or from the DIFC. The DFSA also regulates ancillary service providers (provide legal or accountancy services in the DIFC). The DFSA prohibits offshore casinos or Internet gaming sites in the UAE, and requires firms to send suspicious transaction reports to the AMLSCU (along with a copy to the DFSA). To date, there have been 18 suspicious transaction reports issued from firms operating in the DIFC (nine in 2007). Although firms operating in the DIFC are subject to Law No. 4/2002, the DFSA has issued its own anti-money laundering regulations and supervisory regime, which has caused some ambiguity about the Central Bank's and the AMLSCU's respective authorities within the DIFC. Ongoing discussions continue between the DFSA and the UAE Central Bank to create a formal bilateral arrangement.

As a result, the DIFC acknowledged the need to enhance its regulatory and compliance authority. On July 18, 2007, it enacted regulations for nonfinancial Anti-Money Laundering Anti Terrorist Finance which applies Financial Action Task Force (FATF) compliant requirements in the DIFC jurisdiction to real estate agents, dealers in precious metals and stones, dealers in high value goods (cash payments of over U.S. $15,000), nonAuthorized Service Providers, lawyers, accountants, auditors, and nonDFSA regulated Trust and Company Service Providers. These regulations do not apply to DFSA regulated firms. With regard to auditors and accountants, for example, this would apply to those that do not audit authorized firms. The DFSA has undertaken a campaign to reach out to other international regulatory authorities to facilitate information sharing. As of November 2007, the DFSA has MOUs with several other regulatory bodies, including the UK's Financial Services Authority (FSA), the Emirates Securities and Commodities Authority, and the U.S. Commodity Futures Trading Commission (CFTC). On October 23, 2007, the DFSA entered into a MOU with the five U.S. banking supervisors.

The UAE is a party to the 1988 UN Drug Convention and to all twelve UN conventions and protocols relating to the prevention and suppression of international terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism. It has signed and ratified the UN Convention against Corruption. The UAE ratified the UN Convention against Transnational Organized Crime on May 7, 2007. The UAE supported the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF) in November 2004, and will assume its presidency for 2008.

International Monetary Fund (IMF) conducted and assessment of the UAE financial system in 2007. The report concluded that the government of the UAE is in the midst of implementing an important agenda for further strengthening the country's banking system and its prudential and regulatory oversight. The report contains no information on the UAE compliance with the FATF's 40 recommendations and Nine Special Recommendations.

The Government of the UAE has shown some progress in enhancing its AML/CTF program. Information sharing between the AMLSCU and foreign FIUs has substantially improved. However, several areas requiring further action by the UAEG remain. Law enforcement and customs officials need to proactively recognize money laundering activity and develop cases based on investigations, rather than wait for case referrals from the AMLSCU that are based on SARs. Additionally, law enforcement and customs officials should conduct more thorough inquiries into large and undeclared cash imports into the country, as well as require—and enforce—outbound declarations of cash and gold. All forms of trade-based money laundering must be given greater scrutiny by UAE customs and law enforcement officials, including customs fraud, the trade in gold and precious gems, commodities used as counter-valuation in hawala transactions, and the misuse of trade to launder narcotics proceeds. The UAE should increase the resources it devotes to investigation of AML/CTF both federally at the AMLSCU and at emirate level law enforcement. The Central Bank should move from the initial phase of hawaladar registration to compliance and enforcement coupled with investigations. The cooperation between the Central Bank and the DFSA needs improvement, and lines of authority need to be clarified. Cabinet Resolution No. 28 of 2007 should help in this regard. The UAE should

conduct more follow-ups with financial institutions and the MSA regarding the recent tightening of regulations on charities to ensure their registration at the federal level. The UAE should also continue its regional efforts to promote sound charitable oversight, and engage in a public campaign to ensure all local charities are aware of registration requirements. The IMF recently conducted the UAE's mutual evaluation AML/CTF assessment, which is scheduled for discussion at the April 2008 MENAFATF Plenary and the June 2008 FATF Plenary. The UAE should work toward implementing the recommendations of the IMF assessment upon its completion.

United Kingdom

The United Kingdom (UK) plays a leading role in European and world finance and remains attractive to money launderers because of the size, sophistication, and reputation of its financial markets. Although narcotics are still a major source of illegal proceeds for money laundering, the proceeds of other offenses, such as financial fraud and the smuggling of people and goods, have become increasingly important. The past few years have witnessed the movement of cash placement away from High Street banks and mainstream financial institutions as these entities have tightened their controls and increased their vigilance. The use of bureaux de change, cash smugglers (into and out of the UK), and traditional gatekeepers (including solicitors and accountants) to move and launder criminal proceeds has been increasing since 2002. Also on the rise are credit/debit card fraud and the purchasing of high-value assets to disguise illegally obtained money.

Criminal proceeds are mostly generated in the large metropolitan areas in the UK. Drug traffickers and other criminals are able to launder substantial amounts of money in the UK despite improved anti-money laundering measures introduced under the 2002 Proceeds of Crime Act (POCA). Much of the money made in the UK benefits criminals who operate in the UK. Cities such as London, Liverpool and Birmingham have large drug markets and also serve as supply points for markets in smaller cities and towns, drawing in significant flows of illicit cash.

According to an analysis by the UK's Serious Organized Crime Agency (SOCA), such crimes in the UK generate about £15 billion (approximately U.S. $29.3 billion) per annum. Businesses that are particularly attractive to criminals are those with high cash turnovers and those involved in overseas trading. Illicit cash is consolidated in the UK, and then moved overseas where it can more readily enter the legitimate financial system, either directly or by means such as purchasing property. Cash can be smuggled in a number of ways: it can be transported by courier, freight or post and moved through the various points of exit from the UK. Cash smuggling techniques are adaptable; smugglers can easily change techniques if they suspect law enforcement is targeting a particular route or method.

Because cash is the mainstay of the drugs trade, traffickers make extensive use of money transmission agents (MTA), cash smuggling, and Informal Value Transfer Systems ("underground banking") to remove cash form the UK. Heroin proceeds from the UK are often laundered through Dubai en route to traffickers in Pakistan and Turkey. Cocaine proceeds are repatriated to South America via Jamaica and Panama.

As money laundering laws become stricter, money laundering becomes more difficult. Because dealers in the UK generally collect sterling, most traffickers are left with excess small currency (usually £10 notes). This has created cash smuggling operations to move large sums of sterling out of the country. The SOCA analysis suggests that more sterling has exited the UK in recent years than entered due to the relative ease of converting sterling in other countries.

The UK has implemented many of the provisions of the Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations. Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from other serious crimes has been criminalized by subsequent legislation. Banks and nonbank financial institutions in the UK must

report suspicious transactions. The UK underwent a FATF mutual evaluation process in 2006, and the report was accepted by that body in June 2007. The mutual evaluation report (MER) cited many improvements to the anti-money laundering and counter-terrorist financing (AML/CTF) regime since the previous on-site assessment, conducted in 1996. On the 49 recommendations, the UK received 24 ratings of "compliant" and 12 ratings of "largely compliant." Of the 5 core FATF recommendations (Recommendations 1, 5, 10, and 13, Special Recommendations II and IV), the UK's AML/CTF regime was deemed at least compliant in all of them.

In 2001, money laundering regulations were extended to money service bureaus (e.g., bureaux de change, money transmission companies), and in September 2006, the Government published a review of the regulation and performance of money service businesses in preventing money laundering and terrorist financing. Since 2004, more business sectors are subject to formal suspicious activity reporting (SAR) requirements, including attorneys, solicitors, accountants, real estate agents, and dealers in high-value goods, such as cars and jewelry. Sectors of the betting and gaming industry that are not currently regulated are being encouraged to establish their own codes of practice, including a requirement to disclose suspicious transactions.

Following an extensive consultation period in late 2006, Her Majesty's Treasury published Money Laundering Regulations in July 2007. The regulations implement the Directive 2005/60/EC (also known as the Third EU Money Laundering Directive), agreed under the UK's EU Presidency in 2005. The provisions include: extended supervision so that all businesses in the regulated sector comply with money laundering requirements; strict tests of money services businesses; extra checks on customers identified by firms as posing a high risk of money laundering; a requirement to establish the source of wealth of customers who are high ranking public officials overseas; and a strengthened and risk-based regime in casinos, in line with international standards. The regulations took effect December 15, 2007. EU Council Regulation No. 1889/2005, known as the "Cash Controls Regulation", also became applicable in the UK on June 15, 2007. This regulation obliges each EU state to maintain a cash declaration system for every person entering or exiting the EU with 10,000 euros cash or its equivalent in other currencies. The UK employs a written declaration system.

The Proceeds of Crime Act 2002 (POCA) created a new criminal offense, applicable to all regulated sectors, of failing to disclose suspicious transactions in respect to all crimes, not just "serious," narcotics- or terrorism-related crimes, as had previously been the rule. The POCA also expanded investigative powers relative to large movements of cash. Sections 327 to 340 of the Act address possession, acquisition, transfer, removal, use, conversion, concealment or disguise of criminal or terrorist property, inclusive of but not limited to money. The POCA also criminalizes tipping off. The "Money Laundering Regulations 2003," along with amending orders for the POCA and the Terrorism Act, impose requirements on various entities, including attorneys, and introduce a client identification requirement, requirements on internal reporting procedures and training. The introduction of the Fraud Act 2006, which took effect on 15 January 2007, saw significant changes to offenses in the fraud and forgery offence group. Changes were also made to the way in which the police record fraud offenses.

The UK's banking sector provides accounts to residents and nonresidents, who can open accounts through various intermediaries that often advertise on the Internet and also offer various offshore services. Private banking constitutes a significant portion of the British banking industry. Both resident and nonresident accounts are subject to the same reporting and record-keeping requirements. Individuals typically open nonresident accounts for tax advantages or for investment purposes.

Bank supervision falls under the Financial Services Authority (FSA). The FSA's primary responsibilities relate to the safety and soundness of the institutions under its jurisdiction. The FSA also plays an important role in the fight against money laundering through its continued involvement in the authorization of banks, and investigations of money laundering activities involving banks. The FSA regulates some 29,000 firms, which include European Economic Area (EEA) firms "passporting"

into the UK (firms doing business on a cross-border basis), ranging from global investment banks to very small businesses, and around 165,000 individuals. The FSA also regulates mortgage and general insurance agencies, totaling over 30,000 institutions. The FSA administers a civil-fines regime and has prosecutorial powers. The FSA has the power to make regulatory rules with respect to money laundering, and to enforce those rules with a range of disciplinary measures (including fines) if the institutions fail to comply. In October 2006, the financial services sector adopted National Occupational Standards of Competence in the fields of compliance and in anti-money laundering. The 2007 FATF mutual evaluation cited a number of concerns including the enforceability of the guidance to some financial institutions regarding customer due diligence, politically exposed persons, and beneficial ownership.

