Departamento de América del Norte

Bureau Of International Narcotics And Law Enforcement Affairs
2009 International Narcotics Control Strategy Report (INCSR)
Report
February 27, 2009

Afghanistan

Afghanistan is not a regional financial or banking center, and is not considered an offshore financial center. However, its formal financial system is expanding rapidly while its traditional informal financial system remains significant in reach and scale. Afghanistan remains a major drug trafficking and drug producing country and the illicit narcotics trade is the primary source of laundered funds. Afghanistan enacted anti-money laundering and terrorist financing laws through presidential decree in October 2005. These laws are currently pending approval in parliament. While efforts continue to strengthen police and customs forces, there remain few resources, limited capacity, little expertise and insufficient political will to seriously 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 also a significant problem. Afghanistan ranks 176 out of 180 countries in Transparency International's 2008 Corruption Perception Index.

According to United Nations Office of Drug Control (UNODC) statistics, opium poppy cultivation declined 19 percent in 2008. Poppy free provinces rose from 13 to 18. Despite these successes, Afghanistan still accounts for over 90 percent of the world's opium production. Opium gum is sometimes used as a currency—especially by rural farmers—and is used to store 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.

The majority of opium production comes from Taliban provincial strongholds in primarily the southern part of the country. The Taliban impose taxes on farmers and narcotics dealers, which undoubtedly helps finance their insurgency 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 a growing number of production labs 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. 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. 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. It is estimated that between 80 percent and 90 percent of all financial transfers in Afghanistan are made through hawala. 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. Hawala is a traditional form of finance and is deeply entrenched and widely used throughout Afghanistan and the neighboring region. Although the hawala system and formal financial sector are distinct, the two systems have links. Hawala dealers often keep accounts at banks and use wire-transfer services, while banks will occasionally use hawaladars to transmit funds to hard-to-reach areas within Afghanistan.

There are some 300 known hawala dealers in Kabul, with branches or additional dealers in each of the 34 provinces. There are approximately 1,500 dealers spread throughout Afghanistan that vary in size and reach. Primary hawala hubs include: Jalalabad, Kandahar, Herat, and Mazar-e-Sharif. 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 and take note of currencies traded, international pricing, deposit balances, debits and credits with other dealers, lending, cash on hand, etc. Hawaladars are required to be licensed. To address this requirement, Da Afghanistan Bank (DAB) the Central Bank of Afghanistan, issued a new money service provider regulation in 2006 that streamlined the licensing process and substantially reduced the ongoing compliance burden for hawaladars. The focus of the regulation is largely on anti-money laundering and counterterrorist financing (AML/CTF). The regulation requires and provides standard mechanisms for record keeping and reporting of large transactions. The DAB is currently studying ways to improve the licensing process and streamline the reporting process, which is largely paper-based. In Kabul, 110 licenses have been issued under the regulation, which is the result of DAB outreach, law enforcement actions, and pressure from commercial banks where hawaladars hold accounts. However, DAB supervision beyond Kabul remains limited and presents an important regulatory challenge. In response, the DAB has begun outreach efforts to money service providers in other large cities, including Jalalabad, Mazar-e-Sharif and Herat, and hopes to expand the licensing to these cities in 2009. Given how widely used the hawala system is in Afghanistan, financial crimes undoubtedly occur through these entities.

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, the Financial Transactions and Reports Analysis Center of Afghanistan (FinTRACA), Afghanistan's FIU, was established and functions as a semi-autonomous unit within the DAB. The FIU was opened in October 2005 with the assignment of a General Director, office space, and other basic resources. Since 2005, the FIU has expanded its operations into a new, secure building and added new analysts and law enforcement liaison officers.

Banks and other financial and nonfinancial institutions are required to report to the FIU all suspicious transactions (of any value) and large cash transactions above the equivalent of $10,000, as prescribed by the DAB. These financial institutions are also required to maintain their records for a minimum of 10 years. Approximately 22,000-25,000 large cash transaction reports are received from financial institutions and processed each month. This is a significant increase from last year and a clear indicator that financial flows through the formal financial system are gaining ground. The FIU currently has on record close to 500,000 large transaction reports. These reports are stored in a sophisticated and secure 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 and the FIUs of other nations through information sharing agreements. Currently, FinTRACA has information sharing agreements with the following countries: Belarus, Kyrgyz Republic, Russia, Turkey, Sri Lanka, and the United Kingdom. FinTRACA is not yet a member of the Egmont Group.

The formal banking sector consists of fifteen 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. Recent ABA meetings have centered on the ensuring that banks submit suspicious transaction reports (STRs) in higher numbers and of better quality. Twenty-seven STRs were received in 2008, several of which were referred to law enforcement for investigation. By comparison,

the FIU received seven STRs in 2007. Despite the increase in STR reporting, new workshops are planned to address this issue further in 2009.

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. Many banks also run their own compliance software to screen customers against UN and OFAC lists.

The Supervision Department within the DAB was formed at the end of 2003 and has been reorganized several times since then. The Supervision Department is currently divided into five divisions: Licensing, General Supervision (which includes on-site and off-site supervision), Special Supervision (which deals with special cases of problem banks), Regulation, and AML/CTF compliance. The AML/CTF compliance division is the newest addition. It is responsible for conducting examinations, overseeing money service providers, and conducting outreach to the commercial banking sector in the area of AML/CTF. Despite recent changes, the effectiveness of the Supervision Department in the AML area remains limited due to staffing, disjointed organization, and ongoing management issues. As a result, FinTRACA has taken on some supervisory responsibilities, yet resources at the FIU are limited for this task.

The Ministry of Interior (MOI) and the Attorney General's Office (AGO) 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 specialized knowledge in financial crimes enforcement and the resources to trace, seize, and freeze assets. According to DAB, it is not aware of Afghanistan freezing, seizing, or forfeiting related assets in 2008. To address this area of concern, FinTRACA is building on an existing MOU with the MOI for cooperation and currently shares information with the Sensitive Investigations Unit (SIU), a law enforcement group within the MOI. Moreover, FinTRACA recently signed an MOU with the AGO and is awaiting finalization of another information sharing agreement with the National Directorate of Security (NDS).

Pursuant to the Central Bank law, a Financial Services Tribunal was established to review certain decisions and orders of the DAB. As part of its duties, the Tribunal reviews supervisory actions of the DAB, but does not prosecute cases of financial

crime. At present, all financial crime cases are being forwarded to the Kabul Provincial Court where there has been limited activity in the past several years. The process to prosecute and adjudicate cases is long and cumbersome, significantly underdeveloped, and corruption often plays an important role across various levels. Afghanistan did not prosecute anyone for terrorist financing or money laundering in 2008.

Border security continues to be a major issue throughout Afghanistan. At present there are 14 official 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 under policed or not policed at all. These areas are therefore susceptible to illicit cross-border trafficking, trade-based money laundering, and bulk cash smuggling. Furthermore, officials estimate that there are over 1,000 unofficial border crossings along Afghanistan's porous border. Customs authorities, with the help of outside assistance, have made important improvements, but much work remains to be done.

Customs collection and enforcement has improved in some areas and remained static in others, 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 official or unofficial border crossing. However, a new pilot program is underway at Islam Qalah (a key border crossing point between Iran and Afghanistan) to search suspected cargo. In addition, a pilot program is underway for declaring large, cross-border currency transactions at the Kabul International Airport (KIA). This prototype serves as the foundation for expansion to other land and air crossings. Currently, KIA requires incoming and outgoing passengers to fill out declarations forms for carrying cash in an amount of 1 million Afghanis (approximately $20,000) or its equivalent. There is no restriction on transporting any amount of declared currency. The DAB is working with Customs authorities to further improve enforcement of airport declarations at KIA and other international airports in country. Currently, cash smuggling reports from KIA are entered into the Customs database. This Customs data is shared with the FIU for analysis. To address cash smuggling at the border, the DAB sent delegations to key border crossings to assess capacity and describe the provisions of the law to the local

authorities. Serious commitment is needed to adequately police the border to detect and intercept bulk cash smuggling.

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 extremely weak, 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 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 the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Afghanistan has signed, but not yet ratified the UN Convention against Corruption (UNCAC). Ratification of UNCAC and amendment of domestic laws to conform to the UNCAC's obligations, among the benchmarks established under the London Compact, 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.

The Government of Afghanistan has made progress over the past year in developing its overall AML/CTF regime. Recent improvement includes encouraging steps at the FIU, an increase in the reporting of large cash transactions, active participation in international AML bodies, continued work to improve AML compliance awareness among Afghan banks, and development and integration of information technology systems. However, Afghanistan must commit additional resources and find the political will to aggressively combat financial crimes, including corruption. Increasing the capacity of the DAB Supervision Department to conduct onsite AML/CTF supervision must be a priority. This should include both the formal and informal

banking sectors. Specifically, the GOA must develop, staff, and fund a concerted effort to bring hawaladars into compliance in Kabul and major areas of commerce. As part of this effort, Afghanistan is developing secure, reliable, and capable relationships among departments and agencies involved in law enforcement. Afghanistan should also continue efforts to develop the investigative capabilities of law enforcement authorities in various areas of financial crimes, particularly money laundering and terrorist finance. Judicial authorities must also 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. Afghanistan should ratify the UN Convention against Corruption and make corresponding changes in its domestic laws.

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. Albania continues to be a source country for human trafficking. 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. The European Commission's (EC) November 2008 progress report on Albania identifies corruption, judicial deficiencies, politicization of the civil service, and organized crime as the biggest problems in Albania. The report also says money laundering, organized crime, and drug-trafficking are "serious concerns," stating that Albania has made "limited progress" in its fight against organized crime and money laundering.

Criminals frequently invest tainted money in real estate and business development projects. Because of its high level of consumer imports and weak customs controls, Albania has a significant black market for certain smuggled goods such as tobacco, jewelry, and mobile phones. 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.

Because Albania's economy, particularly the private sector, remains largely cash-based, the proceeds from illicit activities are easily laundered in Albania. Albanian customs authorities report that organized criminal elements launder their illegal proceeds by smuggling bulk cash into and out of Albania by using international trade and fraudulent practices through import/export businesses. According to the Bank of Albania (the Central Bank), 23 percent of the money in circulation is outside of the banking system, compared to an average of ten percent in other Central and Eastern European transitioning economies. A significant portion of remittances enters the country through unofficial channels. It is estimated only half of total remittances enter Albania through banks or money transfer companies. The Central Bank estimates that in 2007, remittances comprised nearly 14 percent of Albania's annual gross domestic product (GDP). Black market exchange is still present in the country. However, it is declining steadily as a result of concerted efforts by the Government of Albania (GOA) to impede such exchanges. The Bankers Association estimates about half of all financial transactions take place through formal banking channels. Similarly, the GOA estimates proceeds from the informal sector account for approximately 30-60 percent of Albania's GDP. Although current law permits free trade zones, none are currently in operation.

The GOA is committed to fighting informality in the financial sector. There are 17 banks in Albania, and most of them have expanded both their national presence and the variety of services they offer. Electronic and automated teller machine (ATM) transactions are growing, especially in the urban areas, as more banks introduce this technology. ATM and debit and credit card usage expanded after the GOA decided to deliver public administration salaries through electronic transfers in 2005, and then compelled the private sector to follow suit in 2007. A May 2007 ruling also requires the private sector to channel at least 90 percent of its transactions through the banking sector. As of August 2008, 710,000 cards have been issued, almost entirely debit cards, but only a small number of people possess them and usage is primarily limited to a few large vendors.

Albania criminalizes money laundering through Article 287 of the Albanian Criminal Code of 1995, as amended. Albania's original money laundering law is "On the Prevention of Money Laundering," Law No. 8610 of May 17, 2000. In June 2003, Parliament approved Law No. 9084, which strengthens Law No. 8610 and improves the Criminal Code and the Criminal Procedure Code. Law No. 9084 redefines the legal concept of money laundering, revises its definition to harmonize it with international standards, outlaws the establishment of anonymous accounts, and permits the confiscation of accounts. The law also mandates the identification of beneficial owners and places reporting requirements on both financial institutions and individuals. According to the law, obliged institutions are required to report to Albania's financial intelligence unit (FIU) all transactions exceeding $20,000 as well as those transactions that involve suspicious activity, regardless of amount. Currently, no law criminalizes negligence by financial institutions in money laundering cases.

In 2006, the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force (FATF)-style regional body, conducted a mutual evaluation of Albania's anti-money laundering/counterterrorist financing (AML/CTF) regime. In an attempt to address the many deficiencies identified by MONEYVAL, in May 2008, the Albanian Parliament passed Law No. 9917, "On Money Laundering and Terrorist Financing." The law entered into force in September 2008. The new anti-money laundering (AML) law lowers the reporting threshold for cash transactions from $20,000 to $15,000. Law No. 9917 strengthens customer due diligence (CDD) requirements by requiring the identification of all customers regardless of the size of their transactions, mandating that reporting subjects maintain on-going due diligence of clients according to the know-your-customer (KYC) concept, and establishing the requirement to perform enhanced due diligence on a risk sensitive basis. The law also includes a better definition of "client" to include any natural or legal person that is party to a business relationship, and mandates that CDD measures apply in transactions where terrorist financing is suspected. The law also increases the number of reporting entities, clarifies record keeping requirements, and better defines the responsibilities of the FIU.

Covered 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 have compromised client confidentiality.

The Central Bank has established a task force to confirm banks' compliance with customer verification rules. It is the responsibility of the licensing authority to supervise intermediaries for compliance with AML regulations. For example, the Ministry of Justice is responsible for oversight of attorneys and notaries, and the Ministry of Finance (MOF) for accountants. Although regulations also cover nonbank financial institutions, enforcement remains poor in practice. There is an increasing number of suspicious transaction reports (STRs) coming from banks as that sector matures. A large number of STRs continue to come from tax and customs authorities and foreign counterparts.

Individuals must report to customs authorities all cross-border transactions that exceed approximately $10,000. Reportedly, Albania provides declaration forms at border crossing points but apparently only to those individuals who voluntarily make a declaration that would require completing the form. 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 establishes an administrative FIU, the General Directorate for the Prevention of Money Laundering (DPPPP), 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. Albania is in the process of preparing a new administrative law on FIU operations. Referred to as the "draft law," it will clarify certain AML 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 obligated entities, analyzes them, and then disseminates the results of its analysis to the Prosecutor's Office. Despite improvements of facilities and equipment, the Albanian FIU continues to face many operational obstacles. The FIU's capacity remains limited as staff turnover is a

persistent problem, and coordination and cooperation with the Prosecutor's Office remains problematic.

Since 2005, the FIU has referred to the Prosecutors Office 24 cases of both money laundering and terrorist financing, eight of which were reported during the first nine months of 2008. One case of money laundering has been prosecuted and currently there are two cases ready to be sent to the court. However, prosecution was declined for the rest. In January 2008, the first terrorist financing criminal case began in the First Instance Court for Serious Crimes. The case is against a Jordanian citizen accused of concealing funds allegedly intended to finance terrorism.

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 conviction for the predicate offense before issuing an indictment for money laundering. 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 Prosecutors 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 MOF's Customs Service and Tax Police, and Albanian intelligence services. The ECCJIU also cooperates with the FIU and the National Intelligence Service. The ECCJIU has responsibility for the prosecution of money laundering cases within the District of Tirana.

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 to support the volume of assets. During the first half of 2008, the Serious Crimes Prosecution Office rendered eight sequestration and confiscation decisions pursuant to the anti-mafia law. The properties sequestered include one hotel and $7,000 in cash. The properties confiscated include $13,000 in cash and bank accounts, seven vehicles, and a coffee bar. The Agency for the Administration of the Sequestration and

Confiscation of Assets (AASCA) was created in 2004, and is charged with the responsibility of administering confiscated assets. So far the agency has failed to function in a meaningful fashion. However, in response to pressure from U.S. government officials, the agency has started to perform better and has effectively taken control over several properties.

Article 230/a of the Penal Code criminalizes terrorist financing. The financing of terrorism, or its support of any kind, is punishable by a term of imprisonment of at least 15 years, and carries a fine of $50,000 to $100,000. The Penal Code also contains additional provisions dealing with terrorist financing, including sections dealing with disclosing information regarding an investigation or identification to identified persons and conducting financial transactions with identified persons. In an effort to make Albania's terrorist financing legislation comply more fully with international standards, the GOA, in 2007, amended its penal code to include a more specific definition for terrorist organizations. In addition, actions for terrorist purposes were identified and Albania's jurisdiction in terrorist financing cases was extended to include both resident and nonresident foreign citizens.

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 terrorist financiers, particularly with regard to the United Nations (UN) updated lists of designees. While comprehensive, it lacks implementing regulations and thus is not fully in force. As of June 2008, the MOF claimed to maintain asset freezes against six individuals and 14 foundations and companies on the UN Security Council's 1267 Committee's consolidated lists of identified terrorist entities. In total, assets worth more than $10,000,000, belonging to six persons, five foundations and nine companies, remain sequestered, including 83 bank accounts containing more than $3,950,000; 18 apartments in an expensive high rise apartment building in the center of Tirana; and several other properties throughout Albania. The full extent of sequestered assets is unknown.

The MOF is the main entity responsible for issuing freeze orders. After the MOF executes an order, the FIU circulates it to other government agencies, which then sequester any discovered assets belonging to the UNSCR 1267 named individual or

entity. The sequestration orders remain in force as long as the subject's name remains on the list.

Albania is a party to the UN 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 MONEYVAL, and the FIU is a member of the Egmont Group. The FIU has signed memoranda of understanding with 31 countries, Turkey being the most recent.

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 program deficiencies continue to hamper progress. In addition, although the new AML law was adopted in May 2008, it is difficult to evaluate the effectiveness of the new measures as implementing regulations have not yet been passed. The Government of Albania must provide the competent authorities adequate resources to administer and enforce the AML/CTF measures included in the May 2008 law. Albania also should incorporate into AML 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 remove the requirement of a conviction for the predicate offense before a conviction for money laundering can be obtained. The FIU, prosecutors and the ECCJIU should enhance their effectiveness through improved cooperation with one another and outreach to other entities. The FIU should take steps to achieve effective analysis of the large volume of currency transaction reports and STRs received. The GOA should enact its draft law on FIU operations and promulgate implementing regulations for all applicable laws as soon as possible. The GOS should ensure that those charged with pursuing financial crime increase their technical knowledge to include modern financial investigation techniques. The GOA should provide its police force with the means to adequately maintain and retrieve its case files and records. The link between criminal intelligence and investigations remains weak as there is a lack of coordination between the prosecutors and the police. Investigators and prosecutors should implement case management techniques, and prosecutors and judges need to become more conversant with the nuances of money laundering. The GOA should devise implementing regulations for Law 9258

regarding sequestration and confiscation of assets linked to terrorist financing so that it can be fully effective. The GOA also should improve the enforcement and enlarge the scope of its asset seizure and forfeiture regime, including fully funding and supporting the AASCA.

Algeria

Algeria is not a regional or 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.