The Serious Organized Crime and Police Act of 2005 (SOCAP) amended the money laundering provisions in the POCA. One of these changes was the creation of the Serious Organized Crime Agency (SOCA), which houses the UK's financial intelligence unit (FIU). In 2006, SOCA assumed all FIU functions from the National Criminal Intelligence Service (NCIS). SOCA has three functions: the prevention and detection of serious organized crime; the mitigation of the consequences of such crime; and the function of receiving, storing, analyzing and disseminating information, including suspicious activity reports (SARs). Under the law, SOCA's functions are not restricted to serious or organized crime but are applicable to all crimes, and those functions include assistance to other agencies in their enforcement responsibilities. The number of SARs has steadily increased since the establishment of the SOCA even with the slightly relaxed reporting requirements, that allow banks (but no other obliged entities) to proceed with low value transactions not exceeding 250 pounds (approximately $500) involving suspected criminal property without requiring specific consent to operate the account. However, the reporting of every such transaction is still required. Additionally, under the SOCAP, foreign acts would no longer be considered money laundering and would not be considered as such if they do not violate the law in the foreign jurisdiction.

The Serious Crime Act 2007 merges ARA's operational arm with the Serious Organised Crime Agency (SOCA) and ARA's training function with the National Policing Improvement Authority (NPIA), as well as extending the powers of civil recovery to wider prosecution authorities and the powers of cash seizure to a wider range of law enforcement bodies. The POCA has enhanced the efficiency of the forfeiture process and increased the recovered amount of illegally obtained assets by consolidating existing laws on forfeiture and money laundering into a single piece of legislation, and, perhaps most importantly, creating a civil asset forfeiture system for the proceeds of unlawful conduct. The Assets Recovery Agency (ARA), established to enhance financial investigators' power to request client information from any bank, is a product of this legislation. The Act provides for confiscation orders and for restraint orders to prohibit dealing with property. It also allows for asset recovery of property obtained through or used for unlawful conduct. Furthermore, the Act shifts the burden of proof to the holder of the assets to prove that the assets were acquired through lawful means. In the absence of such proof, assets may be forfeited, even without a criminal conviction. The Act gives standing to overseas requests and orders concerning property believed to be the proceeds of criminal conduct. The POCA also provides the ARA with a national standard for training investigators, and gives greater powers of seizure at a lower standard of proof. In light of this, Her Majesty's Revenue and Customs (HMRC) has increased its national priorities to include investigating the movement of cash through money exchange houses and identifying unlicensed money remitters. The total value of assets recovered by all agencies under the Act (and earlier legislation) in England, Wales, and Northern Ireland approximately U.S. $250 million in 2006, a fivefold increase in five years.

In one illustrative case, Operation Labici was an investigation into an organized group of money launderers operating in the UK but controlled from Dubai and Pakistan. They used hawala, to eventually move drug money between the UK, Pakistan and Dubai as well as to and from other countries. The UK end of the organization provided laundering services to UK drug dealers. Records

seized showed that almost £15 million (U.S. $30 million) in cash had been passed. In September 2007 the last of eight men was sentenced as a result of Operation Labici. The main defendant received ten years imprisonment; the eight defendants together received 39 years for money laundering.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual to provide financial or related services, directly or indirectly, to or for the benefit of a person who commits, attempts to commit, facilitates, or participates in the commission of acts of terrorism. The Order also makes it an offense for a covered entity to fail to disclose to Her Majesty's Treasury a suspicion that a customer or entity is attempting to participate in acts of terrorism. The Anti-Terrorism, Crime, and Security Act 2001 provides for the freezing of assets. In March 2006, the Terrorism Act received Royal Assent. This Act aims to impede the encouragement of others to commit terrorist acts, and amends existing legislation by introducing warrants enabling police to search any property owned or controlled by a terrorist suspect. The Act also extends terrorism stop and search powers to cover bays and estuaries, with improved search powers at ports; extends police powers to detain suspects after arrest for 28 days (although intervals exceeding two days must be approved by a judicial authority); and increases the flexibility of the proscription regime, including the power to proscribe groups that glorify terrorism.

As a direct result of the events of September 11, 2001, the FID established a separate National Terrorist Financing Investigative Unit (NTFIU), controlled by the Metropolitan Police Services (MPS), also known as "Scotland Yard," to maximize the effect of reports from the regulated sector. The NTFIU chairs a law enforcement group to provide outreach to the financial industry concerning requirements and typologies. The operational unit that responds to the work and intelligence development of the NTFIU has seen a threefold increase in staffing levels directly due to the increase in the workload. The Metropolitan Police has responded to the growing emphasis on terrorist financing by expanding the focus and strength of its specialist financial unit dedicated to this area of investigations.

Charitable organizations and foundations are subject to supervision by the UK Charities Commission. Such entities must be licensed and are subject to reporting and record-keeping requirements. The Commission has investigative and administrative sanctioning authority, including the authority to remove management, appoint trustees and place organizations into receivership. The Government intends to revise its reporting requirements to develop a risk-based approach to monitoring with a new serious incident reporting function for charities.

The UK cooperates with foreign law enforcement agencies investigating narcotics-related financial crimes. The UK is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. SOCA is a member of the Egmont Group and has information sharing arrangements in place with the FIUs of the United States, Belgium, France, and Australia. The Mutual Legal Assistance Treaty (MLAT) between the UK and the United States has been in force since 1996, and the two countries signed a reciprocal asset sharing agreement in March 2003. The UK also has an MLAT with the Bahamas. Additionally, there is a memorandum of understanding in force between the U.S. Immigration and Customs Enforcement and HM Revenue and Customs.

The United Kingdom has a comprehensive AML/CTF regime. However, as discussed in the FATF mutual evaluation, there are areas that should be further addressed by the authorities. The UK should develop legislation and clearly enforceable implementing regulations to ensure that beneficial owners are identified and verified and that customer due diligence is required and ongoing, regardless of an already established relationship with the client. The UK should also develop clear regulations regarding politically exposed persons as well as correspondent banking relationships. Risk-based measures should be codified and taken, not only in the context of customer due diligence, but also

with regard to the identification and treatment of wire transfers, the standards and measures set by the designated nonfinancial businesses and professions, and to more effectively target the resources of the supervisory entities. The 2005 Gambling Act should be amended to require the gaming industry to be covered in the same manner as the financial and designated nonfinancial businesses and professions, including giving the Gambling Commission a full range of sanctions. Authorities should track and examine the effects of the SOCAP change regarding acts and assets in or from foreign jurisdictions, and revisit this legislation to determine whether it has been effective, or whether it has enabled exploitation. Authorities should also ensure the FIU's operational and authoritative independence.

Uruguay

In the past, Uruguay's strict bank secrecy laws, liberal currency exchange, capital mobility regulations, and overall economic stability made it a regional financial center vulnerable to money laundering, though the extent and the nature of suspicious financial transactions have been unclear. In 2002, banking scandals and mismanagement, along with massive withdrawals of Argentine deposits, led to a near collapse of the Uruguayan banking system, significantly weakening Uruguay's role as a regional financial center. This crisis has diminished the attractiveness of Uruguayan financial institutions for money launderers in the medium term.

Uruguay is a founding member of the Financial Action Task Force for South America (GAFISUD). Since early 2005, the former director of the Government of Uruguay's (GOU) Center for Training on Money Laundering Issues (CECPLA) has served as the GAFISUD Executive Secretary. In 2005, the IMF concluded a thorough examination of Uruguay's money laundering regime, which also served as a GAFISUD mutual evaluation. The examination recognized Uruguay's advances with its new legislation but pointed out that some regulations still needed to be drafted. It also noted the understaffing of Uruguay's financial intelligence unit (FIU). An IMF risk assessment is planned for March 2008.

Money laundering is criminalized under Law 17.343 of 2001 and Law 17.835 of 2004. Under Law 17.343, predicate offenses include narcotics trafficking; corruption; terrorism; smuggling (value over U.S. $20,000); illegal trafficking in weapons, explosives and ammunition; trafficking in human organs, tissues, and medications; trafficking in human beings; extortion; kidnapping; bribery; trafficking in nuclear and toxic substances; and illegal trafficking in animals or antiques. Money laundering is considered an offense separate from the underlying crimes. The courts have the power to seize and confiscate property, products or financial instruments linked to money laundering activities. Law 17.835 significantly strengthens the GOU's anti-money laundering regime by including specific provisions related to the financing of terrorism and to the freezing of assets linked to terrorist organizations, as well as provisions for undercover operations and controlled deliveries.

The first arrest and prosecution for money laundering under Law 17.835 occurred in October 2005. The case is still underway. A more recent high profile case, involving money laundering tied to the largest cocaine seizure in Uruguay's history is also underway, with 14 people indicted in September 2006 for money laundering. This case has significantly invigorated the GOU's efforts to fight money laundering and to push for increased reporting of suspicious activities. A more recent case (September 2007), also involving a large cocaine seizure and proceeds from trafficking, is in the initial stages of investigation. There have been no prosecutions in 2007.

Uruguay's FIU, the Financial Information and Analysis Unit (UIAF), is a directorate of the Central Bank. Created in 2000 under Central Bank Circular 1722, the UIAF receives, analyzes, and disseminates suspicious activity reports (SARs). Law 17.835 of 2004 expands the realm of entities required to file SARs, makes reporting of such suspicious financial activities a legal obligation, and confers on the UIAF the authority to request additional related information.

Compliance by reporting entities has increased from 94 SARs in all of 2006 to 98 SARs in just the first half of 2007. While the level of staffing at the UIAF is still not adequate, the Central Bank has hired 3 additional staff for a total of 7 full-time personnel and established a timeline of June 2008 to reach full staffing of 19 people. The recent high profile narcotics money laundering cases have provided a boost to the Central Bank's efforts. In addition, the UIAF is updating its hardware and software systems through funding from the Organization of American States.

Under Law 17.835, all obligated entities must implement anti-money laundering policies, such as thoroughly identifying customers, recording transactions over U.S. $10,000 in internal databases, and reporting suspicious transactions to the UIAF. This obligation extends to all financial intermediaries, including banks, currency exchange houses, stockbrokers, insurance companies, casinos, art dealers, and real estate and fiduciary companies. Implementing regulations have been issued by the Central Bank for all entities it supervises (banks, currency exchange houses, stockbrokers, and insurance companies), and are being issued by the Ministry of Economy and Finance for all other reporting entities. On November 26, 2007, the Central Bank issued Circular 1.978, which requires financial intermediary institutions, exchange houses, credit administration companies and correspondent financial institutions to implement detailed anti-money laundering and counter-terrorist financing policies, and report wire transfers over U.S. $1,000. This circular requires these institutions to pay special attention to business with politically exposed persons (PEPs); persons, companies, and financial institutions from countries that are not members of the Financial Action Task Force (FATF) or a FATF-style regional body; and persons, companies, and financial institutions from countries that are subject to FATF special measures for failure to comply with the FATF Recommendations.