The Algerian unemployment rate hovers unofficially above 25 percent, and mostly affects males under 30. This contributes to the crime rate, particularly kidnapping, theft, extortion, drug trafficking, and arms and cigarette smuggling. In addition to general criminal activity, terrorism has been on the rise. Al-Qaida in the Islamic Maghreb (AQIM) has committed a number of suicide attacks, kidnappings, roadside bombs, and assassinations throughout the country as well as in Algiers.

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 CTRF's leadership is composed of officials from the Ministries of Finance, Justice, Customs, Interior and the Central Bank.

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 also 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. Since 2004, 204 suspicious transaction reports (STRs) have been received by the CTRF. Of that number, two have been referred for prosecution, with one referral resulting in a conviction.

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 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 $700 to $70,000). 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 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.

In 2006, the Government of Algeria (GOA) decreed that payments exceeding a certain value must be made by check, wire transfer or other specified methods that are

traceable, rather than in cash. However, a nation-wide electronic check-clearing system has been slow to develop, and actors in the government, banking system and business community have been split as to what the cash payment limit should be, and if exceptions should be made for certain vendors such as traders of vegetables and fish. While nonresidents would be exempt from the requirements, they would still be obliged (like all travelers to and from the country) to report foreign currency in their possession to the Algerian Customs Authority.

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 undoubtedly escape the notice of government monitoring efforts.

There are reports that Algerian customs and law enforcement authorities are increasingly concerned with cases of customs fraud and trade-based money laundering. Other risk areas for financial crimes include unregulated alternative remittance and currency exchange systems; tax evasion; misuse of real estate transactions as a means of money laundering; commercial invoice fraud, and a cash-based economy. Most money laundering is believed to occur primarily outside the formal financial system, given the large percentage of financial transactions occurring in the informal gray and black economies.

Algerian authorities are taking steps to coordinate information sharing between concerned agencies. In 2008, the Ministry of Justice established a specialized cadre of investigators, prosecutors and judges who are being trained in the investigation and prosecution of financial crimes.

In November 2004, Algeria became a member of the Middle East and North Africa Financial Action Task Force (MENA FATF). Algeria is a party to the UN Convention against Transnational Organized Crime, the UN 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 Government of Algeria has taken significant steps to enhance its statutory regime against anti-money laundering and terrorist financing. It needs to move forward now

to implement those laws and eliminate bureaucratic barriers among various government agencies. The CTRF should be the focal point for anti-money laundering/counterterrorist finance (AML/CTF) suspicious transaction report analysis, which would require the CTRF to develop an in-house analytical capability. The CTRF should conduct outreach to the formal and informal financial sectors, adhere to international standards, and take steps to prepare for membership in the Egmont Group. In addition, given the scope of Algeria's informal economy, new emphasis should be made to identify value transfer mechanisms not covered in Algeria's AML/CTF legal and regulatory framework, and to limit the frequency and the size of cash transactions. Algerian law enforcement and customs authorities should enhance their ability to investigate trade-based money laundering, value transfer, and bulk cash smuggling used for financing terrorism and other illicit financial activities.

Angola

No new information was received for 2008. The following is a reprint of last year's report:

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, 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 due to its offshore financial sector and Internet gaming industry. Illicit proceeds from the transshipment of narcotics and from financial crimes occurring in the U.S. also are laundered in Antigua and Barbuda.

As of 2008, Antigua and Barbuda has eight domestic banks, seven credit unions, seven money transmitters, 18 offshore banks, two trusts, three offshore insurance companies, 2,967 international business corporations (IBCs), and 20 licensed Internet gaming companies. In addition, there are approximately 33 real estate agents, five casinos, and 14 dealers of precious metals and stones. 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 naturalized 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 $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.

The Money Laundering Prevention Act of 1996 (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 creates a Supervisory Authority. In 2003, the director of the Office of National Drug Control and Money Laundering Policy (ONDCP) was designated to act in this capacity. The MLPA covers institutions defined under the Banking Act, IBCA,

and the Financial Institutions (Non-Banking) Act, which include offshore banks, IBCs, money transmitters, 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 $25,000. The GOAB amended the MLPA in 2008 to provide for the licensing and regulation of money transmitters; enhance tipping off and record retention provisions; require financial institutions to review complex or unusual transactions whether the transaction was completed or not; and to extend power to seize and detain suspected currency to ONDCP officers.

Domestic casinos 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 $2,800,000 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 areas deemed as priority by the government. Casinos and sports book-wagering operations in Antigua and Barbuda's free trade zone are supervised by the ONDCP, 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 gaming 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. The GOAB does not have 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 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, the MLPA contains provisions for obtaining client and ownership information. Section 25 of the MLPA states the provisions of the 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 Office of National Drug Control and Money Laundering Policy Act, 2003 (ONDCP Act) establishes the ONDCP as the 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. In its role as the Supervisory Authority, the ONDCP fulfills the responsibilities described in the MLPA, which includes the supervision of all financial institutions with respect to filing suspicious transaction reports (STRs). STRs from domestic and offshore gaming entities are sent to the ONDCP and FSRC. As of December 2008, the ONDCP had received 73 STRs (increased from 43 in 2007), 14 of which were investigated. 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 programs and submit reports 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 (MOU) with the FSRC and is expected to sign another with the ECCB. Other MOUs 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. No arrests, prosecutions or convictions were reported by the GOAB in 2006 or 2007.

Under the MLPA, a person entering or leaving the country is required to report to the ONDCP whether he or she is carrying $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 $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. One arrest was made in January 2008, involving the undeclared importation of approximately $80,000 by a passenger at the airport who carried part of it in his hand luggage and the rest strapped around his waist.

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 for 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 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 has entered into an asset sharing agreement with Canada, and is currently working on asset sharing agreements with other jurisdictions, including the U.S. The director of ONDCP, with Cabinet approval, may enter into agreements and arrangements that cover matters relating to asset sharing with authorities of a foreign State. There are asset sharing agreements with some countries, while others are negotiated on an ad hoc basis. Regardless of its own civil forfeiture laws, currently the

GOAB can only provide forfeiture assistance in criminal forfeiture cases, an anomaly which should be remedied.

In recent years, the GOAB has frozen approximately $6,000,000 in Antigua and Barbuda financial institutions as a result of U.S. requests and has repatriated approximately $4,000,000. The GOAB has frozen, on its own initiative, over $90,000,000 believed to be connected to money laundering cases still pending in the United States and other countries. The GOAB reported seizing $420,236 in 2006, $14,753 in 2007, and $81,601 in 2008.

The GOAB enacted the Prevention of Terrorism Act 2001(PTA), amended in 2005, to implement the UN conventions on terrorism. The PTA 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 PTA 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 PTA requires financial institutions to report every three months on whether 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 suspected to be related to the financing of terrorism to the ONDCP. The GOAB amended the PTA in 2008 to provide the Supervisory Authority and the ONDCP the power to direct a financial institution to freeze property for up to seven days while the authority seeks a freeze order from the court. The amendment also includes provisions making it an offense for individuals to know and/or fail to disclose information leading to prevention of an attempt to commit a terrorist act. Those who conceal wrongdoings will be ordered to pay a penalty of $500,000.

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 the 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 MOU is established. In 1999, a Mutual Legal Assistance Treaty 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), a Financial Action Task Force-style regional body, and underwent a mutual evaluation in June 2008. The evaluation notes several deficiencies in the GOAB's anti-money laundering/counterterrorist financing (AML/CTF) regime including: weak requirements for enhanced customer due diligence for high risk customers such as politically exposed persons; non-enforceable requirements for financial institutions to have policies and procedures in place to address specific risks associated with non-face-to-face customers; non-enforceable requirements prohibiting domestic and offshore banks from having correspondent banking relationships with shell banks; and wire transfer requirements not enforceable in accordance with the FATF Recommendations. Furthermore, the evaluation notes the GOAB needs to enact provisions to require financial institutions to develop internal controls and procedures to include terrorist financing; the supervisory authorities have not been given the responsibility for ensuring financial institutions adequately comply with AML/CTF requirements; and there are no measures in place to ensure that bearer shares under the IBCA are not misused for money laundering.

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, and the UN Convention for the Suppression of the Financing of 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 take steps to amend its legislation of cover intermediaries, enhanced due diligence for PEPs and other high-risk customers, and to provide for enforceable provisions on the prohibition of correspondent accounts for or with shell banks. The GOAB also should implement and enforce all provisions of its AML/CTF legislation, including the comprehensive supervision of its offshore sector and gaming industry. The ONDCP should be given direct access to financial institution records in order to effectively assess their AML/CTF compliance. 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. More comprehensive investigations could lead to higher numbers of arrests, prosecutions, and convictions. Continued efforts should be made to enhance the capacity of law enforcement and customs authorities to recognize money laundering typologies that fall outside the formal financial sector. Continued international cooperation, particularly with regard to the timely sharing of statistics and information related to offshore institutions, and enforcement of foreign civil asset forfeiture orders will likewise enhance Antigua and Barbuda's ability to combat money laundering.

Argentina*

*[*This section has been revised since its original posting to the website. See **version** as submitted to Congress.]*

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. 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 outside the formal financial system (both offshore and in-country), much of it legitimately earned money that was not taxed. To combat capital flight and to encourage the return of these undeclared billions, on December 18, 2008, Argentina's legislature approved a tax moratorium and capital repatriation law that would provide a tax amnesty for persons who repatriate undeclared offshore assets during a six-month window. The law entered into force December 24. Under the law, government tax authorities are prohibited from inquiring into the provenance of declared funds, and some critics have raised concerns that this could facilitate money laundering. Implementing regulations are to be promulgated in February 2009, which will clarify that transactions under this law will be subject to existing laws, rules, and regulations related to the prevention of financial crimes, and will also reportedly include a requirement that transfers from abroad originate in countries that comply with international money laundering and terrorism financing standards. Top level GOA officials have indicated that they will ensure all Argentine legislation, including this law, abides by Argentina's obligations as a member of the Financial Action Task Force (FATF) and the Financial Action Task Force fo South America (GAFISUD). In January the GOA takes over the Presidency of GAFISUD for 2009.

In 2007, the Argentine Congress passed legislation criminalizing terrorism and terrorist financing. Law 26.268, "Illegal Terrorist Associations and Terrorism Financing," 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. With the passage of Law 26.268, Argentina joins Chile, Colombia, and Uruguay as the only countries in South America to have criminalized terrorist financing.

On September 11, 2007, former 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 ongoing challenge is for Argentine law enforcement and regulatory institutions to continue to implement the National Agenda and aggressively enforce the 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 (although money laundering was first criminalized under Section 25 of Law 23.737, which amended Argentina's Penal Code in October 1989). Law 25.246 expanded the predicate offenses for money laundering to include all crimes listed in the Penal Code, set a stricter regulatory framework for the financial sectors, and created 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 requires similar reporting by designated self-regulated nonfinancial entities that report to the UIF. Further, 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 special anti-money laundering and counterterrorism finance prosecution unit of 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 30,000 pesos (approximately $9,000).

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 Counter-narcotics Secretariat (SEDRONAR), and the Justice, Economy, and Interior Ministries. The UIF legally must consult the Board of Advisors, although its 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 a designated period. As of September 2008 the UIF had received 4,032 reports of suspicious or unusual activities since its inception in November 2002, forwarded 491 suspected cases of money laundering to prosecutors for review, and collaborated with judicial system investigations of 155 cases of suspected money

laundering. There have been only two convictions for money laundering since it was first criminalized in 1989 under Article 25 of Narcotics Law 23.737 and none since the passage of Law 25.246 in 2000. A third money laundering case brought under Law 23.737 is pending before Argentina's Supreme Court.

The Central Bank requires by resolution that all banks maintain a database of all transactions exceeding 30,000 pesos, and submit the data to the Central Bank upon request. 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 $3,200). The UIF further receives copies of the declarations to be made by all individuals (foreigners or Argentine citizens) entering or departing Argentina with over $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 a law that 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 anti-money laundering and counterfinancing of terrorism (AML/CTF) regime, Law 25.246 still limits the UIF's role to investigating only money laundering arising from seven specific or "predicate" crimes. Also, the law does not criminalize money laundering as an offense independent 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 $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, Security, and Human Rights became fully functional, managing the government's AML/CTF

efforts and representing Argentina at the Financial Action Task Force (FATF), the Financial Action Task Force for South America (GAFISUD), and the Organization of American States Inter-American Control Commission (OAS/CICAD) Group of Experts. The Attorney General's special prosecution unit set up to handle money laundering and terrorism finance cases began operations in 2007. Although the Argentine Central Bank's Superintendent of Banks has not created a specialized anti-money laundering and counterterrorism finance examination program as previously considered, it began in 2008 specific anti-money laundering and counterterrorism finance inspections of financial entities and exchange houses.

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 provides that proceeds of assets forfeited under this law can primarily be used to fund the UIF. Argentine courts and law enforcement agencies have used the authority to seize and utilize assets on a selective and limited basis, although complex procedural requirements complicate authorities' ability to take full advantage of the asset seizure provisions offered under these laws.

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 provided financial or logistical support to Hizballah and operated in the territory of neighboring countries that border Argentina. This region is commonly referred to as the Tri-Border Area, located between Argentina, Brazil, and Paraguay. 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. One key focus of the TTU, as well as of other TTUs in the region, is financial crime occurring in the Tri-Border Area. The creation of the TTU was also a positive step toward 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 and settling accounts.

The GOA remains active in multilateral counternarcotics and international AML/CTF organizations. It is a member of the 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 Convention for the Suppression of the Financing of 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 U.S. government 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 counterterrorist financing legislation and strengthened mechanisms available under Laws 26.119, 26.087, 25.246, and 26.268 Argentina has the legal and regulatory capability to combat and prevent money laundering and terrorist financing. The new national anti-money laundering and counterterrorist financing agenda

provides the structure for the GOA to improve existing legislation and regulation, and enhance inter-agency coordination. The ongoing challenge is for Argentine law enforcement and regulatory agencies and institutions, including the Ministry of Justice, Central Bank, the UIF, and other institutions to implement fully 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 $16,000) required to establish a money laundering offense. To comply fully with the FATF recommendation on the regulation of bulk money transactions, Argentina should review policy options that are 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

authority over foreign affairs, defense, some judicial functions, human rights, and good governance issue are retained by the Kingdom. 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 one offshore bank, one mortgage bank, one credit union, an investment bank, a finance company, seven life and general insurance companies, and eleven casinos. The island also has four registered money transmitters, two exempted U.S. money transmitters (Money Gram and Western Union), 13 nonlife and general insurance companies, four captive insurance companies, and 11 company pension funds. There are approximately 5,343 limited liability companies of which 372 are offshore limited liability companies or offshore

NVs, which were to have ceased operation in 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 $280 registration fee and must have a minimum of $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 ceased 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

Meeting 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 banks, insurance companies, company pension funds, and money transfer companies and is responsible for on-site and off-site examinations. However, the Central Bank has not conducted any on-site examinations of its offshore banks. 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. Draft legislation to regulate company service providers is also in legislative review.

Aruba's State Ordinance 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 florins $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 (statistics for 2008 are not available). 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 florins ($11,300) 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 on Money Laundering 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 FATF Nine 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 Kingdom of the Netherlands (KON) 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 KON 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 KON 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 Kingdom has not yet extended application of the UN Convention against Corruption to Aruba. Aruba participates in the Financial Action Task Force (FATF) as part of the Kingdom of the Netherlands and underwent a mutual evaluation in November 2008. 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 counterterrorist 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 counterterrorist 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 $78 trillion). Australia's total stock market capitalization is over AU $1.63 trillion (approximately $1.1 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 $ 3 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.

Subsequent to the Financial Action Task Force (FATF) Mutual Evaluation, 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 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 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 2007-08, AUSTRAC published 11 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.

A requirement went into effect for reporting entities to submit an AML/CTF compliance report to AUSTRAC indicating their level of preparedness and compliance with AML/CTF rules, in March 2008. An AML/CTF compliance report provides information about reporting entities' compliance with the AML/CTF Act 2006, the regulations and the AML/CTF Rules. It is required under the AML/CTF Act in Part 3, Division 5, which

came into effect in June 2007. The compliance reports provide AUSTRAC and the reporting entity an indication of their progress in implementing their AML/CTF obligations.

The Australian Government is working 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. As a result of the passage of the AML/CTF (Transitional Provisions and Consequential Amendments) Act, a number of amendments to other Commonwealth legislation, including the FTR Act, were necessary. The AML/CTF Act makes those amendments, which include the repeal of some provisions of the FTR Act. The second tranche includes further obligations in relation to customer due diligence and reporting, commenced in December 2008.

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. $6,500), and all international funds transfers into or out of Australia, regardless of value. The FTR Act will continue to apply to cash dealers who are not reporting entities under the AML/CTF Act.

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 is 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 2007-08 Australian financial year, AUSTRAC's FTR information was used in 2968 operational matters. Results from the Australian Taxation Office (ATO) shows that the FTR information contributed to more than AU $76 million (approximately U.S. $49 million) in ATO assessments during the year. In 2007-08, AUSTRAC received 17,965,373 financial transaction reports, with 99.7 percent of the reports submitted electronically through the EDDS Web reporting system. AUSTRAC received 29,089 suspect transaction reports (SUSTRs), an increase of 19 percent over the previous year.

During 2007-08, there was a significant increase in the total number of financial transaction reports received by AUSTRAC. Significant cash transactions reports (SCTRs) account for 16 percent of the total number of FTRs reported to AUSTRAC in 2007-08 and are reported by cash dealers and solicitors. In 2007-08, AUSTRAC received 2.934,855 SCTRs, an increase of 9.7 percent from the previous year. Cash dealers are also required to report all international funds transfer instructions (IFTIs) to AUSTRAC. Cash dealers reported 14,963,719 IFTIs to AUSTRAC during the financial

year—a 15.0 percent increase from 2005-06. Cross-border movement of physical currency (CBM-PC) reports (which have replaced international currency transfer reports, ICTRs) are primarily declared to the Australian Customs Service (ACS) by individuals when they enter or depart from Australia. For 2007-08, AUSTRAC received 36,131 CPM-PC reports, a 54.7 percent decrease from the previous financial year. This increase in reports came after AUSTRAC and ACS undertook extensive public awareness campaigns during 2007-08 to inform travelers of their obligation to declare physical currency. The Infringement Notice Scheme (INS) is a 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 Minister for Home Affairs launched three new tools to assist industry compliance with AML/CTF obligations, in addition to updating the eLearning application. AUSTRAC Online is a secure Internet-based system that 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/counterterrorist 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 provides AUSTRAC with a civil penalty framework and other intermediate sanctions, such as enforceable undertakings, remedial directions and external audits for noncompliance. AUSTRAC 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. Between July 2007 and July 2008, AUSTRAC delivered more than 215 education sessions to approximately 5000 people from more than 1500 reporting entities ranging from banks and mortgage brokers, to pubs and casinos and designated remittance services. Additionally, AUSTRAC provided more than 100 presentations to partner agencies, including the Australian Federal Police (AFP), the Customs Service, Taxation Office and the State and Territory Police. In 2007-08 AUSTRAC developed and began implementation of a new on-site assessment strategy, including governance arrangements, a target for the number of annual inspections to be done, and inspection selection criteria. AUSTRAC in 2007-08 conducted over 130 on-site assessments of reporting entities to assess their compliance with FTR Act and AML/CTF Act obligations.