Law 17.835 also extends reporting requirements to all persons entering or exiting Uruguay with over U.S. $10,000 in cash or in monetary instruments. This measure has resulted in the seizure of over U.S. $720,000 in undeclared cross-border movements since the declaration requirement entered into force in December 2006.

Three government bodies are responsible for coordinating GOU efforts to combat money laundering: the UIAF, the National Drug Council, and the Center for Training on Money Laundering (CECPLA). The President's Deputy Chief of Staff heads the National Drug Council, which is the senior authority for anti-money laundering policy. The Director of CECPLA serves as coordinator for all government entities involved and sets general policy guidelines. The Director defines and implements GOU policies, in coordination with the Finance Ministry and the UIAF. The Ministry of Economy and Finance, the Ministry of the Interior (via the police force), and the Ministry of Defense (via the Naval Prefecture) also participate in anti-money laundering efforts. The financial private sector, most of which is foreign-owned, has developed self-regulatory measures against money laundering, such as the Codes of Conduct approved by the Association of Banks and the Chamber of Financial Entities (1997), the Association of Exchange Houses (2001), and the Securities Market (2002).

Despite the power of the courts to confiscate property linked to money laundering, real estate ownership is not publicly registered in the name of the titleholder, complicating efforts to track money laundering in this sector, especially in the partially foreign-owned tourist industry. The UIAF and other government agencies must obtain a judicial order to have access to the name of titleholders. The GOU is in the process of implementing a national computerized registry that will facilitate the UIAF's access to titleholders' names. Data is being progressively loaded into the system, with a completion target date of December 2008. The UIAF is already using the loaded data for investigation purposes.

Fiduciary companies called "SAFIs" are also thought to be a convenient conduit for illegal money transactions. As of January 1, 2006, all SAFIs are required to provide the names of their directors to the Finance Ministry. In addition, the GOU implemented a comprehensive tax reform law in July 2007, which prohibited the establishment of new SAFIs as of that date. All existing SAFIs are to be

eliminated by 2010. The tax reform law also implemented a personal income tax for the first time in Uruguay.

Offshore banks are subject to the same laws and regulations as local banks, with the GOU requiring them to be licensed through a formal process that includes a background investigation. There are six offshore banks and 21 representative offices of foreign banks. Offshore trusts are not allowed. Bearer shares may not be used in banks and institutions under the authority of the Central Bank, and any share transactions must be authorized by the Central Bank. There are eight free trade zones in Uruguay, all but two being little more than warehouses for regional distribution. The other two house software development firms, back-office operations, call centers, and some light manufacturing/assembly. Some of the warehouse-style free trade zones have been used as transit points for containers of counterfeit goods bound for Brazil and Paraguay.

The GOU states that safeguarding the financial sector from money laundering is a priority, and Uruguay remains active in international anti-money laundering efforts. Uruguay is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. In January 2007, the GOU ratified the UN Convention against Corruption and the OAS Inter-American Convention against Terrorism. The GOU is a member of GAFISUD and the OAS Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering. The USG and the GOU are parties to extradition and mutual legal assistance treaties that entered into force in 1984 and 1994, respectively.

Uruguay is one of only two countries in South America that is not a member of the Egmont Group of financial intelligence units. Egmont membership would allow its UIAF greater access to financial information that is essential to its efforts to combat money laundering and terrorist financing. The UIAF plans on presenting its candidacy to the Egmont Group in June 2008, with the sponsorship of Spain, Peru, Argentina and Colombia.

The Government of Uruguay has taken significant steps over the past few years to strengthen its anti-money laundering and counter-terrorist financing regime. The passage of legislation criminalizing terrorist financing places Uruguay ahead of many other nations in the region. The UIAF's future membership in the Egmont Group, as well as the GOU's continued implementation and enforcement of its anti-money laundering and counter-terrorist financing programs, should continue to be priorities for the GOU.

Uzbekistan

Uzbekistan is not an important regional financial center and does not have a well-developed financial system. Legitimate business owners, ordinary citizens, and foreign residents generally attempt to avoid using the Uzbek banking system for transactions except when absolutely required, because of the onerous nature of the Government of Uzbekistan's (GOU) financial control system, the fear of GOU seizure of one's assets, and lack of trust in the banking system as a whole. As a result, Uzbek citizens have functioning bank accounts only if they are required to do so by law. They only deposit funds they are required to deposit and often resort to subterfuge to avoid depositing currency. The Central Bank of Uzbekistan (CBU) states that deposits from individuals have been increasing over the past five years.

Narcotics proceeds are controlled by local and regional drug-trafficking organizations and organized crime. Foreign and domestic proceeds from criminal activity in Uzbekistan are held either in cash, high-value transferable assets, such as gold, property, or automobiles, or in foreign bank accounts.

There is a significant black market for smuggled goods in Uzbekistan. Since the GOU imposed a very restrictive trade and import regime in the summer of 2002, smuggling of consumer goods, already a

considerable problem, increased dramatically. Many Uzbek citizens continue to make a living by illegally shuttle-trading goods from neighboring countries and regions, Iran, India, Korea, the Middle East, Europe, and the U.S. The black market for smuggled goods does not appear to be significantly funded by narcotics proceeds. It is likely, however, that drug dealers use the robust black market to clean their drug-related money.

Reportedly, the unofficial, unmonitored cash-based market creates an opportunity for small-scale terrorist or drug-related laundering activity destined for internal operations. For the most part, the funds generated by smuggling and corruption are not directly laundered through the banking system but through seemingly legitimate businesses such as restaurants and high-end retail stores. There appears to be virtually no money laundering through formal financial institutions in Uzbekistan because of the extremely high degree of supervision and control over all bank accounts in the country exercised by the Central Bank, Ministry of Finance, General Prosecutor's Office (GPO), and state-owned and controlled banks. Although Uzbek financial institutions are not known to engage in illegal transactions in U.S. currency, illegal unofficial exchange houses, where the majority of cash-only money laundering takes place, deal in Uzbek soum and U.S. dollars. Moreover, drug dealers and others can transport their criminal proceeds in cash across Uzbekistan's porous borders for deposit in the banking systems of other countries, such as Kazakhstan, Russia or the United Arab Emirates.

Money laundering from the proceeds from drug-trafficking and other criminal activities is a criminal offense. Article 41 of the Law on Narcotic Drugs and Psychotropic Substances (1999) stipulates that any institution may be closed for performing a financial transaction for the purpose of legalizing (laundering) proceeds derived from illicit narcotics trafficking. GOU officials noted that there have been no related cases thus far in Uzbekistan.

Penalties for money laundering are from ten to fifteen years imprisonment, under Article 243 of the Criminal Code. This article defines the act of money laundering to include as punishable acts the transfer; conversion; exchange; or concealment of origin, true nature, source, location, disposition, movement and rights with respect to the assets derived from criminal activity. Although the law has been in effect for more than five years, there is still insufficient information to fully assess the implementation and use of this legislation. Officials from the State Prosecutor's Office reported that Article 243 does not work well because different judges and attorneys can interpret it in different ways.

The CBU, GPO, and the National Security Service (NSS) closely monitor all banking transactions to ensure that money laundering does not occur in the banking system. Banks are required to know, record, and report the identity of customers engaging in significant transactions, including the recording of large currency transactions at thresholds appropriate to Uzbekistan's economic situation. All transactions involving sums greater than U.S. $1,000 in salary expenses for legal entities and U.S. $500 in salaries for individuals must be tracked and reported to the authorities. The CBU unofficially requires commercial banks to report on private transfers to foreign banks exceeding U.S. $10,000. Depending on the type and amount of the transaction, banks are required to maintain records for time deposits for a minimum of five years, possibly not sufficient time to reconstruct significant transactions. The law protects reporting individuals with respect to their cooperation with law enforcement entities. However, reportedly, the GOU has not adopted "banker negligence" laws that make individual bankers responsible if their institutions launder money.

A new law to combat money laundering and terrorist financing, passed in 2004, took effect in January 2006. However, in April 2007 the main provisions of the law were suspended by a Presidential decree until January 2013. This essentially means there may not be an effective anti-money laundering law in Uzbekistan for the next six years. The provisions of the law required certain entities to report cash transactions above U.S. $40,000 (approximately), as well as suspicious transactions. GOU officials claimed that the anti-money laundering law burdened banks and investigators with reporting thousands

of benign suspicious transactions that wasted resources on investigations. They reported 17,000 suspicious transactions in a six-month period before the law was suspended compared with 400 in the six months following the suspension of the law. In addition, this law also covered some nonbanking financial institutions, such as investment foundations, depositaries and other types of investment institutions; stock exchanges; insurers; organizations which render leasing and other financial services; organizations of postal service; pawnshops; lotteries; and notary offices. It did not include intermediaries such as lawyers, accountants, or broker/dealers. Casinos are illegal in Uzbekistan.

An April 2006 Presidential decree established the Department on Combating Tax, Currency Crimes and Legalizations of Criminal Proceeds under the GPO. The Department, which the Government of Uzbekistan claims is the functional equivalent of a Financial Intelligence Unit (FIU), is charged with monitoring and preventing money laundering and terrorist financing. It analyzes information received from banks and financial institutions, creates and keeps electronic databases of financial crimes, and, when warranted, passes information to the CBU, tax and law enforcement authorities, or other parts of the GPO for investigation and prosecution of criminal activity. However, given the suspension of the main provisions of the anti-money laundering law in 2007, it is unclear whether there will be any investigations or prosecutions.

The Law on Banks and Bank Activity (1996), article 38, stipulates conditions under which banking information can be released to law enforcement, investigative and tax authorities, prosecutor's office and courts. Different conditions for disclosure apply to different types of clients—individuals and institutions. In September 2003, Uzbekistan enacted a bank secrecy law that prevents the disclosure of client and ownership information for domestic and offshore financial services companies to bank supervisors and law enforcement authorities. In all cases, private bank information can be disclosed to prosecution and investigation authorities, provided there is a criminal investigation underway. The information can be provided to the courts on the basis of a written request in relation to cases currently under consideration. Protected banking information also can be disclosed to tax authorities in cases involving the taxation of a bank's client. Additionally, under the 2006 Presidential decree and subsequent Cabinet of Ministers' resolution on the disclosure of information related to money laundering, it is mandatory for organizations involved in transactions with monetary funds and other property to report such transactions to the GPO's FIU. GOU officials noted that the secrecy law does not apply if a group is on a list of designated terrorist organizations.

Existing controls on transportation of currency across borders would, in theory, facilitate detection of the international transportation of illegal source currency. When entering or exiting the country, foreigners and Uzbek citizens are required to report all currency they are carrying. Residents and nonresidents may bring the equivalent of U.S. $10,000 into the country tax-free. Amounts in excess of this limit are assessed a one-percent duty. Nonresidents may take out as much currency as they brought in. However, residents are limited to the equivalent of U.S. $2,000. Residents wishing to take out higher amounts must obtain authorization to do so; amounts over U.S. $2,000 must be approved by an authorized commercial bank, and amounts over U.S. $5,000 must be approved by the CBU. International cash transfers to or from an individual person are limited to U.S. $5,000 per transaction; there is no monetary limit on international cash transfers made by legal entities, such as a corporation. However, direct wire transfers to or from other Central Asian countries are not permitted; a third country must be used.

International business companies are permitted to have offices in Uzbekistan and are subject to the same regulations as domestic businesses, if not stricter. Offshore banks are not present in Uzbekistan and other forms of exempt or shell companies are not officially present.

The Department of Investigation of Economic Crimes within the Ministry of Internal Affairs (MVD) conducts investigations of all types of economic offenses. A specialized structure within the NSS and the Department on Tax, Currency Crimes and Legalization of Criminal Proceeds is also authorized to

conduct investigations of money laundering offenses. Unofficial information from numerous law enforcement officials indicates that there have been few, if any, prosecutions for money laundering under article 243 of the Criminal Code since its enactment in 2001. Officials from the Office of the State Prosecutor reported that there were 11 money laundering-related cases in 2006 and five in 2007. Of these 16 recent cases, officials stated that three are still pending. The status or disposition of the other cases is unknown. Overall, the GOU appears to lack a sufficient number of experienced and knowledgeable agents to investigate money laundering.

Article 155 of Uzbekistan's Criminal Code and the law "On Fighting Terrorism" criminalize terrorist financing. The latter law names the NSS, the MVD, the Committee on the Protection of State Borders, the State Customs Committee, the Ministry of Defense, and the Ministry for Emergency Situations as responsible for implementing the counterterrorist legislation. The law names the NSS as the coordinator for government agencies fighting terrorism. The GOU has the authority to identify, freeze, and seize terrorist assets. Uzbekistan has circulated to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the names of individuals and entities included on the UN 1267 consolidated list. In addition, the GOU has circulated the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to the CBU, which has, in turn, forwarded these lists to banks operating in Uzbekistan. According to the CBU and the Office of the State Prosecutor, no assets have been frozen.

Other than a plan to step up enforcement of currency regulations, the GOU has taken no steps to regulate or deter alternative remittance systems such as hawala, black market exchanges, trade-based money laundering, or the misuse of gold, precious metals and gems. GOU officials noted that most overseas migrants work in more advanced countries such as Russia or Korea where remittances can be easily tracked through financial institutions. We are not aware of any legislative initiatives under consideration. Although officially there is complete currency convertibility, in reality convertibility requests can be significantly delayed or refused.

The GOU closely monitors the activities of charitable and nonprofit entities, such as NGOs, that can be used for the financing of terrorism. In February 2004, the Cabinet of Ministers issued Decree 56 to allow the government to vet grants to local NGOs from foreign sources, ostensibly to fight money laundering and terrorist financing. Given the degree of supervision of charities and other nonprofits, and the level of threat Uzbekistan perceives from the Islamic Movement of Uzbekistan (IMU) and other extremist organizations, it is extremely unlikely that the NSS would knowingly allow any funds to be funneled to terrorists through Uzbekistan-based charitable organizations or NGOs.

Uzbekistan has established systems for identifying, tracing, freezing, seizing, and forfeiting proceeds of both narcotics-related and money laundering-related crimes. Current laws include the ability to seize items used in the commission of crimes such as conveyances used to transport narcotics, farm facilities (except land) where illicit crops are grown or which are used to support terrorist activity, legitimate businesses if related to criminal proceeds and bank accounts. The banking community, which is entirely state-controlled and with few exceptions, state-owned, cooperates with efforts to trace funds and seize bank accounts. Uzbek law does not allow for civil asset forfeiture, but the Criminal Procedure Code provides for "civil" proceedings within the criminal case to decide forfeiture issues. As a practical matter, these proceedings are conducted as part of the criminal case. We are aware of no new legislation or changes in current law under active consideration by the GOU regarding seizure or forfeiture of assets. The obstacles to enacting such laws are largely rooted in the widespread corruption that exists within the country.

In 2000, Uzbekistan set up a fund to direct confiscated assets to law enforcement activities. In accordance with the regulation, the assets derived from the sale of confiscated proceeds and instruments of drug-related offenses were transferred to this fund to support entities of the NSS, the MVD, the State Customs Committee, and the Border Guard Committee, all of which are directly

involved in combating illicit drug trafficking. According to the GOU, a total of 115 million soum (approximately U.S. $97,000) has been deposited into this fund since its inception. Roughly U.S. $80,000 has been turned over to Uzbek law enforcement agencies. In 2004, however, the Cabinet of Ministers issued an order to close the Special Fund as of November 1, 2004. Under the new procedure, each agency manages the assets it seizes. There is also a specialized fund within the MVD to reward those officers who directly participate in or contribute to law enforcement efforts leading to the confiscation of property. This fund has generated 20 percent of its assets from the sale of property confiscated from persons who have committed offenses such as the organization of criminal associations, bribery and racketeering. The GOU enthusiastically enforces existing drug-related asset seizure and forfeiture laws. The GOU has not been forthcoming with information regarding the total dollar value of assets seized from crimes. Reportedly, existing legislation does not permit sharing of seized narcotics assets with other governments.

The GOU realizes the importance of international cooperation in the fight against drugs and transnational organized crime and has made efforts to integrate the country in the system of international cooperation. Uzbekistan has entered into agreements with Uzbek supervisors to facilitate the exchange of supervisory information including on-site examinations of banks and trust companies operating in the country. Uzbekistan has entered into bilateral agreements for cooperation or exchange of information on drug related issues with the United States, Germany, Italy, Latvia, Bulgaria, Poland, China, Iran, Pakistan, the Commonwealth of Independent States (CIS), and all the countries in Central Asia. It has multilateral agreements in the framework of the CIS, under the Shanghai Cooperation Organization, and under memoranda of understanding. An "Agreement on Narcotics Control and Law Enforcement Assistance" was signed with the United States on August 14, 2001, with two supplemental agreements that came into force in 2004.

Uzbekistan does not have a Mutual Legal Assistance Treaty with the United States. However, Uzbekistan and the United States have reached informal agreement on mechanisms for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious crime investigations. In the past, Uzbekistan has cooperated with appropriate law enforcement agencies of the USG and other governments investigating financial crimes and several important terrorist-related cases. However, cooperation in these areas has become increasingly problematic in an atmosphere of strained U.S.-Uzbekistan bilateral relations. Uzbekistan joined the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), a FATF-style regional body, at the group's December 2005 plenary meeting. The EAG will conduct a mutual evaluation of Uzbekistan in 2008, which will include an analysis of Uzbekistan's decision to suspend the key provisions of the money laundering law.

The GOU is an active party to the relevant agreements concluded under the CIS, the Central Asian Economic Community (CAEC), the Economic Cooperation Organization (ECO), the Shanghai Cooperation Organization, and the "Six Plus Two" Group on Afghanistan. Uzbekistan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Uzbekistan has yet to become a party to the UN Convention against Corruption.

A lack of trained personnel, resources, and modern equipment continues to hinder Uzbekistan's efforts to fight money laundering and terrorist financing. Moreover, the April 2007 decree suspending the main provisions of the money laundering law until 2013 is likely to result in major setbacks. The GOU should rescind this decree, reinstating the provisions of the law, while continuing to refine its pertinent legislation to bring it up to international standards. Additional refinements should expand the cross-border currency reporting rules to cover the transfer of monetary instruments, and precious metals and gems. Access to financial institution records should be given to appropriate regulatory and law enforcement agencies so that they can properly conduct compliance examinations and investigations. While the establishment of an FIU was a positive step in 2006, much will depend, in the future, on the

unit's ability to effectively cooperate with other GOU law enforcement and regulatory agencies in receiving and disseminating information on suspicious transactions. In the short term, FIU operations will depend on whether there is any incoming reporting activity at all, given the suspension of the law.

Vanuatu

Vanuatu's offshore sector is vulnerable to money laundering, as Vanuatu has historically maintained strict banking secrecy provisions that have the effect of preventing law enforcement agencies from identifying the beneficial owners of offshore entities registered in the sector. Due to allegations of money laundering, and in response to pressure from the Financial Action Task Force (FATF), a few United States-based banks announced in December 1999 that they would no longer process U.S. dollar transactions to or from Vanuatu. The Government of Vanuatu (GOV) responded to these concerns by introducing reforms designed to strengthen domestic and offshore financial regulation. The GOV passed amendments to four of its main pieces of legislation relative to money laundering and terrorist financing during its last session of Parliament in November 2005. The four pieces of legislation affected are the Mutual Assistance in Criminal Matters Act No. 31 of 2005, the Financial Transaction Reporting Act No. 28 of 2005, the Counter-Terrorism and Transnational Organized Crime Act No. 29 of 2005, and the Proceeds of Crime Act (Amendment) Act No. 30 of 2005. The International Companies Act was amended in 2006. Taken with Ministerial Order No. 15 (April 2007), this amendment immobilized Bearer Shares and required the identification of Bearer Share custodians.

Vanuatu's financial sector includes five domestic licensed banks (that carry out domestic and offshore business); one credit union; eight international banks; seventy insurance companies (both life and general); and eight foreign exchange instrument dealers, money remittance dealers and bureaux de change, all of which are regulated by the Reserve Bank of Vanuatu. Since the passage of the International Banking Act of 2002, the Reserve Bank of Vanuatu regulates the offshore banking sector that includes the eight international banks and approximately 3,603 international business companies (IBCs), as well as offshore trusts and captive insurance companies. These institutions were once regulated by the Financial Services Commission. IBCs are now registered with the Vanuatu Financial Services Commission (VFSC). This change was one of many recommendations of the 2002 International Monetary Fund Module II Assessment Report (IMFR) that found Vanuatu's onshore and offshore sectors to be "noncompliant" with many international standards.

Regulatory agencies in Vanuatu have instituted stricter procedures for issuance of offshore banking licenses under the International Banking Act No. 4 of 2002, and continue to review the status of previously issued licenses. All financial institutions, both domestic and offshore, are required to report suspicious transactions and to maintain records of all transactions for six years, including the identities of the parties involved.

The Financial Transaction Reporting Act (FTRA) of 2000 established the Vanuatu Financial Intelligence Unit (VFIU) within the State Law Office. Under the Financial Transactions Reporting (Amendment) Act No. 28 of 2005, the VFIU has a role in ensuring compliance by financial services sector with financial reporting obligations. The VFIU receives suspicious transaction reports (STRs) filed by banks and distributes them to the Public Prosecutor's Office, the Reserve Bank of Vanuatu, the Vanuatu Police Force, the Vanuatu Financial Services Commission, and law enforcement agencies or supervisory bodies outside Vanuatu. The VFIU also issues guidelines to, and provides training programs for, financial institutions regarding record keeping for transactions and reporting obligations. The Act also regulates how such information can be shared with law enforcement agencies investigating financial crimes. Financial institutions within Vanuatu must establish and maintain internal procedures to combat financial crime. Every financial institution is required to keep records of all transactions. Five key pieces of information are required to be kept for every financial transaction:

the nature of the transaction, the amount of the transaction, the currency in which it was denominated, the date the transaction was conducted, and the parties to the transaction.