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. It 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.

The Australian Government is also developing a strategy for improving controls to prevent the misuse of non profit organizations (NPOs) for financing terrorism. A critical aspect of this strategy will be to work in partnership with the NPO sector to raise awareness about the vulnerability of the sector to abuse for terrorism financing. A review is underway to determine if any gaps exist in information currently collected from the NPO sector by Australian government agencies.

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. The Australian Federal Police accepted 52 new money laundering investigations from July 2007 to April 2008 and restrained AU $37,831,143 (approximately U.S. $24,630,000) of which AU $341,923 (approximately $6,082,000) was forfeited. From July 2007 through mid-May 2008, the CDPP reported that 68 indictments for money laundering were issued. At the July 2008 plenary of Asia Pacific Group held in Bali, Indonesia, Australian delegation mentioned that a

conviction for money laundering involving AU $43,000 (approximately $30,000) was the largest sum ever involved in a successfully prosecuted money laundering case in the country. 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. This group of five countries includes 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's CEO was appointed to a one-year term as Chair of the Egmont Commission in May 2008. 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 52 other countries. AUSTRAC has also signed 34 domestic MOUs with Commonwealth, State, and Territory partner agencies covering a spectrum of agencies to include regulatory, law enforcement, social justice, national security and revenue.

Following the bombings in Bali in October 2002, the Australian Government announced an AU $10 million (approximately $6.5 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. AUSTRAC, ACS and the AFP worked closely with agencies from the United States and Japan to hold the South-East Asian Regional Bulk Cash Smuggling Workshop at the Jakarta Centre for Law Enforcement Cooperation (JCLEC) in Semarang, Indonesia in April 2008. As part of Australia's broader regional assistance initiatives, AUSTRAC has 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; this program will continue until 2009-10. AUSTRAC assisted the Indonesian FIU, PPATK (Indonesian Financial Transaction Reports and Analysis Center), in developing a program for the receipt and analysis of suspicious transaction reports and the improvement of data quality and information processing. In the Pacific region, AUSTRAC has developed and provided unique software ("FIU-in-a-Box") 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, and conducted a review of these FIUs in June 2008. AUSTRAC concluded IT Needs Assessments in Papua New Guinea and Nauru in 2007-08 as part of its engagement with Pacific FIUs. The AGD received a grant of AU $7.7 million (approximately U.S. $5.1 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 United Nations Global Program against Money Laundering and employs residential and intermittent mentors to develop or enhance

existing AML/CTF regimes in the non-FATF member states of the Pacific Islands Forum.

The GOA continues to pursue a comprehensive anti-money laundering/counterterrorist 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

Austria is a major financial center, and Austrian banking groups control significant shares of the banking markets in Central, Eastern and Southeastern Europe. According to Austrian National Bank statistics, Austria ranks among those with the highest numbers of banks and bank branches per capita in the world, with 870 banks and one bank branch for every 1,610 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 volume 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. The law is 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. Since January 1, 2008, the GOA has implemented strict new criminal regulations against corruption that define corruption as an additional predicate offense, and has appointed a special public prosecutor with responsibility for corruption investigations and indictments in all of Austria.

The Law on Responsibility of Associations mandates 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.

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 $14,300) or more. This declaration, which includes information on source and use, must be provided when crossing an external EU border. 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 (approximately $21,450)

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 non-face-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.

An amendment to the Banking Act, in effect since January 1, 2008, tightens 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 also require institutions to determine the identity of beneficial owners and introduce risk-based customer analysis for all customers. Financial institutions must also 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 apply if the customer has not been physically present for identification purposes (for example, non-face-to-face transactions or 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 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, tightens record keeping requirements for insurance companies.

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 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 suspicious transaction reports (STRs) and record keeping for dealers in high value goods, auctioneers, real estate agents, casinos, lawyers, notaries, certified public accountants, and auditors. Amendments to the Stock Exchange Act, the Securities Supervision Act, the Insurance Act, and Austrian laws governing lawyers and notaries came into effect on January 1, 2008. The amendment to the Gambling Act has been in effect since August 26, 2008, and the amendment to the law governing accounting professionals since April 23, 2008. These introduced stricter regulations regarding customer identification procedures, including requiring customer identification for all transactions of more than 15,000 euros (approximately $21,450) for customers without a permanent business relationship. Lawyers and notaries are exempt from their reporting obligations for information obtained in the 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 requires 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 (approximately $21,450) 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 January 1, 2007, financial institutions require customer identification for all fund transfers of 1,000 euros (approximately $1,430) or more.

Austria's FIU is located within the Austrian Interior Ministry's Bundeskriminalamt (Federal Criminal Intelligence Service). The FIU is the central repository of STRs and has police powers. During the first ten months of 2008, the FIU received approximately 910 STRs from banks and others—a figure indicating little change from the 1,085 suspicious transactions reported in 2007. The FIU has also responded to requests for information from Interpol, Europol, other FIUs, and other authorities. There were ten money laundering convictions in 2006 and 18 in 2007.

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 2008, Austrian courts froze assets worth more than 110 million euros (approximately $157,000,000).

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 introduces the following criminal offense categories: terrorist "grouping," terrorist criminal activities, and financing of terrorism, in line with UNSCR 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 Executive Order 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 (35 in 2007 and 26 during the first ten months of 2008) with the Austrian Interior Ministry's Federal Agency for State Protection and Counterterrorism (BVT). There were no convictions for terrorist financing in 2006 or 2007.

The GOA has undertaken important efforts that may help thwart the misuse of charitable or nonprofit entities as conduits for terrorist financing. The Law on Associations covers charities and all other nonprofit associations in Austria. The law regulates the establishment of associations, by-laws, 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 (approximately $4,300,000) or annual donations of more than 1 million euros (approximately $1,430,000) 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 of monitoring for charities and nonprofit organizations, particularly in cases where business relationships suggest they could be connected to money laundering or 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.—GOA agreement on sharing of forfeited assets is pending signature in both the U.S. and Austria. 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 and with Croatia.

Austria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Austria is a member of the FATF and will undergo a FATF mutual evaluation in 2009. The FIU is a member of the Egmont Group.

The Government of Austria has implemented a viable, comprehensive anti-money laundering and counterterrorist financing regime. The GOA should ensure it provides the FIU and law enforcement the resources 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 should consider mandating the reporting of all currency transactions exceeding an established

threshold. The GOA also should consider enacting legislation that will provide for asset sharing with other governments.

Azerbaijan

The following information was obtained primarily from the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) public statement of December 12, 2008 and the mutual evaluation report on Azerbaijan adopted at the MONEYVAL plenary in December 2008.

At the crossroads of Europe and Central Asia and with vast amounts of natural resources, Azerbaijan is a rapidly growing economy. The illicit drug trade generates the largest amount of illicit funds by far, followed by theft and fraud. Illicit funds also derive from robbery, tax evasion, and smuggling, and in recent years, trafficking in persons has also become an increasing problem that generates illicit funds. Corruption is endemic in the country, and organized crime groups exist as well, although authorities do not have a good understanding of the groups or their operations. Azerbaijani authorities believe that money laundering and terrorist financing operates largely through the banking sector.

Economic growth, fueled by the oil and natural gas resources present in Azerbaijan and the energy sector, is strong. International trade has also been increasing since independence, as has foreign investment. At the end of 2007, Azerbaijan had 46 commercial banks, 6 of which worked mostly with foreign capital. Two banks are completely state-owned. There were 77 licensed credit unions and 18 licensed microfinance institutions, as well as 29 licensed insurance companies. As of January 1, 2008, Azerbaijan had 37 licensed professional securities actors.

Azerbaijan's Customs authorities have received no guidance regarding identification of potential money launderers or terrorist financiers entering or exiting the country. Even if Customs suspected financial crime, the agency does not have the legal authority to interdict or confiscate currency, nor does it have the obligation to report suspicions to other law enforcement authorities.

In 2003, law enforcement found a number of charitable organizations linked to terrorist financing and shut them down. Authorities remain cognizant of the vulnerabilities that the nonprofit sector poses and consider nonprofit organizations

(NPOs) reporting entities. However, Azerbaijan has not examined the risks of this sector and authorities have not reviewed the organizations for terrorist financing vulnerabilities.

In February 2006 MONEYVAL initiated Compliance Enhancing Procedures against Azerbaijan due to its failure to pass satisfactory and comprehensive AML/CTF preventive legislation, lack of an FIU and lack of a legally based and effective STR regime. In February 2008, MONEYVAL conducted a high-level visit to draw the attention of senior Azerbaijani authorities to the importance of an anti-money laundering/counterterrorist financing (AML/CTF) regime. In April 2008, MONEYVAL assessors conducted an on-site evaluation of the Azerbaijan AML/CTF regime, which the plenary adopted in December 2008. In December 2008, MONEYVAL issued a public statement registering its concern with Azerbaijan's failure to pass and implement an AML/CTF law, and calling upon member states and other countries to advise their financial institutions to apply enhanced due diligence to transactions with links to Azerbaijan.

The Government of Azerbaijan (GOAJ) has no AML/CTF preventative law in place, although a draft law passed a second reading on October 31, 2008. Reportedly, when implemented, the draft law anti-money law will, in part, address some of the current shortcomings, such as anonymous accounts, enhanced due diligence for politically exposed persons (PEPs), freezing and seizure protocols and the filing of suspicious transaction reports, although the draft law does not comport with international standards. The GOAJ has recently advised that it intends to amend the draft law to meet international standards. The GOAJ has instituted some provisions aimed at criminalizing money laundering, but the current provisions in place designed to criminalize money laundering have major deficiencies and there has been no implementation. Only natural persons are subject to criminal liability for money laundering. Azerbaijan has not applied the principles of corporate criminal liability, so no legal persons can be punished for money laundering or terrorist financing. Azerbaijan has taken the "all crimes" approach to predicate offenses. However, insider trading and market manipulation are not considered offenses.

The mutual evaluation report (MER) noted that the GOAJ provided no evidence of investigations or court proceedings involving money laundering as a stand-alone

offense. Under the current patchwork regime, it is unclear whether prosecutors must obtain a conviction for the predicate offense in order to open a money laundering investigation. It is also unclear whether authorities can pursue money laundering if the predicate offense takes place in another country. Azerbaijan has no criminal liability for legal persons. Only natural persons can receive punishment for money laundering and terrorist financing.

Although in the absence of a comprehensive law there are no specific supervisory bodies for AML/CTF compliance in the various sectors, authorities maintain that the AML/CTF competencies are addressed by the supervisors in the course of general supervisory activities. The National Bank of Azerbaijan (NBA) is the supervisory authority for banks and credit unions. The Ministry of Finance supervises insurance companies, and the State Committee on Securities supervises the securities sector. The competent authorities appear knowledgeable, well-resourced, and well-trained in AML/CTF issues and conduct inspections regularly. However, only the NBA includes an AML/CTF component in its inspections.

Customer due diligence (CDD) measures derive from a number of laws and regulations. GOA-issued regulations are enforceable, although for the most part a legislative body has not authorized or issued them. The NBA has issued "Methodological Guidance on the Prevention of the Legalization of Illegally Obtained Funds or Other Property Through the Banking System," but this guidance is not law and is not binding. There is no legal provision in the law for sanctioning violations of AML/CTF guidance or regulations. Likewise, there are few customer identification obligations outlined in the law "On Banks." While the law does prohibit the opening of anonymous accounts, it does not require institutions to verify the beneficial owner of an account. Joint stock companies can issue unlimited numbers of bearer shares. There is no particular enhanced due diligence requirement for dealings with PEPs, and Azerbaijani banks lack regulations governing their actions when opening correspondent accounts elsewhere as well as when conducting non face-to-face transactions or establishing relationships in this manner. There are no prohibitions on financial institutions executing transactions with shell banks. Although there is a record-keeping requirement, it lacks clarity regarding the records that need to be retained and provides no possibility for extending the record-keeping time, even when

requested by a competent authority. Azerbaijan does not mandate its financial institutions to ensure that their foreign branches and subsidiaries submit to the requirements of the country where their headquarters are located. Bank secrecy provisions do not pose obstacles for law enforcement investigations. A court decision will mandate the lifting of professional secrecy.

Azerbaijan has no law obliging financial institutions to file suspicious transaction reports (STRs) when they suspect or have reasonable grounds to suspect that funds are the proceeds of crime. The NBA issued letters to banks in 2007, generating approximately 500 STRs. Of these, the NBA passed 24 to law enforcement. There is also no legal obligation on financial institutions to report suspicion of terrorist financing to a financial intelligence unit (FIU). Azerbaijani authorities have not conducted any training our outreach with regard to money laundering and terrorist financing. Even the formal financial sector lacks awareness and understanding of AML/CTF issues: one major commercial bank was unaware of STRs and STR reporting. There are no legal obligations for financial institutions to establish AML/CTF programs or designate a compliance officer.

Because there is no effective law, the designated nonfinancial businesses and professions (DNFBPs) have no AML/CTF obligations. There are no competent authorities to serve as the AML/CTF supervisors. Tax advisors, the 800 lawyers, the 94 auditors and accountants (of which none are independent) do not fall under the AML/CTF rubric at all, as authorities consider them to be a small portion of the nonbank sector and low risk. The 150 notaries in Azerbaijan and approximately 1000 dealers in precious metals and stones may have reporting obligations in the future. The Assay Chamber supervises the dealers in previous metals and stones, but lacks any AML/CTF component. Azerbaijan has prohibited gaming and casino activities, although it does run a state lottery.

The MER reported that there appeared to be little coordination at the policy and at the working level between the agencies charged with combating AML/CTF and between the supervisory bodies.

Azerbaijan lacks an FIU. The GOAJ has advised that until adoption of the AML/CTF law, it will not be able to establish an FIU. Currently, the 3-member AML Division of the National Bank of Azerbaijan (NBA) has taken on some of the functions that an FIU

would manage. However, the General Prosecutor's office was unaware of the existence of any suspicious transaction reports (STRs).

Investigatory authority in AML/CTF cases lies ultimately with the General Prosecutor. The Ministry of National Security has also worked with AML/CTF issues, reporting that the majority of STRs relate to terrorist financing. However, few terrorist-related investigations or prosecutions appear to have taken place. Although there are ways that the current criminal law could be effective, the Prosecutor's Office does not use it. Law enforcement authorities have not received training or outreach with regard to money laundering and terrorist financing issues, and lack overall awareness of the offense. They also lack training in financial investigation techniques. While law enforcement overall appears to have proper authority and enough resources, the amount of resources directed to pursuing money launderers as opposed to other crime seems scant. There is an overall perception that prosecutions for money laundering would be very difficult and would not add value to the conviction for the predicate offense. Authorities interpret the money laundering offense to mean self-laundering only and have not considered third party laundering or the use of money laundering in organized crime.

Azerbaijani authorities did not provide statistics regarding asset seizure and confiscation, but told the MONEYVAL assessors that they have issued such orders. The only crimes whose proceeds would be subject to confiscation are money laundering and crimes punishable by two years or more in prison. Because there is no criminal liability for legal persons, the authorities cannot confiscate property from legal persons.

Although the GOAJ has criminalized the financing of terrorism, it has applied a very narrow definition. As the definition now stands, it is not wholly a predicate offense for money laundering. Authorities would also need to provide evidence of financial or material support for specific terrorist acts, as Azerbaijan has not explicitly criminalized the financing of terrorist organizations or an individual terrorist; it also has omitted as a criminal offence the support of recruitment and other activities by terrorist organizations and support of the families of terrorists. Prosecutors have obtained one successful prosecution against an individual collecting money to finance future terrorist acts.

Azerbaijan appears to have instituted a system to implement UNSCR 1267 and 1373, and the Ministry of Foreign Affairs has sent out the lists to other Ministries and supervisory bodies. However, there has been no guidance issued, even to the financial sector, and no one outside the banking sector appears to be aware of the lists. The nonbank sectors have never frozen assets in conjunction with the UNSCRs. There does not appear to be an authority charged with designating persons or entities subject to freezing orders. Since 2003, Azerbaijani authorities have not issued any freezing orders.

Azerbaijan has entered into a number of mutual legal assistance treaties, although the absence of criminal liability for legal or corporate persons and the dual criminality requirement could pose challenges to legal cooperation. Azerbaijan does not have a mutual legal assistance treaty with the United States. Azerbaijan's law enforcement authorities are developing a network of cooperation and information exchange at the intelligence level. Although the lack of an FIU means that Azerbaijan's cooperation with the FIU community is severely hampered, the NBA has responded to requests from two FIUs.

Azerbaijan has ratified the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism. It is a member of the MONEYVAL Committee.

It is encouraging that the Government of Azerbaijan (GOAJ) will have passed AML/CTF legislation in early 2009 that will provide for the development of a financial intelligence unit. However, that legislation will require amending to conform to international standards. The GOAJ should begin implementing the new legislation through promulgating binding and enforceable regulations for both the financial sectors and the DNFBPs. It should conduct awareness and outreach campaigns for the entities that will be subject to the law, and work to establish an FIU so that upon passage of the legislation, the FIU will be able to begin its work. Azerbaijan should prohibit bearer shares. The GOAJ should ensure that the regulatory authorities and enforcement agencies have resources targeted specifically to the pursuit of money laundering and terrorist financing/ The GOAJ should provide training, in particular for law enforcement and prosecutors, to enable authorities to conduct complex

investigations and obtain convictions. The GOAJ should establish venues for both strategy formulation and coordination and cooperation between the relevant authorities charged with AML/CTF work. The GOAJ should conduct outreach regarding the UN Security Council Resolutions and freezing orders.

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 registered in the offshore financial sector.

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, and societies. Regulated designated nonfinancial businesses and

professions include casinos; lawyers; accountants; real estate agents; and company service providers. Dealers in precious metals and stones are not included.

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 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, augments 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. In May 2008, amendments to the Banks and Trust Companies Regulation (Amendment) Act 2008 and the Central Bank of Bahamas Act 2008 formally place money transmission businesses under the supervision of the Central Bank. The Banks and Trust Companies (Money Transmission Business) Regulations 2008 requires money transmission agents to register with the Central Bank.

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 from to full physical presence is

complete. Some industry sources have suggested that this requirement has contributed to a decline in shell banks and trusts from 301 in 2003 to 136 as of June 30, 2008.

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.

The Proceeds of Crime Act 2000 criminalizes money laundering. The POCA provides for four main money laundering offenses: the transfer or conversion of property with the intent to conceal or disguise the property; assisting another to conceal the proceeds of criminal conduct; the acquisition, possession or use of the proceeds of crime; and a legal obligation to make a report to the financial intelligence unit (FIU) or police when it is known or suspected that another person is engaged in money laundering. Individuals found guilty of money laundering can be fined up to $100,000 or imprisoned for up to five years or both, or up to twenty years and/or an unlimited fine. Individuals found guilty of failing to disclose and/or tipping off can be fined up to $50,000 or imprisoned up to three years or up to ten years and/or an unlimited fine.

The Financial Transaction Reporting Act 2000 (FTRA) establishes customer due diligence “know your customer” (KYC) requirements. The FTRA requires the verification of identity of any customer before establishing a business relationship; transactions exceeding $15,000; structured transactions in the amount exceeding $15,000; when it is known or suspected a customer’s transaction is the proceeds of crime; doubt of customer’s identity; and transactions conducted on behalf of a third party. 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 were frozen.

The FTRA is limited to transactions involving cash and does not cover all occasional transactions. Financial institutions are not required to undertake customer due diligence measures when carrying out occasional transactions that are wire transfers. Enforceable requirements related to politically exposed persons (PEPs) are applicable only to banks and trust companies through the Central Bank's AML/CTF Guidelines. Non-enforceable provisions regarding PEPs were adopted by the Securities Commission's Guidelines and the Compliance Commission's Code of Practice. In December 2008, amendments were passed to the FTRA, the Securities Industry Act, the Financial Service and Corporate Providers Act, and the Financial Intelligence Unit Act to address these deficiencies and bring The Bahamas into compliance with international standards for customer due diligence. The amendments provide for the enforceability of the guidelines, codes, procedures, and rules issued by regulators other than the Central Bank.

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. 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. The FIU receives approximately 100-150 STRs annually; most are related to suspicions of fraud, corruption and drug trafficking. If money laundering or terrorist financing 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. Data on STRs received in 2008 was unavailable prior to the annual report published by FIU in early 2009.

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. The FIU plans to implement the National Strategy to Prevent Money Laundering in early 2009. 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.

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 2008, nearly $4 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 and UN Security Council Resolution 1373 and make provision for preventing and combating 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. The ATA was amended in 2008 to clarify aspects of the legislation and further comply with UN Conventions related to terrorist financing. In 2007, The Royal Bahamas Police Force established a Special Anti-Terrorism Unit to investigate cases of terrorism and terrorist financing.

The Royal Bahamas Police Force (RBPF) has cooperated with the U.S. Immigration and Customs Enforcement (ICE) in various financial investigations, including sharing of records and other financial data. In 2008, ICE obtained the cooperation of RBPF

officials with the identification of subjects and assets identified as relating to or generated by money laundering activities, particularly pertaining to the smuggling of bulk currency, a preferred method for drug dealers and other criminals to move illicit proceeds across international borders. Between January 2000 and September 2008, 17 individuals were charged with money laundering by the Royal Bahamas Police Force's T&F/MLIS, leading to seven convictions. Seven defendants await trial, while two defendants fled the jurisdiction prior to trial.

The Bahamas is a member of the Offshore Group of Banking Supervisors and the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body. 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 (MOUs) with other counterpart FIUs to exchange information.

The Bahamas is a party to the UN 1988 Drug Convention, and the UN International Convention for the Suppression of the Financing of Terrorism. In 2008, The Bahamas became a party to both the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. 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 Bahamas has a Mutual Legal Assistance Treaty (MLAT) with the United States, which entered into force in 1990, and agreements with the United Kingdom and Canada. Recently, several successful cases involving asset sharing have occurred between the United States and the Bahamas resulting in large amounts being shared by each government with the other.

The Government of the Commonwealth of The Bahamas should continue to enhance its anti-money laundering and counterterrorist financing regime by implementing the National Strategy on the Prevention of Money Laundering. It should also ensure that there is a public 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.

Bahrain

Bahrain is an important international financial center in the Gulf region. In contrast with its Gulf Cooperation Council (GCC) neighbors, Bahrain has a service based economy, with the financial sector providing more than 20 percent of GDP. It hosts a diverse group of financial institutions, including 195 banks, of which 57 are wholesale banks (formerly referred to as off-shore banks or OBUs); 46 investment banks; and 26 commercial banks, of which 19 are foreign-owned. There are 35 representative offices of international banks. Bahrain has 38 Islamic banks and financial institutions. There are 22 moneychangers and money brokers, and several other investment institutions, including 87 insurance companies. While Bahrain is not a major money laundering country, the greatest risk of money laundering stems from foreign proceeds that transit through the country. 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.

In January 2001, the Government of Bahrain (GOB) enacted an anti-money laundering law (AML) that criminalizes the laundering of proceeds derived from any predicate offense. The law stipulates 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.

The 2001 AML was amended in August 2006 by Law 54/2006, which 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. In June 2008, the government moved to increase supervision of its borders, by placing Ports and

Customs inspections under the Ministry of Interior. The Ministry of Interior subsequently instructed its officials to strictly enforce laws against the illegitimate movement of currency.

A controversial provision of Law 54 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 2001 AML law, the Bahrain Monetary Agency (BMA) was the principal financial sector regulator and de-facto central bank, issuing regulations and 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. Immunity from criminal or civil action is given to those who report suspicious transactions. Even prior to the enactment of Law 54, financial institutions were obligated to report suspicious transactions greater than 6,000 dinars (approximately $16,000) to the BMA/Central Bank. The current requirement for filing STRs stipulates no minimum thresholds and since 2005 the BMA/Central Bank 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 with the Central Bank of Bahrain (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 2001 AML 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 CBB.

In addition, the 2001 AML 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 suspicious transaction reports (STRs); 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 counterterrorist financing (AML/CTF) regulations, but it does not independently investigate the STRs as the 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 eight insurance companies in 2007 and had conducted eleven more inspections by October 2008. Additional insurance industry inspections are scheduled for 2009. 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 announced an increased focus on enforcement, including car dealers, jewelers, and real estate agencies noting 274 visits to DNFBPs in 2007, and 271 through October 2008. Of the 271 visits in 2008, 145 were assigned an MOIC compliance officer as a result. The MOIC has also increased its inspection team staff from seven to nine.

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 2008, the AMLU has received and investigated 201 STRs, 42 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 expatriate felons with sentences of one and three years and fines of $380 and $1900 respectively.

In October 2007 the government used the new AML/CTF law of 2006 to bring charges against five suspects. In January 2008, they were convicted of a range of charges, including the financing of terrorism. The five were sentenced to six months' imprisonment. In June 2008, authorities arrested two Bahrainis on charges of financing terrorism. The case remained pending as of December 2008.

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 September 2009.

There are 57 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 38 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 does not have a mutual legal assistance agreement with the United States. Bahrain is 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. Bahrain is not a party to the UN Convention against Corruption. 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. Bahrain hosts the Secretariat and is a member of the Middle East and North Africa Financial Action Task Force (MENFATF), a FATF-style regional body that was established 2004. In November 2006, MENAFATF approved the mutual evaluation report on Bahrain.

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. The AMLU 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. Supporting regulations should be enacted and enforced governing bulk cash smuggling. Bahrain should become a party to the UN Convention against Corruption.

Bangladesh

Bangladesh is not a regional or offshore financial center. Under the 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 $180 million in proceeds—a fraction of the estimated total amount of corrupt funds located both domestically and abroad. Fighting corruption is a keystone of the caretaker government under the state of emergency. 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 and $7.9 billion in fiscal year 2008. 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 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.

The Government of Bangladesh (GOB) realized that it did not have a mechanism to request assistance from other nations to help track illegal proceeds flowing overseas, some of which is related to corruption and capital flight. As a result, in February 2007 the GOB acceded to the UN Convention against Corruption (UNCAC). Pursuant to UNCAC, the GOB designated the Attorney General's Office as the central authority for mutual legal assistance requests. In August 2008, Bangladesh signed the South Asian Association for Regional Cooperation (SAARC) Convention on Mutual Assistance in Criminal Matters. Using UNCAC as the legal basis, the government has so far sent Mutual Legal Assistance Requests on tracing, freezing and seizure to foreign jurisdictions.

In April and June 2008 the government promulgated the Money Laundering Prevention Ordinance (MLPO 2008) and the Anti-Terrorism Ordinance (ATO 2008). The laws facilitate international cooperation in recovering money illegally transferred to foreign countries and mutual legal assistance in terms of criminal investigation, trial proceedings, and extradition matters. The GOB has formed a national level committee headed by the Law Adviser and an inter-agency Task Force headed by the Governor of the CB to retrieve illegally transferred money.

For the past twenty years, corrupt practices became so common that, between 2001 and 2005, Transparency International ranked Bangladesh in its Corruption Perception Index as the country with the highest level of perceived corruption in the world. In 2008, Bangladesh was ranked 147 out of 180 countries surveyed. 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. The GOB does not place a limit on how much currency can be brought into the country, but amounts over $5,000 must be declared

within 30 days. The Customs Bureau is primarily a revenue collection agency, accounting for 40-50 percent of Bangladesh's annual government income.

The MLPO of 2008 introduced a new set of financial organizations that must report to the CB regarding their activities in a manner similar to that of banks and financial institutions. These reporting organizations (ROs) include insurance companies, money changers and remitters, fund-transfer companies or organizations, and companies permitted to operate as business organizations under the CB's authority. The CB also has the right to notify other organizations that they must function as ROs for purposes of the MLPO of 2008. The inclusion of these new ROs pose new regulatory and oversight challenges for the CB's Anti-Money Laundering Department (AMLD) In addition, the GOB regulates insurance companies and money changers and remitters under the Foreign Exchange Regulation Act (FERA), 1947.

The CB regularly conducts training, conferences and seminars for the staff and officers of 48 commercial banks around the country regarding "know your customer" procedures. The CB carries out additional training focusing on identifying suspicious and cash transactions and reporting them to the CB, where the country's financial intelligence unit (FIU) is located.

In May 2007, the GOB identified the CB's AMLD as Bangladesh's financial intelligence unit (FIU). The MPLO of 2008 officially established the existence of the FIU. The FIU depends on the CB for its operation and budget. The CB enjoys complete operational and budgetary independence. An Executive Director of the CB heads the FIU, which consists of approximately 25 officials.

The MLPO of 2008 allows the FIU to enter into agreements and arrangements with foreign FIUs to receive and request information in relation to money laundering offenses or suspicious transactions. In August 2008, the FIU signed its first Memorandum of Understanding (MOU) with the Malaysia's FIU to facilitate the exchange of information on money laundering, terrorism financing, and related criminal activity. In October 2008, the FIU signed its second MOU with the Nepal's FIU. The FIU is negotiating similar agreements with other counterparts. However, many counterparts require that the Bangladesh FIU be a member of the international association of FIUs, the EGMONT Group, before negotiating MOUs with Bangladesh.

The recently enacted ordinances, MLPO 2008 and ATO 2008, enhance the powers and responsibilities of the CB and its FIU in many ways. The CB is empowered and authorized to analyze suspicious transaction reports (STRs) and cash transaction reports (CTRs) and maintain a financial intelligence database and related information. In September 2007, the Cash Transaction Report (CTR) threshold increased from 500,000 to 700,000 takas (approximately $10,250). The CB may call for and receive from ROs any information related to transactions where there are reasonable grounds to suspect the transaction involves money laundering and/or terrorist financing. The CB can direct ROs to take measure to combat money laundering and terrorist financing activities. Overall, the CB can monitor and observe the activities of banks as well as nonbanking institutions. The CB can, if necessary, conduct on-site inspection of ROs. Finally, the CB can arrange training, conferences and seminars for all ROs. The FIU spearheads national efforts and promotes national awareness in detecting and preventing money laundering and terrorism financing.

The new ordinances allows the CB, without a court order, to order any bank or financial institution to suspend a transaction or freeze an account for a period of 30 days when there are reasonable grounds to suspect that a transaction involves the proceeds of a crime. The CB may extend such orders for an additional 30 days for the purpose of further investigation. The CB is authorized to have access to the information of bank accounts of any individual or company on demand without a court order if the CB has reasonable grounds to suspect that a transaction involves the proceeds of a crime.

The MLPO of 2008 designates the Anti-Corruption Commission (ACC), established pursuant to the Anti-Corruption Commission Act, 2004, as the national Investigating Organization (IO) regarding money laundering matters. Any official empowered to act on behalf of ACC may be considered part of the IO. The Bangladesh police are in charge of investigating crimes under ATO 2008. Under separate authorities, the National Board of Revenue (NBR), the country's tax authority, is allowed to freeze an account without a court order for tax purposes only. Under the MLPO of 2008, on an application of the IO, a court may pass a freezing or attachment order on the property of the accused, situated within or outside Bangladesh, in which the people of the state

have interest. The law allows for only conviction based forfeiture against the property connected to the crime.

The ACC is not adequately staffed and trained to handle money laundering investigations. Media accounts and discussions with ACC staff indicate that the ACC has largely confined itself to gathering records of the assets of corruption suspects and using them to pursue less complicated criminal cases. The offense of "Amassing wealth through illegal means beyond known source of income" is a typical charge brought against suspects investigated by the ACC. The MLPO of 2008 requires the ACC prove one of the designated predicate offenses in order to successfully prosecute the crime of money laundering. The MLPO of 2008 lists 16 predicate offenses, including corruption and bribery; counterfeiting currency or documents; extortion; fraud; forgery; and illicit trafficking in persons or arms or narcotic drugs and psychotropic substances. Under the prior money laundering law (MLPA 2002), the ACC was not required to prove a predicate offense. The money laundering prosecutions currently pending have been carried out pursuant to MLPA 2002.

Following passage of MLPA 2002, the GOB made the now defunct Bureau of Anti-Corruption (BAC) responsible for taking legal steps regarding money laundering crimes. Between 2002 and 2004, BAC filed 35 cases for money laundering. The ACC had no jurisdiction to initiate legal steps on money laundering charges until the middle of 2007, when the offence was included in the ACC Act 2004.

In recent years, Bangladesh law enforcement has made little progress in pursuing money laundering investigations, in part due to difficulties in procedure and inter-agency cooperation. A major setback occurred in December 2005 when the newly created ACC advised the CB that it would not investigate money laundering cases and returned them to the CB. As a result, the Criminal Investigation Division of the national police force agreed to investigate the cases. During 2006, the CB and police hammered out a procedure to pursue investigations initiated through suspicious transactions reports. The State of Emergency in 2007 brought a differently-configured law enforcement regime headed by military officers. The government set up ten fast-track courts to try graft suspects. As of October 2008, the ACC and the NBR had filed 244 cases in the fast-track courts. Of those cases, the court delivered verdicts in 122 cases. Most of the remaining cases were stayed at different stages by the Supreme

Court. The court stayed some cases before charge framing, some after charge framing, and others just before the delivery of verdict. When verdicts were delivered, the court passed confiscation and forfeiture orders in most cases. The ACC has so far won two money laundering cases in 2008. Both cases were tried under MLPA 2002. In October 2008, the International Criminal Police Organization (Interpol) detected laundered money deposited with a Hong Kong bank by a former BNP minister and his son. ACC is currently working on the case.

Bangladesh authorities have not yet tried any cases under the newly enacted ATO 2008. According to published media reports, the trials of Jama'atul Mujahideen Bangladesh (JMB) members responsible for staging over 400 bombings around Bangladesh in August 2005 were mostly conducted under the Arms Act 1878 and the Explosive Substances Act 1908. As of August 2008, the Bangladesh courts completed 77 trials, during which 271 JMB leaders and activists were convicted. As a result, the courts have awarded 41 death sentences, 98 terms of life imprisonment and 132 different other jail terms. Intelligence officials told news media that 72 persons were acquitted in the cases, as allegations against them were not proved.

The ATO of 2008 authorizes the filing of STRs related to terrorist finance, empowers the CB to monitor suspect financial transactions related to terror finance and prohibits a person from enjoying or possessing property or proceeds of terrorist activity. Property or proceeds of terrorist activity, which is in the possession of a terrorist or a person who is or is not an accused or convicted under the provisions of the ordinance, is liable to be confiscated and forfeited in favor of the government. A judge may pass an order of forfeiture/seizure of proceeds of terrorist activity if he or she is satisfied that such property was seized or confiscated because of its terrorist-related nature.

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.

Since the Money Laundering Prevention Act (MLPA) was enacted in 2002, the Central Bank has received approximately 483 STRs. Between April and October 2008, ROs submitted 23 STRs to the CB. 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, Bangladesh became a party to the UN International Convention for the Suppression of the Financing of Terrorism. Bangladesh is also a party to the 1988 UN Drug Convention and the UN Convention against Corruption. Bangladesh is not a signatory to the Convention against Transnational Organized Crime.

Bangladesh is a member of the Asia-Pacific Group (APG), a Financial Action Task Force-style regional body. In August 2008, a regional team of experts visited Bangladesh as part of APG's mutual evaluation of the country's safeguards against money laundering and terrorism financing. Earlier in 2008, the GOB formed a National Coordination Committee and a Working Level Committee to prepare for the visit. In the coming year, Bangladesh will face the twin challenges of successfully completing the evaluation and implementing the recommendations of the APG. The GOB has expressed interest in membership in the EGMONT Group, signing MOUs with other FIUs for intelligence gathering and sharing purposes, effectively analyzing and employing STRs/CTRs, and establishing an effective inter-agency working relationship with national stakeholders (law enforcement, regulators and other authorities).

Although positive legislation has been passed and 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. The GOB should support technology enhancements to reporting channels from outlying districts

to the Central Bank. While the FIU is growing steadily, the FIU analysts and investigators need to enhance their ability to conduct analysis, investigations, understand money laundering and terror finance methodologies and guide the ROs. Bangladesh law enforcement and customs should examine forms of trade-based money laundering and initiate money laundering and financial crimes investigations at the "street level" instead of waiting for a STR to be filed with the FIU. 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

Barbados remains vulnerable to money laundering, which primarily occurs in the formal banking system. Domestically, money laundering is largely drug-related and appears to be derived from the trafficking of cocaine and marijuana, as Barbados is a transit country for illicit narcotics. 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 October 2008, there are six commercial banks in Barbados. The offshore sector includes 3,334 international business companies (IBCs), compared to 3,615 in 2007,163 exempt insurance companies and 65 qualified exempt insurance companies, five mutual funds companies and one exempt mutual fund company, seven trust companies, five finance companies, and 57 offshore banks. There are no free trade zones and no domestic or 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 enhances 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 (AML) policy documents and analyzing prudential returns. Additionally, permission must be obtained from the Central Bank to move currency abroad.

The Government of Barbados (GOB) criminalizes 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 extend 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 $1,000,000. 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. Customer due diligence measures include customer identification and due diligence; beneficial ownership requirements; and, enhanced due diligence for new technologies and correspondent banking, and for high risk customers such as politically exposed persons and non-face-to-face customers. Financial institutions are required to conduct on-going due diligence on business relationships engaging in exchanges of $10,000 or more, and all instructions for international funds transfers of $10,000 or those transiting Barbados. Financial institutions must also report suspicious transactions to the Anti-Money Laundering Authority (AMLA). Tipping off is prohibited.

In 2007, the Central Bank revised the AML guidelines for licensed financial institutions to reflect a risk-based approach, and to include guidance on how licensees can fulfill their obligations in relation to combating terrorist financing. The guidelines apply to all entities that are incorporated in Barbados and are licensed under the Financial Institutions Act 1996 (FIA) and the IFSA. The Central Bank conducts off-site surveillance and undertakes regular on-site examinations of licensees to assess compliance with AML legislation and regulations. Licenses can be revoked by the Minister of Finance for noncompliance. In 2008, the GOB announced its intentions to consolidate regulatory functions into a single agency (except for the Central Bank) to enhance supervision. The proposed Financial Services Commission (FSC) will include: the Office of the Registrar of Co-operatives and Friendly Societies; the Office of Supervisor of Insurance and Pensions; the Securities Commission; and the regulatory and supervisory functions of the office of the Director of International Business. The FSC will regulate nonbanking activities including insurance, pensions, credit unions, securities and mutual funds.