Although the amendments have been withdrawn from Parliament twice, the FTRA amendments were finally passed in November 2005 and enacted in late February 2006. The amendments include mandatory customer identification requirements; broaden the range of covered institutions required to file STRs to include auditors, trust companies, and company service providers; and provide safe harbor for both individuals and institutions required to file STRs. In addition to STR filings, financial institutions will now be required to file currency transaction reports (CTRs) that involve any single transaction in excess of Vanuatu currency Vatu (VT) 1,000,000, or its equivalent in a foreign currency, and wire transfers into and out of Vanuatu in excess of VT 1,000,000 (approximately U.S. $9,100). The amendments also require financial institutions to maintain internal procedures to implement reporting requirements, appoint compliance officers, establish an audit function to test their anti-money laundering and counter-terrorist financing procedures and systems, as well as provide the VFIU a copy of their internal procedures. Failure to do so will result in a fine or imprisonment for an individual, or a fine in the case of a corporate entity. The amendments supersede any inconsistent banking or other secrecy provisions and clarify the VFIU's investigative powers.

The amended FTRA defines financial institutions to include casinos licensed under the Casino Control Act No.6 of 1993, lawyers, notaries, accountants and trust and company service providers. The scope of the legislation is so broad that entities such as car dealers and various financial services that currently do not exist in Vanuatu (and are unlikely to in the future) are covered. Applications by foreigners to open casinos are subject to clearance by the Vanuatu Investment Promotion Authority (VIPA) which reviews applications and conducts a form of due diligence on the applicant before issuing a certification to the Department of Customs and Inland Revenue to issue an appropriate license. The Department of Customs and Inland Revenue receives applications from local applicants directly.

The Vanuatu Police Department and the VFIU are the primary agencies responsible for ensuring money laundering and terrorist financing offences are properly investigated in Vanuatu. The Public Prosecutions Office (PPO) is responsible for the prosecution of money laundering and terrorist financing offences. The Vanuatu Police Department has established a Transnational Crime Unit (TCU), and is responsible for investigations involving money laundering and terrorist financing offences, the identification and seizure of criminal proceeds, as well as conducting investigations in cooperation with foreign jurisdictions.

Supervision of the financial services sector is divided between three main agencies: the Reserve Bank of Vanuatu (RBV), the Vanuatu Financial Services Commission (VFSC) and the Customs and Revenue Branch of the Ministry of Finance. The RBV is responsible for supervising and regulating domestic and offshore banks. The VFSC supervises insurance providers, credit unions, charities and trust and company service providers, but is unable to issue comprehensive guidelines or to regulate the financial sectors for which it has responsibility. The Customs and Revenue Branch issues operating licenses.

The Serious Offenses (Confiscation of Proceeds) Act 1989 criminalized the laundering of proceeds from all serious crimes and provided for seizure of criminal assets and confiscation after a conviction. The Proceeds of Crime Act (2002) retained the criminalization of the laundering of proceeds from all serious crimes, criminalized the financing of terrorism, and included full asset forfeiture, restraining, monitoring, and production powers regarding assets. The Proceeds of Crime Act No. 30 of 2005 through its new Section 74A effective in November 2005, required all incoming and outgoing passengers to and from Vanuatu to declare to the Department of Customs cash exceeding one million VT in possession (approximately U.S. $9,100).

Vanuatu passed the Mutual Assistance in Criminal Matters Act in December 2002 for the purpose of facilitating the provision of international assistance in criminal matters for the taking of evidence, search and seizure proceedings, forfeiture or confiscation of property, and restraints on dealings in property that may be subject to forfeiture or seizure. The Attorney General possesses the authority to grant requests for assistance, and may require government agencies to assist in the collection of information pursuant to the request. The Extradition Act of 2002 includes money laundering within the scope of extraditable offenses.

The amended International Banking Act has now placed Vanuatu's international and offshore banks under the supervision of the Reserve Bank of Vanuatu. Section 5(5) of the Act states that if existing licensees wish to carry on international banking business after December 31, 2003, the licensee should have submitted an application to the Reserve Bank of Vanuatu under Section 6 of the Act for a license to carry on international banking business. If an unregistered licensee continued to conduct international banking business after December 31, 2003, in violation of Section 4 of the Act, the licensee is subject to a fine or imprisonment. Under Section 19 of the Act, the Reserve Bank can conduct investigations where it suspects that an unlicensed person or entity is carrying on international banking business. Since this time, three international banking businesses have had their licenses revoked.

One of the most significant requirements of the amended legislation is the banning of shell banks. As of January 1, 2004, all offshore banks registered in Vanuatu must have a physical presence in Vanuatu, and management, directors, and employees must be in residence. At the September 2003 plenary session of the Asia/Pacific Group on Money Laundering (APG), Vanuatu noted its intention to draft new legislation regarding trust companies and company service providers. The VFSC has prepared the Trust and Company Services Providers Bill and the GOV will present the bill before Parliament during the first half of 2008. The new legislation will cover disclosure of information with other regulatory authorities, capital and solvency requirements, and "fit and proper" requirements. In 2005, Vanuatu enacted Insurance Act No. 54, drafted in compliance with standards set by the International Association of Insurance Supervisors. Insurance Regulation Order No.16 of 2006 was issued on May 2006, and regulates the insurance industry, to include intermediary and agents roles.

International Business Companies (IBC) traditionally could be registered using bearer shares, shielding the identity and assets of beneficial owners of these entities. Secrecy provisions protected all information regarding IBCs and provided penal sanctions for unauthorized disclosure of information. These secrecy provisions, along with the ease and low cost of incorporation, made IBCs ideal mechanisms for money laundering and other financial crimes. Section 125 of the International Companies Act No. 31 of 1992 (ICA), provided a strict secrecy provision for information disclosure related to shareholders, beneficial ownership, and the management and affairs of IBCs registered in Vanuatu. This provision, in the past, has been used by the industry to decline requests made by the VFIU for information. However, section 17(3) of the new amended FTRA clearly states that the new secrecy-overriding provision in the FTRA overrides section 125 of the ICA. Moreover, the International Companies (Amendment) Act No. 45 of 2006 (ICA) revised the regime governing IBC operations. Ministerial Order No. 15 of 2007 created a Guideline of Custody of Bearer Shares, which immobilized Bearer Shares and requires the identification of Bearer Share custodians.

In November 2005, Vanuatu passed the Counter-Terrorism and Transnational Organized Crime Act (CTTOCA) No. 29 of 2005. The CTTOCA was brought into force on 24 February 2006. The aim of the Act is to implement UN Security Council Resolutions and Conventions dealing with terrorism and transnational organized crime, to prevent terrorists from operating in Vanuatu or receiving assistance through financial resources available to support the activities of terrorist organizations, and to criminalize human trafficking and smuggling. Terrorist financing is criminalized under section 6 of the CTTOCA. Section 7 of the CTTOCA makes it an offence to "directly or indirectly, knowingly make available property or financial or other related services to, or for the benefit of, a terrorist group." The

penalty upon conviction is a term of imprisonment of not more than 25 years or a fine of not more than VT 125 million (U.S. $1,000,000), or both. Section 8 criminalizes dealing with terrorist property. The penalty upon conviction is a term of imprisonment of not more than 20 years or a fine of not more than VT 100 million (U.S. $876,500), or both. There were no terrorist financing or terrorism-related prosecutions or investigations in 2006.

In addition to its membership the Asia Pacific Group on Money Laundering, Vanuatu is a member of the Offshore Group of Banking Supervisors, the Commonwealth Secretariat, and the Pacific Island Forum. Its Financial Intelligence Unit became a member of the Egmont Group in June 2002. The GOV acceded to the UN International Convention for the Suppression of the Financing of Terrorism in October 2005, and acceded to both the UN Convention against Transnational Organized Crime and the 1988 UN Drug Convention in January 2006. The GOV has not yet signed the UN Convention against Corruption. The VFIU has a memorandum of understanding with Australia.

In March 2006, the APG conducted a mutual evaluation of Vanuatu, the results of which were reported at the APG plenary meeting in November 2006. The APG evaluation team found that Vanuatu had improved its anti-money laundering and counter-terrorist financing regime since its first evaluation in 2000 by criminalizing terrorist financing, requiring a wider range of entities to report to the VFIU and enhancing supervisory oversight of obligated entities. However, some deficiencies remain: the GOV has not taken a risk-based approach to combating money laundering and terrorist financing; a person who commits a predicate offense for money laundering cannot also be charged with money laundering; and current law does not require the names and addresses of directors and shareholders to be provided upon registration of an IBC.

The Government of Vanuatu should implement all the provisions of its Proceeds of Crime Act and enact all additional legislation that is necessary to bring both its onshore and offshore financial sectors into compliance with international standards. The GOV should also establish a viable asset forfeiture regime and circulate the updated UNSCR 1267 Sanctions Committee updated list of designated terrorist entities.

Venezuela

Venezuela is one of the principal drug-transit countries in the Western Hemisphere, with an estimated 250 metric tons of cocaine passing through the nation annually. Venezuela's proximity to drug producing countries, weaknesses in its anti-money laundering regime, refusal to cooperate with the United States on counternarcotics activities, and rampant corruption throughout the law enforcement, judicial, banking, and banking regulatory sectors continue to make Venezuela vulnerable to money laundering. The main sources of money laundering are from proceeds generated by cocaine and heroin trafficking organizations and the embezzlement of dollars from the petroleum industry. Trade-based money laundering, such as the Black Market Peso Exchange, through which money launderers furnish narcotics-generated dollars in the United States to commercial smugglers, travel agents, investors, and others in exchange for Colombian pesos, remains a prominent method for laundering narcotics proceeds. It is reported that many of these black market traders ship their wares through Venezuela's Margarita Island free trade zone. Reportedly, some money is also laundered through the real estate market in Margarita Island.

Venezuela is not a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking sector, which consists of 49 banks, primarily serves the domestic market. All but one of these banks belong to the Venezuelan Association of Banks. Membership is voluntary and meetings are held monthly.

Money laundering in Venezuela is criminalized under the 2005 Organic Law against Organized Crime. Under the Organic Law against Organized Crime, money laundering is an autonomous offense,

punishable by a sentence of eight to twelve years in prison. Those who cannot establish the legitimacy of possessed or transferred funds, or are aware of the illegitimate origins of those funds, can be charged with money laundering, without any connection to drug trafficking. In addition to establishing money laundering as an autonomous predicate offense, the Organic Law against Organized Crime broadens asset forfeiture and sharing provisions, adds conspiracy as a criminal offense, strengthens due diligence requirements, and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques, such as the use of undercover agents. This law, coupled with the Law Against the Trafficking and Consumption of Narcotics and Psychotropic Substances, effectively brings Venezuela's Penal Code in line with the 1988 UN Drug Convention.