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 activity reports (SARs) from financial institutions; instructing financial institutions to take steps to facilitate an investigation; and, conducting awareness training in regard to record keeping 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 or 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. Between January 1, 2008 and June 30, 2008, the FIU had received 76 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 the FIU. The Royal Barbados Police Force pursues all potential prosecutions.

Barbados has a cross-border reporting system for all persons carrying BDS 10,000 (approximately $5,000) entering and leaving Barbados. Customs has the ability to share information on declarations and seizures with domestic and foreign counterparts. It should be noted that suspicion of money laundering, terrorist financing, or making a false declaration does not provide a basis for stopping and seizure of currency and negotiable instruments. The Money Laundering Financing of Terrorism (Prevention and Control) Act (MLFTA) contains provisions to control bulk cash smuggling and the use of cash couriers.

The MLPCA provides 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 MLFTA, criminalizes the financing of terrorism. 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. However, there is no requirement to freeze terrorist funds or other assets of persons designated by the UN al-Qaida and Taliban Sanctions Committee. In 2008, 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 the 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 Barbados entered into force in 2000.

Barbados is a member of the Caribbean Financial Action Task Force (CFATF), a Financial Action Task Force-style regional body, and underwent a mutual evaluation in December 2006, which was finalized in 2008. The evaluation noted deficiencies in the areas of record keeping; designated nonfinancial businesses and professions (DNFBPs); special attention for higher risk countries; and AML requirements for money/value transfer services. Barbados also 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 Convention for the Suppression of the Financing of Terrorism. Barbados has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

The Government of Barbados has taken a number of steps in recent years to strengthen its anti-money laundering and counterterrorist 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 devote sufficient resources to ensure the FIU, law enforcement, supervisory agencies, and prosecutorial authorities are properly staffed and have the capacity to perform their duties. The GOB should amend its legislation to allow for the seizure of suspected illegal funds at the border and to allow the freezing of funds or assets linked to terrorist financing, al-Qaida or the Taliban. Barbados should consider the adoption of civil forfeiture and asset sharing legislation. Supervision of nonprofit organizations, charities, DNFBPs, and money transfer services should be strengthened, as should information sharing between regulatory and enforcement agencies. Finally, to further enhance its legal framework against money laundering, Barbados should move expeditiously to become a party to 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. Corruption (including embezzlement through abuse of office, taking bribes, and general abuses of power or office) and illegal narcotics trafficking are primary sources of illicit proceeds. 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 January 1, 2008, 27 banks with 368

branches comprised the banking sector. Of these, 23 were banks with foreign capital, including 7 banks with 100 percent foreign capital. 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. Banks and branches have separate business units such as payment processing centers, banking service centers, and foreign exchange offices. 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. Nonbank financial credit institutions have gradually closed, due to money laundering concerns and other factors.

Based on a 1996 Presidential Decree, Belarus has established one free economic zone (FEZ) in each of Belarus' six regions. 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.

Officials have reported several cases of attempts to smuggle undeclared cash across borders. 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. However, the declaration system was not designed, nor is it used to detect the physical cross-border movement of currency and bearer negotiable instruments to prevent and interdict bulk cash smuggling for money laundering and terrorist financing purposes. Individuals may import or export securities certificates

denominated in foreign currencies and payment instruments in foreign currencies without any limitations on the amount, and without the need to declare them in writing to the customs authorities. Customs authorities do not store information on declarations that they consider suspicious and are unable to apply sanctions against persons moving funds cross-border on the basis of suspicion of money laundering or terrorist financing.

The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), a Financial Action Task Force (FATF)-style regional body, evaluated the anti-money laundering and counterterrorist financing (AML/CTF) regime of Belarus in July 2008. The EAG adopted the mutual evaluation report (MER) at the December 2008 plenary meeting. The major deficiencies outlined in the MER focused on the lack of adequate customer due diligence (CDD) requirements, including allowing electronic cash accounts in fictitious names , no clear requirement to perform CDD on establishing business relations with a customer in the banking, insurance and securities sectors; no requirement for CDD for legal entities below ($300,000) threshold; no affirmative obligation to identify beneficial ownership in the banking sector, and no beneficial ownership or ongoing monitoring requirements for other sectors; and lack of effective regulation and supervision for correspondent accounts and designated nonfinancial businesses and professions (DNFBPs); inadequate record keeping requirements; inadequate wire transfer identifier requirements; and shortcomings in the Belarusian cross-border cash declaration regime.

By law, only licensed banks and the postal service can conduct money transfers. The government does not acknowledge alternative remittance systems and allows currency exchange only through licensed currency exchange kiosks. The Department of Humanitarian Assistance in the Presidential Administration has registered all charities. Presidential Decree 24, passed in 2003, requires all organizations and individuals receiving charity assistance, including assistance provided by foreign states, international organizations and individuals, to open charity accounts in a local bank.

Belarus' "Law on Measures to Prevent the Laundering of Illegally Acquired Proceeds" (AML Law), adopted in 2000 and amended in 2005, establishes the legal and organizational framework to prevent money laundering and terrorist financing. The

AML/CTF law does not fully incorporate the requirements of the Vienna and Palermo Conventions (e.g., acquisition possession or use are not covered, nor are indirect proceeds). Belarus criminalizes self-laundering, but restricts the self-laundering offense to cases that involve using the illicit proceeds to carry out entrepreneurial or other business activities. Belarus also criminalizes the financing of terrorism. Although Belarus has adopted an all crimes approach to money laundering predicates, with some exceptions for tax evasion crimes, it does not criminalize insider trading and market manipulation, and therefore does not meet FATF requirements for the minimum list of predicate offenses. A money laundering conviction does not require conviction of the predicate offense. Legal entities are not criminally liable and there also is no administrative liability of r legal entities for money laundering. However, if a legal entity aids an organized group or criminal organization or is created with funds of an organized group or criminal group, it can be liquidated by the Supreme Court of Belarus and its assets seized by the state. The criminal code provides adequate sanctions for individuals convicted of money laundering, including fines and incarceration for two-1- years. The law defines “illegally acquired proceeds” as currency, securities or other assets, including real and intellectual property rights, obtained in violation of the law.

Financial institutions are obligated to report suspicious transactions regardless of value, and large value transactions, for which the reporting threshold for individual financial transactions is approximately $27,000 and for corporate transactions is approximately $270,000. In Belarus, these reporting obligations attach to transfers that are subject to special monitoring. Specifically, transactions subject to special monitoring include: 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 transactions exceeding the currency reporting threshold that involve cash, property, securities, loans or remittances. Financial institutions conducting such transfers are required to disclose to the FIU—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. 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. 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 reporting requirements (extraordinary inspection). The government has used the AML Law as a pretext for preventing several pro-democracy NGOs from receiving foreign assistance.

The AML Law authorizes the following government bodies to monitor financial transactions for the purpose of preventing money laundering: the State Control Committee (SCC); 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. Under the 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.

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. However, casinos do not need to address AML/CTF issues before receiving operating licenses, and the system for supervising and applying sanctions for noncompliance with AML/CTF requirements is not effective. Belarus has similar shortcomings with the other DNFBPs: there is little effective monitoring for compliance with AML/CTF measures for most of these sectors, and accountants lack a supervisory agency—even a self-regulating organization—so they completely lack supervision and monitoring altogether. Across sectors, there is no clear customer identification requirement for DNFBPs at the establishment of the business relationship, there are no beneficial ownership identification requirements, and exceptions in the reporting requirements

mean that there may be times that DNFBPs do not perform client identification measures even when they suspect the client of involvement in money laundering or terrorist financing. These sectors also lack the legal obligation to execute enhanced CDD measures for high-risk clients. Likewise, Belarus has no requirements for these sectors to obtain information from the customer regarding his or her source of funds or the expected purpose of the business relationship. The MER notes an overall lack of implementation across these sectors, in particular, the absence of effectiveness in the gaming sector, as well as with regard to dealers in precious metals and stones.

In 2003, Belarus established the DFM as its financial intelligence unit (FIU). Although it is an autonomous unit within the State Control Committee of Belarus with the rights of a legal entity, it does not have an independent budget and cannot independently hire staff. 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 since 2007 it is a member of the Egmont Group. The DFM also has the authority to initiate its own investigations. In 2007 the DFM received and analyzed 269,701 suspicious transaction reports (STRs) and forwarded 2,088 reports to law enforcement and control authorities.

The DFM has noted that there is increased interest by law enforcement in the FIU's work. Belarusian legislation provides for broad seizure powers for law enforcement to identify and trace assets. The Criminal Code provides for asset forfeiture 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.

Belarus has focused on targets beyond money laundering. In June 2007 Parliament passed Criminal Code amendments to toughen penalties for various offenses 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 has made an effort to ensure cooperation and coordination between state bodies through the Interdepartmental Working Group established specifically to address 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.

Terrorism is a crime in Belarus and 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. Article 290-1 of the Criminal Code explicitly criminalizes terrorist financing. However, the law does not criminalize indirect provision of money for purposes of terrorist financing and does not criminalize provision of funds for a terrorist organization or an individual terrorist, if the funds are not intended for a specific act of terrorism. The Criminal Code also does not criminalize the financing of theft of nuclear materials for terrorist purposes. Legal entities are not criminally liable for terrorist financing, but organizations engaged in the financing of terrorism may be liquidated by decision of the Supreme Court upon indictment by the General Prosecutor. In December 2005, the Parliament amended the Criminal Code to stiffen the penalty for 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.

Belarus does not have an adequate system in place to freeze without delay terrorist assets. The AML/CTF (Article 5) requires financial institutions and DNFBPs to suspend a financial transaction if one of its participants is a person suspected of being involved in terrorist activities or controlled by terrorists. The National Bank provides banks with

the State Security Committee's lists of persons suspected of being involved in terrorist activities or controlled by persons engaged in terrorism—including persons on the United Nations Security Council Resolution (UNSCR) 1267 Sanctions Committee's consolidated list—and has given banks and nonbank credit institutions an instruction on the procedure for freezing funds. DNFBPs do not receive the terrorism lists and have little awareness of freezing requirements. In addition, the AML/CTF law (Article 11) also authorizes the Financial Monitoring Department to suspend a transaction for up to five days, after which time it must decide either to report the information to law enforcement, which can attach the funds, or resume the transactions. 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. Belarus has no procedures in place for reviewing requests to remove persons from the list or for unfreezing the funds of persons to whom the freezing mechanism was accidentally applied.

Belarus is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. 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. The United States and Belarus do not have a mutual legal assistance agreement in place. Belarus is a member of the EAG. The DFM is a member of the Egmont Group. Belarus is ranked number 151 out of 180 territories listed in Transparency International's 2008 International Corruption Perception Index.

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 further amended to comport with international standards and to provide for more transparency and accountability. The GOB should,

for example, extend 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 also bring the nonfinancial sectors under the same AML/CTF requirements that it imposes on the financial sector, and ensure resources for supervision, monitoring and a sanctions regime for noncompliance. 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

Belgium's banking industry is of medium size, with assets of over $2 trillion dollars in 2008. Illicit funds, formerly consisting mostly of narcotics-trafficking proceeds, now derive mainly from financial fraud, including tax fraud. Other noteworthy predicate offenses include trafficking in persons and in diamonds, due to Belgium's active diamond industry, as well as in other goods. Authorities note that criminals are increasing their use of remittance transactions and shell companies, and misuse of the nonfinancial sectors, in particular lawyers, real estate and nonprofit organizations to launder money.

Strong legislative and oversight provisions are in place in the formal financial sector to combat money laundering and terrorist financing. Belgium criminalized money laundering with the Law of 11 January 1993, On Preventing Use of the Financial

System for Purposes of Money Laundering. Additional laws expanded the scope of the legislation: the Law of 22 March 1993, On the Legal Status and Supervision of Credit Institutions; and the Law of 6 April 1995, On Secondary Markets, On Legal Status and Supervision of Investment Firms, On Intermediaries and Investment Advisors. These laws mandate the customer due diligence and reporting requirements that apply to banks and the formal financial sector as well as nonfinancial businesses and professions, including estate agents, private security firms, funds transporters, diamond merchants, notaries, bailiffs, auditors, chartered accountants, tax advisors, certified accountants, surveyors and casinos. Article 505 of the Penal Code sets penalties of up to five years of imprisonment for money laundering convictions. Any unlawful activity may serve as the predicate offense.

The Law of 12 January 2004 amended Belgian domestic legislation by making it applicable to attorneys and broadening the scope of money laundering predicate offenses beyond drug trafficking to include the financing of terrorist acts or organizations. The Belgian bar association challenged this law and brought it to the Court of Arbitration, which referred the challenge to the European Court of Justice. The bar argued that the Second EU Directive, which served as the basis for this law, violates the right to a fair trial, because the reporting obligations prejudice lawyers against fully and independently representing their clients. In October 2008, the European Commission referred Belgium to the European Court of Justice over non-implementation of the Third Money Laundering Directive, which requires members to update their AML regimes to comport with the most up-to-date standards, particularly with regard to regulation and terrorism financing.

Belgium is currently working to address the deficiencies described in the 2005 Financial Action Task Force (FATF) mutual evaluation report (MER), including due diligence and regulation requirements for designated nonfinancial businesses and professions, 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.

Authorities believe that 3,500 phone shops—small businesses where customers can make inexpensive phone calls and access the internet—may be operating in Belgium. Only an estimated one-quarter of these shops are formally licensed, 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. Since 2004, Belgian police made a series of raids on "phone shops." In some phone shops, authorities uncovered money laundering operations and hawala-type banking activities. In 2006 and 2007 raids in some locations uncovered numerous counterfeit phone cards in addition to evidence of money laundering activities. Authorities have closed more than 200 such shops since 2004, and estimate that the Belgian state loses up to $256 million in 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. In 2007, the cities of Antwerp and Gent also increased enforcement activities against such phone shops.

Despite some diffusion in recent years, Belgium continues as the world's diamond-trading center. Fully 90 percent of the world's crude diamonds and 50 percent of cut diamonds pass through Belgium. 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. The Kimberley certification process has introduced much-needed transparency into the global diamond trade. A regulation approved by a Royal Decree dated October 22, 2006 contains a detailed description of the obligations that diamond dealers must observe. This regulation primarily deals with the different aspects of the client's identification, including the identification of 'non-face-to-face' operations and of the beneficial owner, customer due diligence and obligations regarding the internal organization. Belgium's robust diamond industry presents special challenges for law enforcement, but authorities have transmitted a number of cases relating to diamonds to the public prosecutor, and they monitor the sector closely in cooperation with local police and diamond industry officials.

The Belgian financial institutions are supervised by the Belgian Banking and Finance Commission (CBFA) supervises financial institutions, 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.

Financial institutions must comply with “know your customer” principles, regardless of 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 $12,500) as well as retain records of suspicious transactions reported to the FIU for at least five years.

Financial institutions or other entities with reporting requirements are liable for illegal activities occurring under their control. Financial institutions must train their personnel in the detection and handling of suspicious transactions that could be linked to money laundering. Failure to comply with the anti-money laundering legislation, including failure to report, carries a fine of up to $1.72 million.

Money laundering legislation imposes restrictions on cash payments for real estate. Purchasers may not use cash for amounts exceeding 10 percent of the purchase price or approximately $18,750, whichever is lower. Cash payments over $25,000 for goods are also illegal.

Belgium had long permitted the issuance of bearer bonds (“titres au porteur”), widely used to transfer wealth between generations and to avoid taxes. As of January 1, 2008, companies may no longer issues bearer bonds, although bearer bonds issued before that date are still valid, as are non-Belgian bearer bonds. Bearer shares are permitted for individuals as well as for banks and companies.

In Belgium, the Royal decree of 5 October 2006 on measures to control cross-border transportation of cash came into force on June 15, 2007. The Royal decree stipulates the obligation to declare transportation of currency worth 10,000 euros or more in cash entering or leaving the EU/Belgium.

In cases of a failure to declare, or if there is a suspicion that the cash declared originates from illegal activities or is intended to finance such activities, the Belgian Customs and Excise administration will confiscate the cash for up to 14 days and send a report to the financial intelligence unit (FIU). The FIU examines all the declarations submitted and Customs reports filed. Since June 2007, Belgian Customs has received information about 4.5 million euros in cash passing through Zaventem International airport. To date, Belgian Customs has confiscated 670,000 euros and filed 196 reports with the FIU.

Belgian officials are working to increase transparency in the nonprofit sector through better enforcement of registration and reporting procedures. Nonprofit organizations must register, furnish copies of their statutes and membership lists, provide minutes from council meetings, and file budget reports.

The Belgian financial intelligence unit, known in French as the Cellule de Traitement des Informations Financières and in Flemish as Cel voor Financiële Informatieverwerking (CTIF-CFI), was created by a Royal Decree issued on June 11, 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 (STRs) submitted by obliged 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. Employees and representatives of institutions who report transactions to CTIF-CFI in good faith are exempt from civil, penal, or disciplinary actions. 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 also been very active in

analyzing the diamond industry and working to eliminate its potential for money laundering and terrorist financing.

The FIU is composed of financial experts, including three magistrates (public prosecutors), appointed by the King, who serve six-year renewable terms. A magistrate presides over the body. In addition to administrative and legal support, the investigative department consists of inspectors/analysts. There are also liaisons that maintain contact with the various law enforcement agencies in Belgium, including three police officers, one customs officer, and one officer of the Belgian intelligence service.

From its founding in 1993 until the end of 2007, CTIF-CFI received 127,293 disclosures and opened a total of 30,223 individual case files (numerous disclosures may be linked to a single case). Of these, the FIU has transmitted 8,310 cases to the public prosecutor aggregating approximately $16.5 billion. In 2007, the FIU received 12,830 disclosures, opened 4,927 new cases, and transmitted 1,166 cases to the public prosecutor, up from 912 cases transmitted in 2006. Reports from credit institutions comprise about 81 percent of disclosures on files transmitted to the federal prosecutor. Foreign exchange offices and foreign counterpart units accounted for an additional 12 percent of the files transmitted, with notaries, casinos, and other entities also reporting. The files concerning serious and organized tax fraud represented 36.7 percent of the total number of cases in 2007, while cases regarding terrorism and terrorist finance represent 7 percent of the total amount (up from 6 percent in 2006). Belgian statistics show that from the start of its activities until the end of 2007, the FIU reported 175 cases regarding terrorism or terrorist financing to the judicial authorities. Thirty-two of theses cases were reported in 2007.

Since the creation of CTIF-CFI in 1993, Belgian courts and tribunals have pronounced sentences in at least 1,046 of the 8,310 cases transmitted to the Federal Prosecutor (some of these convictions are still under appeal). From 1993-2007, the conviction rate was 11.4 percent. To date, Belgian courts have convicted 2,060 individuals for money laundering on the basis of cases forwarded by the FIU, yielding combined total sentences of 3,568 years. Although five years imprisonment 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. The cumulative fines

levied for money laundering total approximately $91 million. Belgian authorities have confiscated more than $788 million connected with money laundering crimes. The majority of convictions related to money laundering are based upon disclosures made by the financial institutions and others to CTIF-CFI.