In spite of the advances made with the passage of the Organic Law against Organized Crime in 2005, major gaps remain. Two years after promulgation, not a single case has been tried under the new law. Many, if not most, judicial and law enforcement officials remain ignorant of the Law against Organized Crime and its specific provisions, and the financial intelligence unit (FIU) does not have the necessary autonomy to operate effectively. Widespread corruption within the judicial and law enforcement sectors also undermines the effectiveness of the law as a tool to combat the growing problem of money laundering. Finally, there is little evidence that the Government of Venezuela (GOV) has the will to effectively enforce the legislation it has promulgated.

Under the Organic Law against Organized Crime and Resolution 333-97 of the Superintendent of Banks and Other Financial Institutions (SBIF), anti-money laundering controls have been implemented requiring strict customer identification requirements and the reporting of both currency transactions over a designated threshold and suspicious transactions. These controls apply to all banks (commercial, investment, mortgage, and private), insurance and reinsurance companies, savings and loan institutions, financial rental agencies, currency exchange houses, money remitters, money market funds, capitalization companies, frontier foreign currency dealers, casinos, real estate agents, construction companies, car dealerships, hotels and the tourism industry, travel agents, and dealers in precious metals and stones. These entities are required to file suspicious and cash transaction reports with Venezuela's FIU, the Unidad Nacional de Inteligencia Financiera (UNIF). Financial institutions are required to maintain records for a period of five years.

The UNIF was created under the SBIF in July 1997 and began operating in June 1998. Under the original draft of the Organic Law against Organized Crime, the UNIF would have become an autonomous entity with investigative powers, independent of the SBIF, but the relevant clauses were removed just prior to the law's passage. The UNIF has a staff of approximately 31 and has undergone multiple bureaucratic changes, with five different directors presiding over the UNIF since 2004. The SBIF and the UNIF are viewed dubiously within the financial sector, with credible reports indicating that both are used by the government to investigate political opponents.

The UNIF receives reports on currency transactions (CTRs) exceeding approximately U.S. $10,000 and suspicious transaction reports (STRs) from institutions regulated by the SBIF: the Office of the Insurance Examiner, the National Securities and Exchange Commission, the Bureau of Registration and Notaries, the Central Bank of Venezuela, the Bank Deposits and Protection Guarantee Fund, and other nonregulated entities now included under the Organic Law against Organized Crime. The Venezuelan Association of Currency Exchange Houses (AVCC), which counts all but one of the country's money exchange companies among its membership, voluntarily complies with the same reporting standards as those required of banks. Some institutions regulated by the SBIF, such as tax collection entities and public service payroll agencies, are exempt from the reporting requirement. The SBIF also allows certain customers of financial institutions—those who demonstrate "habitual behavior" in the types and amounts of transactions they conduct—to be excluded from currency transaction reports filed with the UNIF. SBIF Circular 3759 of 2003 requires financial institutions that fall under the supervision of the SBIF to report suspicious activities related to terrorist financing; however, terrorist financing is not a crime in Venezuela.

In addition to STRs and CTRs, the UNIF also receives reports on the domestic transfer of foreign currency exceeding U.S. $10,000, the sale and purchase of foreign currency exceeding U.S. $10,000, and summaries of cash transactions that exceed approximately U.S. $2,100. The UNIF does not, however, receive reports on the transportation of currency or monetary instruments into or out of Venezuela. A system has been developed for electronic receipt of CTRs, but STRs must be filed in paper format. Obligated entities are forbidden to reveal reports filed with the UNIF or suspend accounts during an investigation without official approval, and are also subject to sanctions for failure to file reports with the UNIF.

The UNIF analyzes STRs and other reports, and refers those deemed appropriate for further investigation to the Public Ministry (the Office of the Attorney General). No statistics are available on the number of STRs or CTRs received in 2007. According to the UNIF, it forwards approximately 30 percent of the STRs it receives to the Attorney General's Office. The Attorney General's office subsequently opens and oversees the criminal investigation. The Venezuelan constitution guarantees the right to bank privacy and confidentiality, but in cases under investigation by the UNIF, the SBIF, or the Attorney General's office, a judge can waive these rights, making Venezuela one of least restrictive countries in Latin America from an investigatorial standpoint.

Prior to the passage of the 2005 Organic Law against Organized Crime, there was no special prosecutorial unit for the prosecution of money laundering cases under the Attorney General's office, which is the only entity legally capable of initiating money laundering investigations. As a result of the limited resources and expertise of the drug prosecutors who previously handled money laundering investigations, there have only been three money laundering convictions in Venezuela since 1993, and all of them were narcotics-related. The Organic Law against Organized Crime calls for a new unit to be established, the General Commission against Organized Crime, with specialized technical expertise in the analysis and investigation of money laundering and other financial crimes. This commission has not been established to date. The Organic Law against Organized Crime also expanded Venezuela's mechanisms for freezing assets tied to illicit activities. A prosecutor may now solicit judicial permission to freeze or block accounts in the investigation of any crime included under the law. However, to date there have been no significant seizures of assets or successful money laundering prosecutions as a result of the law's passage.

The 2005 Organic Law against Organized Crime counts terrorism as a crime against public order and defines some terrorist activities. The law also establishes punishments for terrorism of up to 20 years in prison. However, the Organic Law against Organized Crime does not establish terrorist financing as a separate crime, nor does it provide adequate mechanisms for freezing terrorist assets.

The UNIF has been a member of the Egmont Group since 1999 and has signed bilateral information exchange agreements with counterparts worldwide. However, if the GOV does not criminalize the financing of terrorism, the UNIF faces suspension from the Egmont Group in June 2008. Due to the unauthorized disclosure of information provided to the UNIF by the Financial Crimes Enforcement Network (FinCEN), the United States FIU, FinCEN suspended information exchange with the UNIF in January 2007. FinCEN and the UNIF are currently negotiating a Memorandum of Understanding (MOU) that outlines the parameters for future information exchange between the two FIUs. Once signed, FinCEN will begin sharing financial intelligence with the UNIF again.

Venezuela participates in the Organization of American States Inter-American Commission on Drug Abuse Control (OAS/CICAD) Money Laundering Experts Working Group and is a member of the Caribbean Financial Action Task Force (CFATF). The GOV is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the OAS Inter-American Convention against Terrorism. The GOV has signed, but not yet ratified, the UN Convention against Corruption. The GOV continues to share money laundering information with U.S. law enforcement

authorities under the 1990 Agreement Regarding Cooperation in the Prevention and Control of Money Laundering Arising from Illicit Trafficking in Narcotics Drugs and Psychotropic Substances, which entered into force on January 1, 1991. Venezuela and the United States signed a Mutual Legal Assistance Treaty (MLAT) in 1997, but it has not entered into force.

The Government of Venezuela took no significant steps to expand its anti-money laundering regime in 2007. There were no prosecutions or convictions for money laundering in 2007, and this is unlikely to change in 2008. The 2005 passage of the Organic Law against Organized Crime was a step towards strengthening the GOV's abilities to fight money laundering. However, Venezuela needs to enforce the law by creating procedures to expedite asset freezing, establishing an autonomous financial investigative unit, and ensuring that law enforcement and prosecutors have the necessary expertise and resources to successfully investigate and prosecute money laundering cases. The GOV should also criminalize the financing of terrorism and establish procedures for freezing terrorist assets. The UNIF should sign the MOU with FinCEN that will allow it to resume sharing financial intelligence with the United States, and take the necessary steps to ensure that information exchanged with other financial intelligence units is subject to the appropriate safeguards mandated by the Egmont Group.

Vietnam

Vietnam is not an important regional financial center, but is the site of significant money laundering activities. Vietnam remains a largely cash-based economy and both U.S. dollars and gold are widely used as a store of value and means of exchange. Remittances are a large source of foreign exchange, exceeding annual disbursements of development assistance and rivaling foreign direct investment in size. Remittances from the proceeds of narcotics in Canada and the United States are also a source of money laundering as are proceeds attributed to Vietnam's role as a transit country for narcotics.

The Vietnamese banking sector is in transition from a state-owned to a partially privatized industry. At present, approximately 80 percent of the assets of the banking system are held by state-owned commercial banks that allocate much of the available credit to state-owned enterprises. Almost all trade and investment receipts and expenditures are processed by the banking system, but neither trade nor investment transactions are monitored effectively. As a result, the banking system could be used for money laundering either through over or under invoicing exports or imports or through phony investment transactions. Official inward remittances in the first six months of 2007 were estimated to be approximately $2.8 billion. These amounts are generally transmitted by wire services and while officially recorded, there is no reliable information on either the source or the recipients of these funds. Financial industry experts believe that actual remittances may be double the official figures. There is evidence that large amounts of cash are hand carried into Vietnam, which is legal as long as the funds are declared. The Government of Vietnam (GOV) does not require any explanation of the source or intended use of funds brought into the country in this way. In 2006, Vietnam Airlines was implicated in a U.S. $93 million money laundering scheme uncovered by the Australian Crime Commission. Vietnamese organized crime syndicates operating in Australia and involved in money transfer businesses used the airline to help smuggle money to Vietnam.

A form of informal value transfer service, which often operates through the use of domestic jewelry and gold shops, is widely used to transfer funds within Vietnam. Money or value transmitters are defined as financial institutions by Decree No. 74 and are therefore subject to its AML-related provisions; however, the informal transmitters have not been brought under regulation or supervision.

The U.S. Drug Enforcement Agency (DEA) is engaged in a number of investigations targeting significant ecstasy and marijuana trafficking organizations, composed primarily of Vietnamese legal permanent residents in the United States and Vietnamese landed immigrants in Canada as well as naturalized U.S. and Canadian citizens. These drug trafficking networks are capable of laundering tens of millions of dollars per month back to Vietnam, exploiting U.S. financial institutions to wire or

transfer money to Vietnamese bank and remittance accounts, as well as engaging in the smuggling of bulk amounts of U.S. currency and gold into Vietnam. The drug investigations have also identified multiple United States-based money remittances businesses that have remitted over $100 million annually to Vietnam. It is suspected that the vast amount of that money is derived from criminal activity. Law enforcement agencies in Australia and the United Kingdom have also tracked large transfers of drug profits back to Vietnam.

Article 251 of the Amended Penal Code criminalizes money laundering. The Counter-Narcotics Law, which took effect June 1, 2001, makes two narrow references to money laundering in relation to drug offenses: it prohibits the "legalizing" (i.e., laundering) of monies and/or property acquired by committing drug offenses (article 3.5); and, it gives the Ministry of Public Security's specialized counter narcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. The Penal Code governs money laundering related offenses and no money laundering cases have yet been prosecuted. Article 251 does not meet current international standards and amongst other weaknesses, the law requires a very high burden of proof (essentially, a confession) to pursue AML allegations, so prosecutions are nonexistent and international cooperation is extremely difficult. The GOV has plans to revise Article 251 and present the draft to Parliament in 2008.

In June 2005, GOV issued Decree 74/2005/ND-CP on Prevention and Combating of Money Laundering. The Decree covers acts committed by individuals or organizations to legitimize money or property acquired from criminal activities. The Decree applies to banks and nonbank financial institutions. The State Bank of Vietnam (SBV) and the Ministry of Public Security (MPS) take primary responsibility for preventing and combating money laundering. Neither the Penal Code, nor the decree covers counterterrorist finance. Reportedly, the Prime Minister has discussed the possibility of dealing with terrorist financing through issuance of a government directive. However, such a directive would have no penal force.

The SBV supervises and examines financial institutions for compliance with anti-money laundering/counter terrorist financing regulations. Financial institutions are responsible for knowing and recording the identity of their customers. They are required to report cash transactions conducted in one day with aggregate value of Vietnam Dong (VND) 200 million (approximately U.S. $13,000) or more, or equivalent amount in foreign currency or gold. The threshold for savings transactions is VND 500 million (approximately U.S. $31,000). Furthermore, financial institutions are required to report all suspicious transactions. Banks are also required to maintain records for seven years or more. Banks are responsible for keeping information on their customers secret, but they are required to provide necessary information to law enforcement agencies for investigation purposes.

Foreign currency (including notes, coins and traveler's checks) in excess of U.S. $7,000 and gold of more than 300 grams must be declared at customs upon arrival and departure. There is no limitation on either the export or import of U.S. dollars or other foreign currency provided that all currency in excess of U.S. $7,000 (or its equivalent in other foreign currencies) is declared upon arrival and departure, and supported by appropriate documentation. If excess cash is not declared, it is confiscated at the port of entry/exit and the passenger may be fined.

The 2005 Decree on Prevention and Combating of Money Laundering provides for provisional measures to be applied to prevent and combat money laundering. Those measures include 1) suspending transactions; 2) blocking accounts; 3) sealing or seizing property; 4) seizing violators of the law; and, 5) taking other preventive measures allowed under the law.

The 2005 Decree also provides for the establishment of an Anti-Money Laundering Information Center (AMLIC) under the State Bank of Vietnam (SBV). Similar to a Financial Intelligence Unit (FIU), the AMLIC will function as the sole body to receive and process financial information. It will have the right to request concerned agencies to provide information and records for suspected

transactions. The AMLIC was formally established and began operations since February 2006. The Director of the center is appointed by the Governor of the SBV and reports directly to the Governor on anti-money laundering issues. SBV acts as the sole agency responsible for negotiating, concluding and implementing international treaties and agreements on exchange of information on transactions related to money laundering.

The AMLIC staff is currently split between two office locations with only two computers for its staff members. The Center has 13 full time staff members, and is working to hire more. The AMLIC has established liaison with ministries and agencies such as Ministries of Justice, Public Security, Finance, Foreign Affairs, the Supreme People's Procuracy, the Supreme People's Court, and the Banking Association. Since the Center became operational, it has received 20 suspicious transaction reports and has referred six cases to MPS for investigation. The AMLIC has virtually no IT capacity and a very low level of analytical ability.

The MPS is responsible for investigating money laundering related offences. There is no information from MPS on investigations, arrests, and prosecutions for money laundering or terrorist financing, but the SBV reports that there have been no arrests or prosecutions for money laundering since January 1, 2007. MPS is responsible for negotiating and concluding international treaties on judicial assistance, cooperation and extradition in the prevention and combat of money laundering related offenses. MPS signed a nonbinding Memorandum of Understanding with DEA in 2006 to strengthen law enforcement cooperation in combating transnational drug-related crimes, including money laundering, but claims it is unable to provide such information due to constraints within the Vietnamese legal system. In May 2007, Vietnam became a member of the Asia/Pacific Group on Money Laundering (APG). As a member of APG, Vietnam has committed to a comprehensive review of its AML/CTF regime in 2008.

Vietnam is a party to the 1999 UN International Convention for the Suppression of the Financing of Terrorism. Reportedly, Vietnam plans to draft separate legislation governing counter-terrorist financing, though it will not set a specific time frame for this drafting. Currently SBV circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. No related assets have been identified.

Vietnam is a party to the 1988 UN Drug Convention. Under existing Vietnamese legislation, there are provisions for seizing assets linked to drug trafficking. In the course of its drug investigations, MPS has seized vehicles, property and cash, though the seizures are usually directly linked to drug crimes. Final confiscation requires a court finding. Reportedly, MPS can notify a bank that an account is "seized" and that is sufficient to have the account frozen.

Vietnam has signed but not ratified either the UN Convention against Transnational Organized Crime or the UN Convention against Corruption. Vietnam is ranked 123 out of 179 countries in Transparency International's 2007 Corruption Perception Index.

The Government of Vietnam should promulgate all necessary regulations to implement fully the 2005 decree on the Prevention and Combating of Money Laundering. Vietnam should also pass legislation to make terrorist financing a criminal offense as well as including provisions governing the prevention and suppression of terrorist financing. Vietnam should ratify the UN Conventions against Transnational Organized Crime and Corruption. Vietnamese law enforcement authorities should investigate money laundering, trade fraud, alternative remittance systems, and other financial crimes in Vietnam's shadow economy. The AMLIC needs to be equipped with an electronic information reporting system. Vietnam should take additional steps to establish an anti-money laundering/counter-terrorist financing regime that comports with international standards.

Yemen

The Yemeni financial system is not well developed and the extent of money laundering is not known. Yemen is not considered an important regional financial center; nor is it considered an offshore financial center. Although financial institutions are technically subject to limited monitoring by the Central Bank of Yemen, in practice, alternative remittance systems, such as hawala, are not subject to scrutiny and are vulnerable to money laundering and other financial abuses. The banking sector is relatively small with 17 commercial banks, including four Islamic banks. All banks are under Central Bank supervision. Local banks account for approximately 62 percent of the total banking activities, while foreign banks cover the other 38 percent.

Yemen has a large underground economy. The smuggling of trade goods and contraband is profitable. The use of khat is common in Yemen and there have been a number of investigations over the years of khat being smuggled from Yemen and East Africa into the United States with profits laundered and repatriated via hawala networks. Smuggling and piracy are rampant along Yemen's sea border with Oman, across the Red Sea from the Horn of Africa, and along the land border with Saudi Arabia.

In April 2003 Yemen's Parliament passed anti-money laundering (AML) legislation (Law 35). The legislation criminalizes money laundering for a wide range of crimes, including narcotics offenses, kidnapping, embezzlement, bribery, fraud, tax evasion, illegal arms trading, and monetary theft, and imposes penalties of three to five years of imprisonment. Yemen has no specific legislation relating to terrorist financing, although terrorism is covered in various pieces of legislation that treat terrorism and terrorist financing as serious crimes. In November 2007 the Cabinet sent a draft counter-terrorist financing law to Parliament.

Law 35 requires banks, financial institutions, and precious commodity dealers to verify the identity of individuals and entities that open accounts (or in the case of the dealers for those who execute a commercial transaction), to keep records of transactions for up to ten years, and to report suspicious transactions (STRs). In addition, the law requires that reports be submitted to the Anti-Money Laundering Information Unit (AMLIU), an information-gathering unit within the Central Bank. This unit acts as the financial intelligence unit (FIU), which in turn reports to the Anti-Money Laundering Committee (AMLC), within the Central Bank.

The AMLC is composed of representatives from the Ministries of Finance, Foreign Affairs, Justice, Interior, and Industry and Trade, the Central Accounting Office, the General Union of Chambers of Commerce and Industry, the Central Bank of Yemen, and the Association of Banks. The AMLC is authorized to issue regulations and guidelines and provide training workshops related to combating money laundering efforts.

There are approximately 448 registered money exchange businesses in Yemen, which serve primarily as currency exchangers in addition to performing funds transfer services. Money transfer businesses are required to register with Central Bank for one permit, but can open offices at multiple locations. Fund transfers that exceed the equivalent of $10,000 require permission from the Central Bank. The Central Bank has not begun to examine the money exchange business for AML compliance.

The AMLIU is understaffed with only a few employees, although it also uses the services of field inspectors from the Central Bank's Banking Supervision Department. The AMLIU has no database and is not networked internally or to the rest of the Central Bank. The Central Bank provides training to other members of the government to assist in elements of anti-money laundering enforcement, but the lack of capacity hampers any attempts by the AMLIU to control illicit activity in the formal financial sector.

Law 35 also grants the AMLC the ability to exchange information with foreign entities that have signed a letter of understanding with Yemen. The head of the AMLC is empowered by law to ask local judicial authorities to enforce foreign court verdicts based on reciprocity.

Prior to passage of the AML law, the Central Bank issued Circular 22008 in April 2002, instructing financial institutions to positively identify the place of residence of all persons and businesses that establish relationships with them. The circular also requires that banks verify the identity of persons or entities that wish to transfer more than $10,000, when they have no accounts at the banks in question. The same provision applies to beneficiaries of such transfers. The circular also prohibits inbound and out-bound money transfer of more than $10,000 cash without prior permission from the Central Bank, although this requirement is not strictly enforced. Banks must also report suspicious transactions to the AMLIU. The circular is distributed to the banks along with a copy of the Basel Committee's "Customer Due Diligence for Banks," concerning "know your customer" procedures and "Core Principles for Effective Banking Supervision". In 2005, two STRs were filed with the AMLIU and in 2006, three STRs were filed. The number of STRs filed in 2007 with the AMLIU is not available. However, in 2007 the AMLIU forwarded one suspicious case to the Office of the Public Prosecutor for suspected money laundering. There have not been any money laundering prosecutions or convictions in Yemen.

At present, Yemen has no cross-border cash declarations or disclosure requirements. However, according to the Customs Authority, inspectors will fill out a declaration form after money has been discovered leaving or entering the country at the border.

Yemen has one free trade zone (FTZ) in Aden. Identification requirements are enforced. For example, truckers must file the necessary paperwork in relevant trucking company offices and must wear ID badges. FTZ employees must undergo background checks by police, the Customs Authority and employers. There is no evidence that the FTZ is being used for trade-based money laundering or terrorist financing schemes.

In September 2003, the Central Bank responded to the UNSCR 1267 Sanctions Committee's consolidated list, the Specially Designated Global Terrorists by the United States pursuant to E.O. 13224, and Yemen's Council of Ministers' directives, by issuing circulars 75304 and 75305 to all banks operating in Yemen. Circulars 75304 and 75305 directed banks to freeze the accounts of 144 persons, companies, and organizations, and to report any findings to the Central Bank. As a result, one account was immediately frozen. In 2006, the CBY began issuing a circular every three months containing an updated list of persons and entities belonging to Al-Qaida and the Taliban. However, since the February 2004 addition of Yemeni Sheikh Abdul Majid Zindani to the UNSCR 1267 Sanctions Committee's consolidated list, the Yemeni government has made no known attempt to enforce the sanctions and freeze his assets. There is no information on whether Yemeni authorities have identified, frozen, seized, or forfeited other assets related to terrorist financing.