As with Belgium's FIU, the federal police must 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, and 28 percent involved narcotics. The federal police established a special bureau to combat VAT fraud shortly after 2001, when estimates of lost revenue topped $1.4 billion. In 2007, 57.3 percent of all cases reported to the Public Prosecutor involved VAT carousel fraud. 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. According to the FATF MER, prosecutorial authorities have the necessary power to carry out their functions; however, in places or at times, the prosecutors and police seem to lack resources to properly perform their AML/CTF duties.

Belgium has created a sophisticated and comprehensive confiscation and seizure regime, encompassing the Central Office for Seizure and Confiscation (COSC), operating under the auspices of the Ministry of Justice. The COSC ensures that authorities execute confiscations and seizures smoothly and efficiently in accordance with the law. Belgian law requires a judicial order to execute confiscations and seizures, and allows civil as well as criminal forfeiture of assets. A law passed in July 2006 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.

Seizures in Belgium can be direct or indirect. Direct seizures involve the seizure of items linked directly to a crime. Indirect seizures are "seizures by equivalence," usually of homes, cars, jewels and other items not directly linked to the crime in question. Belgian authorities attempt to sell confiscated items such as cars, computers, and cell phones soon after confiscation in order to minimize the loss of the

market value of the goods over time. If a suspect is later found innocent, he or she receives the cash equivalent of the item(s) sold, plus accrued interest. Money from seizures and from the sale of seized goods is deposited in the Belgian Treasury. 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. Belgium has a verification program to check legal records of suspects to whom the authorities will return seized assets. If the person owes taxes or has overdue fines, COSC can ensure that the Belgian government is paid before proceeds are returned. According the COSC, information concerning the value of seizures is not available publicly.

In January 2004, the Belgian legislature passed domestic legislation criminalizing terrorist acts and material support (including financial support) for terrorist acts, allowing judicial freezes on terrorist assets. The law implemented eight of FATF's Special Recommendations, including prohibiting the provision of material support to terrorists groups by nonprofit organizations. Article 140 of the Penal Code criminalizes participation in the activity of a terrorist group, and Article 141 criminalizes the provision of material resources, including financial assistance, to terrorist groups and carries a penalty of five to ten years' imprisonment.

Under Belgium's 1993 anti-money laundering and counterterrorist finance (AML/CTF) law (amended in 2004), 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 in order to complete its analysis. If criminal evidence exists, the FIU forwards the case to the public prosecutor. In 2006, CTIF-CFI temporarily froze assets in 41 cases, representing approximately $220 million. To date, there are no figures for 2007 or 2008.

Under the January 2004 law, the Ministry of Justice can freeze assets related to terrorist crimes. However, in order for an act to constitute a criminal offense, authorities must demonstrate that the support was given with the knowledge that it would contribute to the commission of a crime by the terrorist group. Since the law does not establish a national capacity for designating foreign terrorist organizations,

authorities must demonstrate in each case that the group that was lent support actually constitutes a terrorist group.

In Belgium, the Ministry of Finance can administratively freeze assets of individuals and entities associated with al-Qaeda, the Taliban and Usama Bin Laden on the United Nations 1267 Sanctions Committee's consolidated list and/or those covered by an EU asset freeze regulation. Seized assets are transferred to the Ministry of Finance. If an entity appears on the UN 1267 Sanctions Committee's consolidated list, the GOB can pass a ministerial decree to freeze assets in order 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.

CTIF-CFI was a founding member of the Egmont Group and headed the Secretariat from 2005 to 2006. Belgium's FIU shares information with its European colleagues. Belgium is also a cooperative and reliable partner in law enforcement efforts. The federal police enjoy good cross-border cooperation with other police and investigative services in neighboring countries. Belgium does not require an international treaty as a prerequisite to lending mutual assistance in criminal cases.

Belgium 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. Belgium also ratified the UN Convention against Corruption in September 2008. A mutual legal assistance treaty (MLAT) between Belgium and the United States has been in force since 2000. Belgium and the United States have since signed a bilateral instruments amending and supplementing this treaty, in implementation of the U.S.-EU Extradition and Mutual Legal Assistance Agreements.

The Government of Belgium's (GOB's) continuing work implementing the FATF recommendations complements an already solid anti-money laundering regime and a clear official commitment to fighting against financial crimes, including the financing of terrorism. Belgium should also prohibit all bearer shares. 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. Belgium should

continue its efforts to uncover, investigate, and prosecute illegal banking operations, as well as the informal financial sector and nonbank financial institutions. The GOB should strengthen enforcement of reporting requirements by some nonfinancial entities in Belgium, in particular lawyers and notaries. 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 that are vulnerable to money laundering. Belize has pegged the Belizean dollar to the U.S. dollar and continues to offer financial and corporate services to nonresidents in its offshore financial sector. Belizean officials suspect that money laundering occurs primarily within that sector. Money laundering, primarily related to narcotics trafficking, and contraband smuggling, is suspected to occur through onshore banks operating in Belize. There is no evidence to indicate that money laundering proceeds are primarily controlled by local drug trafficking organizations organized criminals or terrorist groups. The vulnerability created by the government's lack of supervision of its offshore sector is exacerbated by its the lack of supervision of the gaming sector, including Internet gaming facilities, and the refusal of the Government of Belize (GPB) to fund its financial intelligence unit.

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, all offshore banks must be licensed by the Central Bank and be registered with the international business companies (IBCs) registry. 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 nominee directors.

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. Neither offshore banks nor onshore banks are permitted to issue bearer shares. Only the Central Bank of Belize and authorized dealers/depositories (i.e., commercial banks and casas de cambio) may deal in foreign currencies. Local money exchange houses, which were suspected of money laundering, were closed effective July 2005. Internet gaming is regulated by a Gaming Control Board, which is guided by the Gaming Control Act. There is one licensed internet gaming site, but there are an undisclosed number of Internet gaming sites illegally operating from within the country. Reportedly, there are no offshore casinos.

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 nonbanking sector for the provision of international financial services. 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., formerly primarily engaged in internet gaming, was sold to Belize Telemedia Limited and is now International Communications and Services Limited. It is designated as an Export Processing Zone (EPZ) and is regulated in accordance with the EPZ Act. There are presently 59 EPZ's in Belize. 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. The incidents involving developments in the CFZ have largely been related to counterfeit goods and more recently, pharmaceuticals such as ephedrine and pseudo-ephedrine.

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, and these systems have not yet been deterred through fines or criminal prosecution. Belizean customs authorities monitor such activities at the borders with Mexico and Guatemala; however, no domestic investigations have been undertaken.

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 counterterrorist 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 counterterrorist financing requirements. Government of Belize (GOB) officials have reported an increase in financial crimes, such as bank fraud, cashing of forged checks, suspicious transactions, and counterfeit Belizean and United States currency. The Central Bank of Belize continues to engage in public awareness activities and conduct training sessions related to 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 have bank secrecy legislation that prevents disclosure of client and ownership information but information can be made available at the request of the courts. These bank secrecy provisions significantly hamper the GOB's ability to assist other governments in mutual legal assistance requests for financial records.

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. Although it is a member of the Egmont Group, 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. Currently, the FIU has a seven member staff: a director, a legal officer, an investigator, a financial examiner, an office manager, an office assistant, and a secretary. Historically, there has been a lack of coordination between the FIU and the Director of Public Prosecutions, resulting in the FIU attempting to bring its own cases, which are often dismissed from court.

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 anti-money laundering regime in Belize remains relatively ineffective. The FIU received 49 suspicious transaction reports (STRs) during 2008. Fourteen became the subject of investigations. The FIU usually sends queries to the Securities and Exchange Commission and the Financial Crimes Enforcement Network (FinCEN) in the United States and investigations remain open until responses are received. In 2007, there were press reports indicating a possible money laundering scheme by a former public official, but no subsequent investigation was conducted. In 2008, relatives of high ranking government officials were allegedly linked to a money laundering scheme spanning offshore accounts in several countries including Belize. In December 2008, the FIU dropped charges against two of Belize's most prominent banks, the Belize Bank and First Caribbean International Bank—a Canadian controlled bank. The banks had faced charges related to several millions in "suspicious transactions" they were accused of failing to report. The official reason given for dropping the charges was because foreign correspondent banks were discussing severing ties with local banks, threatening to cause a possible collapse and a destabilization of the country's financial sector. The banks are to fund an electronic reporting system for the country, and fund refurbishment of two parks, equal to a monetary penalty of $300,000. The DPP needs to designate, and specially train, attorneys to pursue money laundering charges.

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 government 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 Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention. Belize is not a party to the UN Convention against Corruption. Belize is a member of the Organization of American States and the Caribbean Financial Action Task Force, a FATF-style regional body. The FIU became a member of the Egmont Group of financial intelligence units in 2004. However, Belize has not established a history of providing formal mutual assistance, and in fact has been a particularly nonreactive partner in the area of freezing and confiscating assets.

The Government of Belize should ensure effective implementation of its anti-money laundering and counterterrorist financing regime. The GOB should consider applying civil penalties as well as criminal penalties to further deter these financial crimes. The GOB should increase resources to provide adequate staffing levels and training to those entities responsible for enforcing Belize's anti-money laundering and counterterrorist 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 onshore and offshore sectors, particularly the lack of supervision of the gaming sector, including Internet gaming facilities, and ensure charitable and nonprofit entities cannot be used to aid in the financing of terrorism. Belize should immobilize bearer shares and ensure that the offshore sector complies with anti-money laundering and counterterrorist financing reporting requirements. The GOB should also become a party to the UN Convention against Corruption.

Bolivia

Bolivia is not a regional financial center; however, its money laundering activities continue to take place throughout the country, and are related primarily to the government's lack of political to combat money laundering, narcotics trafficking, public corruption, smuggling and trafficking of persons, as well as Bolivia's long tradition of bank secrecy and the lack of effective government oversight of nonbank financial activities facilitate the laundering of organized crime and narcotics trafficking profits, the evasion of taxes, and the laundering of other illegally obtained earnings. The majority of existing money laundering criminal investigations is located in the

Department of Santa Cruz and associated with significant narcotics trafficking organizations operating from that area.

Bolivia's financial sector consists of 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 90 percent of deposits and loans distributed in U.S. dollars rather than bolivianos, the local currency. Free trade zones exist in the cities of EI Alto, Cochabamba, Santa Cruz, Oruro, Puerto Aguirre and Desaguadero.

Most entities that move money in Bolivia continue to be unregulated. Hotels, currency exchange houses, illicit casinos, cash transporters, and wire transfer businesses are known to transfer money freely into and out of Bolivia without being subject to anti-money laundering controls. Informal exchange businesses, particularly in the Department of Santa Cruz, also transmit money in order to avoid law enforcement scrutiny. The Government of Bolivia (GOB) recognizes shortcomings in Bolivian financial regulation and proposals have been made to address these deficiencies through modifications to the existing legislation.

Bolivia's current anti-money laundering regime is based on Article 185 of Law 1768 of 1997. Law 1768 modifies the penal code and criminalizes money laundering related only to narcotics trafficking offenses, organized criminal activities and public corruption. It provides for a penalty of one to six years for money laundering and defines the application of asset seizure beyond drug related offenses. Article 185, however, cannot be applied unless the prosecution demonstrates in court that the accused participated in and was convicted of the predicated crime. Although terrorist acts are criminalized under the Bolivian Penal Code, the GOB lacks actual statutes that specifically criminalize the financing of terrorism or that grant the GOB authority to identify, seize, or freeze terrorist assets. Legislation that has been in draft for several years, and now currently in Congress, seeks to address this omission by amending the penal code to including the criminalization of terrorist financing.

Article 185 of Law 1768 created Bolivia's financial intelligence unit, the Unidad de Investigaciones Financieras (UIF), located within the Office of the Superintendence of Banks and Financial Institutions. The UIF's function is to conduct financial

investigations in an effort to produce findings and evidence of money laundering activities and other financial crimes and to share this information with both the Bolivian National Police and the Public Ministry, as appropriate. The UIF is also responsible for implementing anti-money laundering controls, and may request that the Superintendent of Banks sanction obligated institutions for noncompliance with reporting requirements. After conducting an initial analysis, the UIF reports detected criminal activity to the GOB's Public Prosecutor. The UIF also performs on-site investigations of obligated entities to review their compliance with the reporting of suspicious transactions and can request additional information from obligated financial institutions to assist prosecutors with their investigations. Given the UIF's limited resources relative to the size of Bolivia's financial sector, compliance with reporting requirements is extremely low. The actual exchange of information and financial intelligence between the UIF and appropriate police investigative entities is also limited or, in some cases, non-existent.

Bolivia's UIF has endured substantial turmoil since 2006, when the GOB issued Supreme Decree 28695 proposing the replacement of Bolivia's UIF with a new "Financial and Property Intelligence Unit" focused on combating corruption rather than money laundering. As a result of the decree, the UIF lost a significant amount of its staff and although the new Financial and Property Intelligence Unit was never implemented, Bolivia's UIF has been unable to recover. As of 2007, the UIF maintained a staff of seven; however, the lack of personnel, combined with inadequate resources and weaknesses in Bolivia's basic legal and regulatory framework fundamentally limits its reach and effectiveness as a financial intelligence unit (FIU).

Further complicating the situation for Bolivia's UIF is its relationship with the Egmont Group, an international network of FIUs that facilitates the exchange of financial intelligence and analysis. 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. In July of 2007, as a direct result of a lack of terrorism financing legislation within the existing Bolivian laws, the UIF received a "Letter of Suspension" from the Egmont Group for "noncompliance with the international mandate to have appropriate legislation addressing this issue."

The GOB's continued lack of terrorist financing legislation since the Egmont Group's 2004 requirement went into effect resulted in Bolivia's expulsion from the Egmont Group of financial intelligence units in December 2008—an unprecedented move by 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. To regain Egmont membership, Bolivia must reapply and provide written evidence of the UIF's compliance with Egmont requirements. The Egmont Group has offered, and continues to offer, assistance to the Bolivian FIU to address its structure and implementing laws to facilitate its re-admission to the Group.

The GOB's pro-coca policies have enabled drug trafficking organizations to become well entrenched in the country and another major blow to Bolivia's anti-money laundering regime is the expulsion of U.S. Drug Enforcement Administration (DEA) agents from the country in November 2008. This action is likely to diminish the effectiveness of several financial investigative groups operating in the country, including Bolivia's Financial Investigative Team (EIF), the Bolivian Special Counternarcotics Police (FELCN), and the Bolivian Special Operations Force (FOE).

The EIF was created in 2002 within Bolivia's FELCN and is responsible for investigating narcotics-related money laundering cases. Currently, there are three EIF units in Bolivia (La Paz, Santa Cruz, and Cochabamba) consisting of a total of 30 personnel (one civilian auditor, and 29 BNP/FELCN investigators). The National Director of the FOE seeks to expand these financial investigative units from 30 personnel nationwide to a total of 60, which would include four financial auditors, one national legal advisor, one national information technology specialist and 51 financial investigators. This initiative was still pending as of late 2008. During the last 12 months, the EIF reported six new money-laundering cases and a total of approximately $10 million in assets seized. The EIF, UIF, Public Ministry, National Police and FELCN have established mechanisms for the exchange and coordination of information, including formal exchange of bank secrecy information.

Under Supreme Decree 24771, obligated entities such as banks, insurance companies and securities brokers are required to identify their customers, retain records of every transactions 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). Bolivia, until recently, had no requirement for these obligated entities to report cash transactions above a designated threshold, and no requirement stating that persons over a designated threshold.

On August 20, 2008, the GOB signed into law Supreme Decree 29681 requiring nationals and foreigners entering or leaving the country to declare the transportation of currency and also obligates any person or business with the intention of transporting, either into or out of the country, any amount of currency in excess of $50,000 to register the transaction with Bolivia's Central Bank. Additionally, the decree states all transactions reported to customs in excess of $10,000 must be reported on a monthly basis to the UIF. Also, the GOB's Superintendent of Banks issues written instructions to the national banks directing them to report any cash transactions in excess of $10,000 or other suspicious financial activities to the UIF.

Corruption remains a serious issue in Bolivia. In the past, allegations against high-ranking law enforcement officials were routinely dismissed without further investigation. While some improvement in the effectiveness of investigations is apparent, few cases are fully prosecuted. On April 26, 2006, for example, the GOB promulgated Supreme Decree 28695, the Organizational Structure for the Fight against Corruption and Illicit Enrichment, as a means to further combat corruption in the police force and other government agencies. As of October 2008, the Bolivian National Police's Office of Professional Responsibility (OPR) investigated a total of 2,043 cases in 2008 involving allegations of misconduct and/or impropriety by police officers. Of these, 176 cases involved police officers assigned to Bolivia's Special Counter-Narcotics Force (FELCN); none resulted in findings of corruption. A total of 876 cases have been adjudicated before the Police Disciplinary tribunal, the remainder are still in the investigative stage and/or awaiting tribunal action.

There continue to be serious deficiencies in Bolivia's legal framework with regard to civil responsibility in financial and money laundering cases. 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 since the legislation is full of inconsistencies and contradictions, and is open to wide interpretation. As a result, prosecutors are often reluctant to pursue money laundering investigations.

While traditional asset seizure continues to be employed by counternarcotics authorities, the ultimate forfeiture of assets continues to be problematic. 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 and plagued by corruption for years, and has only auctioned confiscated goods sporadically. In late 2006, then newly appointed DIRCABI staff, including the National Director and several Regional Directors, began initiating positive steps to improve the organization's internal operating procedures. In 2007, DIRCABI proposed Supreme Decree 29305, which was signed by the Bolivian President in October 2007 and provides for some positive changes relating to asset seizure, forfeiture, and sharing. DIRCABI is involved in drafting new civil asset forfeiture legislation to address persisting problems in terms of forfeited asset sharing among law enforcement entities. To address the inadequate management and related administrative issues that have plagued DIRCABI for years, special administrative legislation was submitted for approval that will resolve long standing organizational issues that resulted in questionable administrative procedures in these forfeiture cases. As of October 31, 2008, DIRCABI has initiated 615 asset forfeiture cases. In these 615 cases, 1,201 items were seized—the majority of which included electronic equipment, such as cellular phones. In addition, a total of 26 residences, 211 vehicles, as well as cash, jewelry, and other miscellaneous items were seized.

Bolivia is a party to the 1988 UN Drug Convention, UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. Bolivia does not have a mutual legal assistance agreement with the United States, but is a party to the Inter-American Convention on Mutual Assistance in Criminal Matters. Bolivia is also a

member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group on Money Laundering.

The GOB is currently a sanctioned member of the Financial Action Task Force for South America (GAFISUD). The GAFISUD placed sanctions on Bolivia in July 2007 as a result of the GOB's failure to pay three years of its membership dues. The GOB was able to make partial payment of its arrears and a bill is currently pending in Bolivia's Congress to authorize payment of its remaining debt to GAFISUD. At the GAFISUD December 2008 plenary meeting, GAFISUD members agreed to continue sanctions that prohibit Bolivia from having a voice or vote at GAFISUD plenary meetings, with the expectation that Bolivia will have met the requirements to fully reinstate its membership by the June 2009 plenary meeting.

Several of Bolivia's current AML/CTF regime deficiencies can be remedied if the GOB were to enact current draft legislation to improve Bolivian law in the area of financial investigations. With support from the USG and others, the GOB has formed a working group composed of key GOB ministry and police representatives with the goal of creating new legislation to address issues such as the interception of communications, money laundering, civil forfeiture, modifications to the existing Criminal Code of Procedures, consensual recordings, and cooperation agreements. In addition, within this legislative initiative, the area of terrorism financing would be addressed along with a new special administrative law to improve the functions of DIRCABI. The GOB completed this draft legislation in October 2008, received interagency approval, and submitted the bill to the Bolivian Congress for review in late 2008. It is anticipated that the legislation will be approved and written into law at the beginning of 2009. This legislation would significantly improve the abilities of the GOB investigators and prosecutors to more successfully attack criminals and organizations involved in illicit financial activities in Bolivia, including terrorism financing.

The GOB should take all necessary steps to ensure that the draft anti-money laundering legislation is enacted and conforms to international standards. Among the most important legislative adjustments, it is imperative that the GOB criminalizes terrorist financing and allow for the blocking of terrorist assets; doing so is not only mandated by Bolivia's commitments as a member of the United Nations and GAFISUD, but could improve the likelihood that the UIF may successfully re-apply for Egmont

Group membership. In addition, money laundering should be an autonomous offense without requiring prosecution for the underlying predicate offense, and currently unregulated sectors, particularly designated nonfinancial businesses and persons, should be subject to anti-money laundering and counterterrorist financing controls. Bolivia should also ensure that the UIF has sufficient staff and resources. The GOB should also pay the remainder of its GAFISUD dues to avoid being fully suspended from GAFISUD.

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. Statistics from Bosnia's financial intelligence unit (FIU) indicate that financial crimes have increased over the past year. Bosnia is also vulnerable to terrorist financing. The cash-based economy and weak border controls on bulk cash couriers contribute to BiH as an attractive venue for terrorist financiers and organized criminal elements to carry out illicit financial activities.

Corruption is also a serious problem in BiH. The European Commission's November 2008 Progress Report for Bosnia identified widespread corruption as one of the key problems in the country. In addition, Transparency International has recently ranked Bosnia as the most corrupt country in the Balkan region, stating that corruption is of particular concern in Bosnia because it involves political corruption as well as corruption in privatization and public procurement procedures. Bosnia adopted an anticorruption strategy in 2006, but has since failed to fully implement any aspects of the plan.

It is likely that trade-based money laundering occurs in BiH, but there is no indication that law enforcement has taken any action to combat it. There are five active Free Trade Zones in BiH, with production based mainly on automobiles and textiles. There have been no reports that these trade zones are used in trade-based money

laundering. The Ministry of Foreign Trade and Economic Relations is responsible for due diligence and monitors the activities of these zones.

The threat posed by bulk cash couriers is not well understood in BiH. Remittances from abroad are estimated to be in the millions of U.S. dollars annually, and constitute as much as 20 percent of the BiH gross domestic product. Many of these remittances likely enter the country in the form of cash. Customs officials are required to report any cross-border transportation of cash in excess of KM 10,000 (approximately $6,770), but this regulation is not enforced and there is no declaration or disclosure system in place for cash entering the country.

The September 2006, International Monetary Fund's Financial System Stability Assessment report praises Bosnia and Herzegovina for the progress made since the 2005 mutual evaluation by the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force-style regional body. However, the report also cites problems with information-sharing, coordination, and communication, as well as jurisdictional issues between the Financial Police and other State agencies. Those problems continue to exist with little evident correction.

The capabilities of the BiH anti-money laundering/counterterrorist financing (AML/CTF) regime should be viewed in the context of Bosnia's decentralized political structure. There are multiple jurisdictional levels in Bosnia and Herzegovina, including the State, the two entities (the Federation of Bosnia and Herzegovina (the Federation) and the Republika Srpska (the RS)), 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. Each jurisdiction, however, maintains its own separate supervision and 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. This confusion undermines State-level institutions and impedes efforts to improve operational capabilities to combat money laundering and terrorist financing. 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, enacted in 2004, takes an “all serious crimes” approach and 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 an FIU within the State Investigative and Protection Agency (SIPA). Those convicted of money laundering exceeding the equivalent of $30,000 receive prison terms of 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 26 types of entities to report to the FIU all transactions of $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 (NFIs) and designated nonfinancial businesses and professions (DNFBPs), 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 practice, most NFIs and DNFBPs do not understand the law, thereby resulting in very low reporting from those sectors. The FIU is developing an automated AML reporting system, on which all bodies responsible for reporting will eventually be trained. 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. The banking sector and the ITA file the majority of reports.

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 12

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 AML/CTF 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 and alternative remittance systems, 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 to an Economic Crime Unit, the Federation Police has a specialized Financial Police Unit that focuses on public corruption, economic crimes, money laundering, and cybercrime. The RS police has a Special Investigations Unit to investigate financial 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. Because BiH is largely a cash economy, it is typical for individuals to carry large amounts of cash, even across borders. Bosnia and Herzegovina also receives a significant volume of remittances from emigrants. Official remittances constitute over 17 percent of GDP. While some of these will enter the country through bank transfers, others 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 interagency 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. However, 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. During the first nine months of 2008, the FID reports it froze assets in only one case, in the amount of KM 4.3 million ($2,900,000).

The FID currently faces several challenges. Information sharing and interagency cooperation are major operational deficiencies of the FID. Although it receives and analyzes information from reporting entities, it does not effectively share the results of its analysis with relevant law enforcement agencies. One reason for this is an ambiguous provision in the AML law that does not clearly define the FID's obligation to disseminate information to appropriate law enforcement entities. FID officials have interpreted the information sharing provision in the AML law so narrowly that it has resulted in a virtual standstill in the dissemination of reports to agencies outside of SIPA. The failure by the FID to properly disseminate its information has greatly isolated the agency, affecting not only communication and cooperation between the FIU and law enforcement but the overall effectiveness of the FID as well.

Management of the data submitted to the FID is another problem facing the FIU. Obligated entities submit reports to the FIU through an electronic reporting system. However, prior to the implementation of the electronic reporting system, institutions submitted hardcopy reports which were then entered manually into the FID's database. There is currently a backlog of approximately 140,000 reports that have not yet been input into the FID's database.

In the first nine months of 2008, the FID received 208,378 CTRs from banks and other financial institutions. Of these, the FID identified 47 cases as suspicious and investigated them. Of these 47 cases, the FID submitted seven reports to the BiH Prosecutor. Since BiH established its AML regime in 2004, the Court of BiH has pronounced 38 money laundering verdicts: 17 legally binding verdicts in 2004 and

2005 (in which the total amount of laundered money was nearly $10,900,000, and for which nearly $800,000 in assets was forfeited), 12 first instance verdicts in 2006, and nine first instance verdicts in 2007. Statistics for 2008 are not yet available. A major problem facing BiH is the high rate of verdicts overturned or modified on appeal (which is not exclusively a problem for money laundering convictions). So it is possible that some of the 2006 and 2007 verdicts may yet be overturned. The FID is not the only active agency in the AML regime: the RS entity police agency and the Federation Financial Police, among others, all reported money laundering-related cases. In 2008, the Bosnian Court system pronounced five money laundering verdicts involving a total of seven people. Out of these five cases, four included prison sentences and one a suspended sentence.

BiH has no specific asset forfeiture law as regards money laundering, with the exception of the Persons Indicted for War Crimes (PIFWC) support laws that 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 in 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.” 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. Article 133 of the criminal code also allows the courts to 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, although, Article 110 (3) of the Criminal Code appears to contemplate a civil or quasi-civil forfeiture: “a separate proceeding if there is probable cause to

believe that the gain derives from a criminal offense and the owner is not to give evidence that the gain was legally acquired." 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 Code criminalizes terrorist financing. 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. There is no one government entity that regulates or supervises the nongovernmental organization (NGO) sector, but NGOs are subject to some supervision from the relevant ministry, tax administration, labor or other inspectors.

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. 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 March 2008, five Bosnian Muslims belonging to a radical group were arrested for suspected terrorist activity and handed over to the State Prosecutor's Office for investigation. Weapons, including mines and other explosive devices, as well as materials for making explosive devices, were found and seized during the operation. They were subsequently released by the prosecutor for lack of admissible evidence pertaining to formal terrorism charges. A Bosnian investigation is still ongoing.

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, however, 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 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 party. Bosnia is a member of MONEYVAL and the FID is a member of the Egmont Group. Bosnia is scheduled to undergo a mutual evaluation by MONEYVAL in 2009.

The Government of Bosnia and Herzegovina (GOBiH) 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 GOBiH should make efforts to increase funding for its AML/CTF programs and enhance cooperation between concerned departments and agencies. With regard to the FID, BiH should amend its AML law to clarify the FID's obligation to disseminate information outside of SIPA. The FID also needs to reduce the backlog of reports that have not been input into its database. Although prosecutors, financial investigators, and tax administrators have received training on tax evasion, money laundering, and other financial crimes, the GOBiH should enhance their capacity to 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 should increase awareness by improving outreach programs to address major vulnerabilities, including the identification of shell companies and beneficial owners. In addition, GOBiH should implement formal supervisory mechanisms for nonbank financial institutions and intermediaries, and NGOs. BiH law enforcement and customs authorities should take additional steps to control the integrity of the borders and limit

smuggling. The GOBiH should study the formation of centralized regulatory and law enforcement authorities. BiH should take specific steps to completely implement its anticorruption strategy and to combat corruption at all levels of commerce and government. BiH also should adopt a comprehensive asset forfeiture law that 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 party.

Brazil

Brazil is the world's fifth largest country in size and population, and in 2008 its economy remains the tenth largest in the world. Brazil is considered a regional financial center for Latin America. It is also a major drug-transit country. Brazil maintains adequate banking regulations, some controls of capital flows, and requires disclosure of the ownership of corporations. Money laundering in Brazil is primarily related to domestic crime, especially drug-trafficking, corruption, organized crime, and trade in various types of contraband. Trade of all kinds generates funds that may be laundered through the banking system, real estate investment, financial asset markets, luxury goods or informal financial networks. An Inter-American Development Bank study of money laundering in the region found that Brazil's relatively strong institutions helped keep the incidence of money laundering to below average for the region.

Terrorist financing is not an autonomous offense in Brazil, although the money laundering bill currently awaiting legislative action contains language effecting that change. The bill would make it a crime to directly or indirectly provide or to receive from any person or group funds, goods, services or anything else of value, with the intention of causing public panic, and/or trying to constrain or influence a government or international body to act or refrain from acting. Those convicted would be punished for up to 12 years in prison. To implement fully this important change and other aspects of its financial crimes regime, Brazil intends to enact legislation that will provide for the effective use of 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. Currently, such techniques can be used only for information purposes, and are not admissible in court.

The U.S. Government (USG) continues to believe the Brazil-Paraguay-Argentina Tri-Border Area (TBA) to be a source of terrorist financing, although the Government of Brazil (GOB) maintains that it has not seen any such evidence. That said, there may be as much or more reason to be concerned about other areas of the country. GOB and local officials in the states of Mato Grosso do Sul and Parana, for example, have reported increased involvement by Rio de Janeiro and Sao Paulo gangs in the already significant trafficking in weapons and drugs that plagues the states in the tri-border area. Consequently, antismuggling and law enforcement efforts by state and federal agencies have increased. In addition to weapons and narcotics, a wide variety of counterfeit goods, including CDs, DVDs, and computer software (much of it of Asian origin), are routinely smuggled across the border from Paraguay into Brazil. Brazilian customs authorities have continued their efforts to combat contraband in the TBA given the resulting loss of tax revenues.

Brazil's anti-money laundering policy is to advance six goals: improve coordination between federal and state anti-money laundering agencies; develop and make maximum use of computerized databases and public registries to facilitate monitoring and enforcement; constantly evaluate and improve existing mechanisms; increase international cooperation in enforcement and the recovery of assets; promote an anti-money laundering culture in Brazil; and prevent violations before they occur through the foregoing.

Brazil's first anti-money laundering legislation passed in 1998 and has since been amended by subsequent legislation, decree and regulation. Law 9.613 criminalizes money laundering related to drug trafficking, terrorism, arms trafficking, extortion by kidnapping, public administration, the national financial system and organized crime. The 1998 statute requires that individuals bringing more than 10,000 reais (then $10,000, now $4,700) in cash, checks, or traveler's checks into Brazil must fill out a customs declaration. Subsequent modification to the law and associated regulations criminalize the corruption or attempted corruption of foreign public officials involving international commercial transactions, and establishes terrorist financing as a predicate offense for money laundering. The current legal regime also establishes

crimes against foreign governments as predicate offenses, and requires the Central Bank to create and maintain a registry of information on all bank account holders.

The 1998 anti-money laundering statute also created Brazil's financial intelligence unit, the Conselho de Controle de Atividades Financeiras (COAF), which is housed under the Ministry of Finance. COAF staff includes representatives from regulatory and law enforcement agencies, including the Central Bank and Federal Police, and is empowered to request financial information on any individual suspected of criminal activity from all government entities. COAF has a staff of 43 and expects to add 25 new personnel in 2009.

Entities under the authority of the Central Bank, the Securities Commission (CVM), the Private Insurance Superintendence (SUSEP), and the Office of Supplemental Pension Plans (PC), are required to file suspicious activity reports (SARs) with their respective regulator, which passes them to COAF. COAF directly regulates and receives SARs from those financial sectors not already under the jurisdiction of another supervising entity, such as commodities traders, real estate brokers, credit card companies, money remittance businesses, factoring companies, gaming and lottery operators, bingo parlors, dealers in jewelry and precious metals, and dealers in art and antiques.

The Central Bank's Department to Combat Exchange and Financial Crimes (DECIC) examines entities under the supervision of the bank to ensure compliance with suspicious transaction reporting requirements, and forwards information on the suspect and the nature of the transaction to COAF. In 2005, DECIC was able to bring on-line a national computerized registry of all current accounts in the country. A Central Bank regulation issued that same year requires banks to report identifying data on all parties to foreign exchange transactions and money remittances, regardless of the amount involved.

In addition to filing SARs, banks are also required to inform the Central Bank of institutional transactions exceeding 100,000 reais ($57,000) and "unusual" amounts transacted by individuals. Lottery operators must notify COAF of the names and identifying information of winners of three or more prizes equal to or higher than 10,000 reais within a 12-month period. Subsequent changes in the law authorize the monitoring of transactions with possible links to terrorism and by politically exposed persons.

SUSEP requires insurance companies and brokers to report large policy purchases, settlements or otherwise suspicious transactions to both SUSEP and COAF. Insurance-related activities by or on behalf of politically exposed persons are also monitored. In addition, on January 8, 2008, the Securities Commission (CVM) extended monitoring/reporting requirements to include dealers in luxury goods and persons or companies that engage in activities involving a high volume of cash transactions.

COAF has direct access to the Central Bank database, so that it can review its SARs and information about all current accounts. COAF also has access to government databases, and is authorized to request additional information directly from the entities it supervises and the supervisory bodies of other reporting entities. Complete bank transaction information may be provided to government authorities, including COAF, without a court order. Brazilian authorities that register with COAF may directly access COAF databases via a password-protected system.

During the first 10 months of 2008, COAF received information regarding 226,413 cash and 296,070 noncash transactions, an increase of 55 percent compared to 2007. During the same period, the Central Bank received 830,257 reports of transactions exceeding 100,000 reais and 367,566 reports were submitted to SUSEP regarding activities in the insurance sector. Through October 2008, COAF has provided 1,002 Financial Intelligence Reports involving 8,997 individuals to cooperating agencies. The Justice Ministry used COAF reports to seize 640 million reais in 2008. COAF has referred 17 cases for administrative sanctions this year, resulting in fines of 3.8 million reais.

Additional legislative changes are currently under consideration by the Brazilian legislature. The pending legislation, if approved in its current form, would facilitate greater law enforcement access to financial and banking records during investigations, criminalize illicit enrichment, allow seized assets to be monetized to preserve their value, and facilitate prosecution of money laundering cases by making it an autonomous offense. The proposed changes would also help to bring the Brazilian legal regime in line international anti-money laundering standards. This legislation is considered a priority, and is expected to be voted on by Congress shortly.

The National Corruption and Money Laundering Strategy Task Force (ENCCLA—Estratégia Nacional de Combate a Corrupção e Lavagem de Dinheiro) is comprised of

GOB and state agencies with jurisdiction over money laundering and other financial crimes and began convening periodic strategy and planning sessions in 2003. Twenty-eight agencies, ranging from the National Intelligence Agency to the Brazilian Banking Federation attended the first meeting; 51 participated in 2007. In November 2008, ENCCLA met in Salvador, Bahia. Participants from federal, state, and municipal governments took part and established ways to confront administrative fraud, domestic money laundering through business activities, and to regulate investigation techniques.

Some of the agencies, and most of the laws and regulations that comprise Brazil's anti-money laundering apparatus were conceived within the ENCCLA framework, including pending revisions of the current statute. ENCCLA members have also drafted a bill imposing conditions on banking privacy and allowing for the forfeiture of assets. The National Registry of Account Holders, which permits authorities to monitor transactions between individuals and corporations utilizing the national financial system, was also an ENCCLA initiative. Prior to the creation of the registry, information requests from judges could take several weeks to process. Now, detailed information can be compiled and forwarded within 24 hours of the request.

ENCCLA also helped create the Justice Ministry's Department of Asset Recovery, which, among other duties, is responsible for international cooperation on money laundering cases and is empowered to share seized forfeited assets with other countries. The determination that "politically exposed" individuals merited special attention was first proposed at a 2006 ENCCLA meeting. The Central Bank now maintains a registry of 30,000 office holders, persons who have held office in the past five years, and persons who appear to have or have had some financial nexus to them.

The GOB reported regular increases in the number of money laundering investigations, trials and convictions beginning in 2003. The annual number of investigations grew from 198 in 2003 to 625 in the first three quarters of 2006. These investigations led to 26 trials to 41 in the first three quarters of 2006, while convictions increased from 172 in 2003 to 866 in 2006. One reason for the growing number of money laundering prosecutions is the number of cases that are resulting from the Banestado bank scandal of the late 1990s. Through 2008, this investigation

has resulted in 95 indictments against 684 persons, of which 97 have already been tried and found guilty. Yet another reason for the increase in investigations since 2005 is the establishment of Brazil's Trade Transparency Unit (TTU) that identifies discrepancies in trade data that are indications of trade-based money laundering. In its first year of operation, Brazil's TTU (with the assistance of U.S. DHS ICE agents) uncovered a discrepancy so large that 250 search warrants were issued throughout Brazil and eventually led to 128 arrest warrants. The number of investigations and convictions since 2006 is still not available, as the Ministry of Justice remains in the process of developing a unified reporting system that would account for information from the various money laundering courts involved.