The Government of Yemen (GOY) has a forfeiture system in place. A judge must order the forfeiture for the items involved in or proceeds from the crime for which the defendant was convicted. Forfeiture is available for all crimes and extends to funds and property. Authorities deposit forfeited funds into the general treasury unless the funds are the proceeds from a drug offense, in which case the proceeds go to law enforcement authorities, who can use the proceeds to buy vehicles or other equipment. If the court orders a defendant to forfeit property, the judge issues an order to auction off the property to the public, with the funds from the auction going into the general treasury. In some instances, the courts can order real property, such as a dwelling, to be closed for one year before the owner may use it again. Yemen has not yet forfeited any real property.

In 2001 the government enacted a law governing charitable organizations. This law entrusts the Ministry of Social Affairs and Labor (MOSAL) with overseeing their activities. The law also imposes penalties of fines and/or imprisonment on any society or its members convicted of carrying out activities or spending funds for other than the stated purpose for which the society in question was established. Central Bank Circular No. 33989 of June 2002 and Circular No. 91737 of November 2004, ordered banks to enhance controls regulating opening and managing charities' accounts. This

was in addition to keeping these accounts under continuous supervision in coordination with the MOSAL.

The Central Bank is active in educating the public and the financial sector, including money services businesses and money laundering reporting officers, about the proper ways and means of detecting and reporting suspicious financial transactions.

Yemen is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). There is no information available on Yemen's mutual evaluation by MENAFATF. Yemen is a party to the 1988 UN Drug Convention; it has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. The GOY is a party to the UN Convention against Corruption. Yemen is listed 131 out of 179 countries in Transparency International's 2007 Corruption Perception Index.

The Government of Yemen should continue to develop an anti-money laundering regime that adheres to international standards, including the FATF 40 Recommendations and Nine Special Recommendations on terrorist financing. Banks and nonbank financial institutions should enhance their capacity to detect and report suspicious financial transactions to the FIU. The AMLIU needs substantial improvement of its analytical capabilities. Yemen must investigate the abuse of alternative remittance systems such as hawala networks with regard to money laundering and terrorist financing. Law enforcement and customs authorities should also examine trade-based money laundering and customs fraud. Yemen should enact specific legislation with respect to terrorist financing and forfeiture of the assets of those suspected of terrorism. Yemen should enforce sanctions and freeze the assets of Sheikh Abdul Majid Zindani, who was added to the UN 1267 Sanctions Committee's consolidated list in February 2004. Yemen should ratify the UN Convention against Transnational Organized Crime and should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Zimbabwe

Zimbabwe is not a regional financial center, but as economic conditions continue to deteriorate for the eighth straight year, money laundering has become a growing problem. This is a result of official corruption and impunity; a flourishing parallel exchange market; rampant smuggling of precious minerals; widespread evasion of exchange controls by legitimate businesses; and company ownership through nominees. Deficiencies in the Government of Zimbabwe's (GOZ) regulatory and enforcement framework contribute to Zimbabwe's potential as a money laundering destination. These deficiencies include: an understaffed bank supervisory authority; a lack of trained regulators and lack of investigators to investigate and enforce violations and financial crime; financial institutions determined to bypass the regulatory framework; limited asset seizure authority; a laissez-faire attitude toward compliance with the law on the part of elements of the business community; ready acceptance of the U.S. dollar in transactions; and significant gold and diamond exports and illegal gold and diamond trading.

During 2007, the government took some steps to prevent money laundering and illegal smuggling activities, including the installation of a new electronic surveillance system to monitor all transactions in the banking system and launch of an operation targeted at illegal precious minerals mining and trading.

In December 2003, the GOZ submitted the Anti-Money Laundering and Proceeds of Crime Act to Parliament, which enacted the legislation. This bill criminalizes money laundering and implements a six-year record keeping requirement. In 2004, the GOZ adopted more expansive legislation in the Bank Use Promotion and Suppression of Money Laundering Act (the Act) that extends the anti-money laundering law to all serious offenses. The Act mandates a prison sentence of up to fifteen years for a

conviction. It also criminalizes terrorist financing and authorizes the tracking and seizure of assets. The Act has reportedly raised human rights concerns due to the GOZ's history of selective use of the legal system against its opponents, but its use to date has not been associated with any reported due process abuses or provoked any serious public opposition. The Exchange Control Order, enacted in 1996, obligates banks to require individuals who deposit foreign currency into a foreign currency account to submit a written disclosure of sources of the funds.

The Reserve Bank of Zimbabwe (RBZ) is the lead agency for prosecuting money laundering offenses. In May 2006, the RBZ issued new Anti-Money Laundering Guidelines that outline and reinforce requirements established in the Act for financial institutions and designated nonfinancial businesses and professions. These binding requirements make provisions regarding politically exposed persons and include the obligation to gather and make available to regulators more personal data on these high-profile clients. Financial institutions must now keep records of accounts and transactions for at least ten years, and report any suspicious transactions to the financial intelligence unit (FIU). The Act also criminalizes tipping off. Failure to report suspected money laundering activities or violating rules on properly maintaining customer data carries a possible fine of Zimbabwe $3 million (approximately U.S. $100 at the official exchange rate or less than U.S. $2 at the parallel market rate) for each day during which a financial institution is in default of compliance. During the year, the RBZ, in cooperation with police, launched Operation Chikorokoza Chapera ("No Illegal Panning") to crack down on rampant illegal gold mining and smuggling. The RBZ reported that it had secured nearly 100 convictions from 221 investigations to date. In November, the government also enacted stiffer penalties for dealing in illegal minerals under the Precious Stones Trade Amendment Bill. Those convicted of illegally possessing or trading in precious minerals now face a penalty of a minimum of five years imprisonment and a fine of up to Zimbabwe $50 million (approximately U.S. $1,666 at the official exchange rate or less than $33 at the parallel market rate).

The 2004 Act provides for the establishment of The Financial Intelligence Inspectorate and Evaluation Unit (FIIE), Zimbabwe's financial intelligence unit (FIU). The FIIE is housed within the RBZ. The FIIE receives suspicious transaction reports (STRs), issues guidelines, such as the Anti-Money Laundering Guidelines issued in May 2006, and enforces compliance with procedures and reporting standards for obligated entities.

In June 2007, the RBZ installed an electronic surveillance system to track all financial transactions in the banking system. The FIIE reported that after the launch of the new system, there was a noticeable improvement in self-regulation at banks as demonstrated by an increase in the number of STRs received. During the year, the RBZ continued to tightly control limits on daily cash withdrawals for individuals and companies, ostensibly in an effort to curtail money laundering but more likely to inhibit private sector parallel foreign exchange activities. In November 2007, after a sharp devaluation, the Zimbabwe dollar was still trading on the parallel market at a premium of approximately 4,900 percent above the official exchange rate. When requested, the local banking community has cooperated with the GOZ in the enforcement of asset tracking laws. However, increasingly burdensome GOZ regulations and the resulting hostile business climate have led to growing circumvention of the law by otherwise legitimate businesses. In May, the RBZ cancelled the foreign currency exchange license of NMB Bank, the first indigenous bank in Zimbabwe, after a senior NMB official allegedly externalized more than U.S. $4.5 million in embezzled funds and fled the country. RBZ cited a breach of Exchange Control Regulations and a failure to report suspicious transactions as required under the Act.

The GOZ continued to arrest prominent Zimbabweans for activities that it calls "financial crimes." Prosecutions for such crimes, however, have reportedly been selective and politically motivated. The government often targets persons who have either fallen out of favor with the ruling party, or individuals without high-level political backing. Most financial crimes involved violations of currency restrictions that criminalize the externalization of foreign exchange. In light of the inability of the vast

majority of businesses to access foreign exchange from the RBZ, most companies privately admit to externalizing their foreign exchange earnings or to accessing foreign currency on the parallel market. Moreover, the GOZ itself, through the RBZ, has been a major purchaser of foreign currency on the parallel market.

In August 2006, the GOZ implemented a currency re-denomination program that slashed three zeros from Zimbabwe's currency (so that Z$100,000 became Z$100). The purpose of the campaign was to ease bookkeeping and the handling of cash transactions under runaway inflation and at the same time assert greater GOZ control over the financial sector. Although the campaign had nothing to do with cracking down on money laundering, when the holder of cash could not prove a legitimate source of funds, the cash was deposited into zero-interest "anti-money laundering coupons," and the case was referred to the RBZ's Suppression of Money Laundering Unit for further investigation. The government claimed that more than 2,000 persons were arrested for "money laundering" in this period and charged under the Exchange Control Act. The government has not provided any additional information about the status or resolution of any of these cases.

The 2001 Serious Offenses (Confiscation of Profits) Act establishes a protocol for asset forfeiture. The Attorney General may request confiscation of illicit assets. The Attorney General must apply to the court that has rendered the conviction within six months of the conviction date. The court can then issue a forfeiture order against any property. Despite the early date of this law compared to the money laundering legislation that followed, this law does define and incorporate money laundering among the bases for the GOZ to confiscate assets.

With the country in steep economic decline and increasingly isolated, Zimbabwe's laws and regulations remained ineffective in combating money laundering. The government's anti-money laundering efforts throughout the year appeared to be directed more at securing the government's own access to foreign currency, targeting opponents, and tightening control over precious minerals than to ensuring compliance. Despite having the legal framework in place to combat money laundering, the sharp contraction of the economy, growing vulnerability of the population, and decline of judicial independence raise concerns about the capacity and integrity of Zimbabwean law enforcement. Transparency International ranks the Government of Zimbabwe at 150 of 179 countries on its 2007 Corruption Perceptions Index. The banking community and the RBZ have cooperated with the United States in global efforts to identify individuals and organizations associated with terrorist financing.

Zimbabwe is a party to the 1988 UN Drug Convention. In March 2007, the Zimbabwe Parliament ratified the UN Convention against Corruption. However, Zimbabwe has yet to ratify the UN Convention against Transnational Organized Crime and the African Union Convention against Corruption, and has yet to sign the UN International Convention for the Suppression of the Financing of Terrorism. Zimbabwe joined the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) in 2003 and assumed the Presidency for ESAAMLG for the 2006/2007 administrative year. Zimbabwe experienced the first completed mutual evaluation undertaken by ESAAMLG. The report was accepted at the plenary and Council of Ministers meeting in August 2007.

The GOZ leadership should work to develop and maintain transparency, prevent corruption, and to subscribe to practices ensuring the rule of law. The GOZ must also work toward reducing the rate of inflation, halting the economic collapse, and rebuilding the economy to restore confidence in the currency. The GOZ can illustrate its commitment to combating money laundering and terrorist financing by using its legislation for the purposes for which it was designed, instead of using it to persecute opponents of the regime and nongovernmental organizations with which it opposes. Once these basic prerequisites are met, the GOZ should endeavor to develop and implement an anti-money laundering/counter-terrorist financing regime that comports with international standards. The GOZ should also become a party to the UN International Convention for the Suppression of the Financing

of Terrorism, and should ratify the African Union Convention against Corruption and the UN Convention against Transnational Organized Crime.