The GOB also credits the creation of specialized money laundering court branches, founded in 2003, for the increasing number of successful prosecutions. Fifteen such courts have been established in fourteen states, including two in São 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 was formed aimed to build on the success of the specialized courts by creating complementary specialized federal police financial crimes units in the same jurisdictions. In 2008, the Federal Police established such units in the Federal District (Brasilia), and the states of Rio de Janeiro and São Paulo. All other 24 states have established financial working groups.

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.

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.

The USG has placed nine individuals and two entities in the TBA on its list of Specially Designated Nationals, because they have provided financial and/or logistical support to Hezbollah. The nine individuals operate in the TBA 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 Pag 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 TBA.

Brazil is party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism. Brazil is a member of the Financial Action Task Force (FATF) and assumed its presidency for one year in July 2008. Brazil was a founding member of the Financial Action Task Force against Money Laundering in South America (GAFISUD), and held the GAFISUD presidency in 2006. 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. Brazil's financial intelligence unit, the Council for the Control of Financial Activities (COAF), has been a member of the Egmont Group of financial intelligence units since 1999.

The Mutual Legal Assistance Treaty between Brazil and the United States entered into force in 2001, and a bilateral Customs Mutual Assistance Agreement, signed in 2002, became effective in 2005. Using the Customs Agreement framework, the GOB and U.S. Immigration and Customs Enforcement in 2006 established a Trade Transparency Unit (TTU) in Brazil to detect money laundering via trade transactions. The GOB also participates in the "3 Plus 1" Security Group (formerly the Counter-Terrorism Dialogue).

The Government of Brazil should criminalize terrorist financing as an autonomous offense. In order to successfully combat money laundering and other financial crimes, Brazil should 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 in order 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 TBA and among designated nonbanking financial businesses and professions. Additionally, COAF must continue to fight against corruption and ensure the enforcement of existing anti-money laundering laws, including the obligation for all financial institutions to report transactions suspected of being related to terrorist financing.

British Virgin Islands

The British Virgin Islands (BVI) is a Caribbean overseas territory of the United Kingdom (UK), and remains vulnerable to money laundering due to drug trafficking and the exploitation of its offshore financial services.

The BVI is considered a major offshore financial center with the industry contributing nearly fifty percent of the Government's annual revenue. As of June 2008, the BVI has approximately nine banks, nine money remitters, 2,840 active mutual funds, 31 local insurance companies, 392 captive insurance companies, 213 trust licenses, eight authorized custodians, 22 company management companies, 117 registered agents, 532 limited partnerships, 10,666 local companies, and 445,865 active BVI business companies or international business companies (IBCs).

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. Under the BCA, a company limited by shares may issue bearer shares that are immobilized or registered through an authorized custodian. IBCs registered before 2005 with bearer shares have until 2009 to register their bearer shares with an authorized custodian.

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 (the most widely used vehicle); companies limited by guarantee authorized to issue shares (typically used for structuring transactions by combining equity and guarantee membership); companies limited by guarantee (not authorized to issue shares); unlimited companies (authorized to issue shares); unlimited companies (not authorized to issue shares); restricted purposes companies (used primarily in structured finance and securitization transactions); and segregated portfolio companies (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 GOBVI 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 includes banking and fiduciary businesses, investment businesses, insolvency services, accountants, insurance companies, and company management and registration businesses. The FSC is also responsible for off-site and on-site inspections of these institutions. 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. From January to June 2008, the FSC conducted eight on-site inspections and issued four warnings, one advisory, and assessed one fine.

The FSC cooperates with 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 offenses except drug trafficking as predicates for money laundering; drug trafficking predicated money laundering is established under similar provisions in the Drug Trafficking Offenses Act 1992 (DTOA). The POCCA outlines penalties for money laundering. Upon summary conviction, penalties include six months imprisonment or a fine not exceeding three thousand dollars or both; and on indictment to a term of imprisonment not exceeding 14 years or a fine of $20,000 dollars or both. The POCCA and the DTOA 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 not directly linked to narcotics related crimes are unclear.

In February 2008, The Anti-Money Laundering Regulations (AMLR) replaced the Anti-Money Laundering Code of Practice 1999, and the Anti-Money Laundering and Terrorist Financing Code of Practice 2008 (AMLTFCOP) revoked The Guidance Notes 1999. The AMLTFCOP establishes a risk based approach to anti-money laundering (AML) and counterterrorist financing (CTF) supervision and compliance. Issued by the FSC, the AMLTFCOP applies to all financial institutions and designated nonfinancial businesses and professions (DNFBPs) including charities and nonprofit associations. Car dealers, yacht dealers, dealers in precious metals and stones, dealers in heavy machinery, and leasing companies were brought under the sphere of the BVI's AML regime through the Nonfinancial Business (Designation) Notice in February 2008. The Financial and Money Services Act 2008 (FMSA) will require entities that engage in money and currency exchange, money or value transfers, financial services businesses to become regulated entities and subject to the AMLR and the AMLTFCOP.

The AMLTFCOP identifies procedures for customer due diligence, identifying beneficial owners and politically exposed persons, internal controls, shell banks and corresponding banking relationships, wire transfers, record keeping, and anti-money laundering training and reporting requirements. Concerning customer due diligence, regulated entitles must update clients' due diligence information every three years for low risk business relationships and once every year for higher risk business relationships. The AMLR requires the retention of records for a period of at least five years from the date when all transactions relating to a one-off transaction or a series of linked transactions were completed, when the business relationship formally ended, or when the last transaction was carried out. However, there is no formal requirement for account files to be maintained for at least five years following the termination of an account or business relationship.

The POCCA (Amendment) 2006 mandates financial institutions and other providers of financial services to report suspected money laundering transactions including attempted transactions. The AMLR and the AMLTFCOP establishes procedures to identify suspicious transactions and report them to the financial intelligence unit (FIU). Obligated entities are protected from liability for reporting suspicious transactions.

Reporting entities are required to create a clearly defined reporting chain for employees to follow when reporting suspicious transactions, and to appoint a reporting officer to receive such 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 POCCA mandates the creation of an FIU, the Reporting Authority. The Financial Investigation Agency (FIA) Act 2003 reorganized and renamed the FIU. The FIA's staff is comprised of a director, two senior police officers, one senior customs officer, a chief operating officer, a junior analyst, 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, Director of the FIA, Commissioner of Police, and Comptroller of Customs.

The FIA is responsible for the collection, analysis, investigation, and dissemination of suspicious transaction reports (STRs). The FIA receives approximately 200 STRs annually. The FIA refers STRs that warrant further investigation to the Royal Virgin Islands Police Force (RVIPF), which is responsible for investigating drug trafficking, money laundering, and terrorism financing. In 2007, the FIA Act 2003 was amended to redefine the FIA's responsibilities to include investigation and analysis of any offense in relation to money laundering and terrorist financing. The amendment empowered the FIA to investigate matters relating to the breach of any domestic or international sanction prescribed by or under any enactment. It also provided the FIA authority to receive disclosures of suspected terrorist financing. However, a discrepancy exists with the FIA's ability to receive STRs related to the financing of terrorism. Technically, reporting institutions are to submit terrorist financing STRs directly to the RVIPF. It is unclear whether the RVIPF has an obligation to share the STR with the FIA. Presently, no terrorist financing STRs have been reported.

The FIA has the ability to request additional information from reporting institutions. The FIA also 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. The FIA has the authority to provide a written order to freeze a transaction for up to 72 hours, as well as has the

authority to freeze a bank account on behalf of the Governor, Attorney General, the FSC, or a foreign FIU or law enforcement agency for a period of five days.

The POCCA (Amendment) 2008 replaced the Joint Anti-Money Laundering Coordinating Committee (JAMLCC) with the Joint Anti-Money Laundering and Terrorist Financing Advisory Committee (JALTFAC). The JALTFAC is comprised of the Managing Director of the FSC, the Attorney General, Commissioner of Police, Comptroller of Customs, Director of the FIA, and the Financial Secretary. The JALTFAC also includes private sector stakeholders such as the Registered Agents Association, Compliance Officers Association, Bankers Association, Bar Association, and the Society of Trusts and Estate Practitioners. The purpose of the JALTFAC is to assist the FSC in formulating a code of practice; ensure reporting institutions are compliant with relevant AML/CTF measures; and keeping the BVI aware of AML/CTF developments locally and internationally.

The United Kingdom's Terrorism (United Nations Measures) (Overseas Territories) Order 2001 (TUNMOTO) and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002 (ATFOMOTO) 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 (ATUNMOTO) also apply to the BVI. Terrorist financing offenses are covered under the TUNMOTO under article 3 which makes it an offense for any person to invite another person to provide funds, or to receive and provide funds with the intention or knowledge that the funds may be used for the purpose of terrorism. Under the ATFOMOTO a person guilty of terrorist financing may be subject to imprisonment for a term not exceeding 14 years, to a fine, or to both, or on summary conviction to imprisonment for a term not exceeding six months, a fine not exceeding the statutory maximum or both. To date, there are no investigations of terrorism financing in the BVI.

The POCCA and the DTOA provide the ability to freeze or seize assets. Forfeiture is also covered by the POCCA and the DTOA upon conviction. The freezing and forfeiture of funds and property used for terrorist financing is covered by the ATUNMOTO, TUNMOTO, and the ATFOMOTO. The Governor of the BVI is responsible for executing freeze orders related to terrorist financing. Reporting institutions are advised to monitor relevant websites for names of suspected terrorists and related organizations.

No specific guidance has been issued to outline reporting institutions obligations to freeze funds of designated terrorists and terrorist organizations.

The Office of the Director of Public Prosecution (ODPP) is responsible for obtaining forfeiture, charging and restraint orders, and the prosecution of all money laundering and other criminal investigations. Currently, there are two ongoing money laundering investigations. The last money laundering conviction was obtained in 2003. In May 2008, the GOBVI confiscated $45 million in an alleged international money laundering case from the Bermuda based IPOC International Growth Fund. The IPOC case gained international notoriety with allegations that IPOC was a money laundering front with ties to Russia's Telecommunications Minister, among others. Tried in the BVI, the case involved IPOC and three BVI IBCs. A 17-month investigation by BVI authorities revealed a complex web of irregularities with false parties to agreements, allegedly forged signatures, and falsified documents exhibiting that the three BVI IBCs received payments from third parties for services rendered; however, those companies had not provided the services claimed, or had not made the payments. As a result, these entities plead guilty to furnishing false information and obstruction of justice. The BVI intends to confiscate the entire funds of IPOC within its jurisdiction and share the forfeited assets with the Government of Bermuda. The BVI IBCs will be dissolved no later than April 2009.

The BVI is a member of the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body and underwent a mutual evaluation in February 2008. As a result the government enacted anti-money laundering legislation that requires financial institutions to identify the beneficial owners of companies, cut ties with shell banks and refuse requests to open anonymous accounts. This legislation helps the country comply with the European Union's Third Money Laundering Directive. The BVI is an observer to the Offshore Group of Supervisors, and the FIA is a member of the Egmont 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. The U.S. and the British Virgin Islands established a Tax Information Exchange Agreement (TIEA) in 2006. Application of the U.S.-UK Mutual Legal Assistance Treaty (MLAT)

concerning the Cayman Islands was extended to the BVI in 1990. The FIA handles MLAT and other legal assistance requests after they have been reviewed by the Office of the Attorney General.

The Government of the British Virgin Islands (GOBVI) made substantial efforts to bolster their AML/CTF regime during 2008. However, the GOBVI should consider revising money laundering and terrorist financing penalties to dissuade criminals and terrorists from exploiting the territory. The GOBVI should specify that the FIA directly receive STRs related to terrorism financing. The BVI should ensure that designated nonfinancial businesses and professions adhere to the provisions of its AML/CTF regulations particularly with the reporting of STRs. The GOBVI should ensure that there are a sufficient number of regulators and examiners to exercise effective due diligence, regulation, and inspections of its 446, 865 active BVI companies in a manner compliant with international standards.

Bulgaria

The Government of Bulgaria (GOB) needs to seriously strengthen its anti-money laundering regime. While Bulgaria is not considered an important regional financial center or an offshore financial center, it is significant in terms of its geographical position, its well-developed financial sector relative to other Balkan countries, its relatively lax regulatory control, and its government tolerance of corruption and failure to strictly enforce anti-money laundering (AML) laws. Moreover, Bulgaria is a major transit point for the trafficking of drugs and persons into Western Europe, generating criminal proceeds that are subsequently laundered in Bulgaria. Bulgaria is primarily a cash economy, thereby making it more difficult to trace illicit money flows. ATM and credit card fraud remain serious problems. Tax fraud is prevalent. Smuggling remains a problem, reportedly sustained by corrupt Bulgarian businessmen and politicians. Organized crime groups are moving into legitimate business operations, making it difficult to determine the origins of their wealth. While tourism and construction formed the basis for the country's economic revival in recent years, they have also become favorite money laundering routes for organized crime groups with suspected ties to politicians.

Since its admission to the European Union (EU) in 2007, Bulgaria has faced constant criticism and pressure from the European Commission (EC) regarding its failure to

effectively combat corruption. Public officials, watchdog institutions, and journalists who challenge organized crime operations often face intimidation. Corruption, fraud, and organized crime are such pervasive problems in Bulgaria that the EU stripped the country of 220 million Euros (approximately $285,200,000) of funds in November 2008 and said Bulgaria might lose another 340 million Euros (approximately $440,700,000) if it failed to curb corrupt practices and political interference in funding processes by the end of 2009. Although Bulgaria has launched several investigations into government officials and businessmen suspected of funds fraud, it has failed to convict a single senior official of graft and has jailed only one organized crime leader.

Despite the prevalence of corruption and weak enforcement of AML laws, Bulgaria has managed to make some progress in 2008. Facing sharp EU, U.S. and civil society criticism, the Bulgarian government finally closed all duty free shops and petrol stations at Bulgaria's land borders in July 2008. These establishments had been suspected to be major centers for contraband, tax evasion, and money laundering. In October 2008, after repeated requests by the U.S. and EU, and after protracted delays, the government decided to mandate that the actual amount of a cash transaction be listed on reporting forms. This closed an important loophole in AML legislation that had previously served to facilitate money laundering. Despite these improvements, the GOB's AML efforts still need substantial intensification.

Article 253 of the Bulgarian Penal Code criminalizes money laundering related to all crimes. As such, drug-trafficking is but one of many recognized predicate offenses. 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.

The Law on Measures against Money Laundering (LMML) is the legislative backbone of Bulgaria's AML regime. Adopted in 1998, the LMML has since been amended several times, most recently in 2008. The many revisions to the law, though often in the right direction, have rendered the law less comprehensible and hence less effective. 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.

The 2006 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.

In response to pressure from the EU, in 2006, Bulgaria's Parliament tightened the LMML with further amendments. These amendments expand the definition of money laundering and the list of reporting entities; outlaw anonymous bank accounts; expand the definition of "currency"; and require the disclosure of the source of 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 transaction reports (STRs). The banking sector, with some key exceptions, has substantially complied with the law's filing requirement. Reporting by other sectors, in particular reporting related to the explosion of real estate transactions (e.g., notaries and real estate agents), has been much lower.

The Law on Administrative Violations and Penalties, as amended in 2005, establishes the liability of legal persons (companies) for crimes committed by their employees.

Bulgaria's financial intelligence unit (FIU), the Financial Intelligence Directorate (FID) within the State Agency for National Security (DANS) is the main administrative unit for collecting and analyzing information on suspected money laundering transactions. The FID-DANS does not participate in criminal investigations. In the past year, FID has had its powers severely limited. Prior to December 2007, Bulgaria's FIU was a fully independent agency operating under the Ministry of Finance (MOF), with the independence of its director 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 that came into force on January 1, 2008, which limits the FID's effectiveness and autonomy. This law, the Act on the State Agency for National Security, establishes DANS as the new national intelligence agency. The law also restructures the FID by changing its status from an independent agency within the MOF to a directorate within the DANS; consequently, the FID is no longer an individual legal entity with its

own budget. Some of the FID's previous authorities were removed from the law and included only in regulations, further diminishing the FID's status. Other authority was assigned to the director of DANS, but not expressly to the FID, thereby limiting its ability to compel legal compliance by banks. In addition, discrepancies between the LMML and the law creating DANS create uncertainty regarding the FID's inspection and sanctioning authorities, including its ability to perform AML on-site inspections. In addition, the analytical capacity of FID is not precisely defined: the DANS law permits the FIU to acquire and handle national security-related information, but financial crimes information is not necessarily of national security importance. From January 1 to May 1, 2008, the Egmont Group of FIUs temporarily suspended Bulgaria's access to its secure information exchange system, pending a review of FID's authorities under the new legislation.

As of September 2008, the FID-DANS conducted 46 on-site inspections and issued 44 penal decrees totaling 119,500 BGN (approximately $78,826), as compared with 83 such inspections of banking and nonbanking institutions as of October 2007. As of September 2008, there was only one on-site inspection of a bank, and the bank challenged the powers of FID-DANS inspectors to ask for information necessary for completing the inspection. FID-DANS proposed the issuance of three criminal citations related to that on-site inspection for refusal to provide access to bank documents and clients' files.

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 FID-DANS of any cash payment greater than 30,000 BGN ($22,500). Because of inconsistent interpretation of the cash reporting requirement, some believe it covers only cash deposits, allowing a loophole to exist to the benefit of money launderers by leaving an unknown percentage of large cash withdrawals or exchanges unreported. As mentioned previously, as of January 1, 2009, Bulgarian banks will have to include the actual amount of all cash deposits above the 30,000 BGN (approximately $22,500) cash

transaction reporting (CTR) threshold. This is in contrast to the previous requirement mandating banks report only that the transaction occurred but not the actual amount.

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.

Bearer shares can be issued by joint stock companies, although not by banks or state companies. There are no limitations on the issuance. The identity of the first owner is registered; however, subsequent sales are not recorded. The GOB indicated these share are rarely issued.

Bulgaria does not systematically track cross-border electronic currency transactions, thereby making Bulgaria an attractive entry point to funnel money into the European financial system. During the year, the FID-DANS noted an increase in flows of money through Bulgaria. Bulgaria's Customs Agency collects criminal intelligence from its officers at points of entry, reviews cash reporting documents, and requests assistance from foreign partners to determine whether cash couriers are engaged in criminal activity. Customs officers have intercepted enormous quantities of cash in hidden compartments in cars.

Cash transactions in Bulgaria have grown an average of 46 percent per year over the past three years (while the economy has grown, on average, about seven percent). In 2008, the FID-DANS received 344,897 CTRs, but only 592 STRs for a total value of 257,459,070 euros (approximately $347,569,740). Banks submitted 515 of the STRs. Given the scale of growth of cash transactions over the 30,000 BGN (approximately $22,500) reporting threshold, the number of STRs is exceptionally low. Some banks in Bulgaria have not filed any suspicious transaction reports in the past three years, with no clear consequence for the vast majority of them. Other locally-owned Bulgarian banks do inordinate volumes of their business in cash. Despite the cash intensive nature of Bulgaria's economy, the large volume of cash transactions being observed in Bulgarian business is disproportionate to ordinary, customary, and normal practices.

Historically 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. According to its most recent evaluation of Bulgaria conducted in 2007, the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force-style regional body, noted deficiencies in Bulgaria's STR reporting regime, citing (among other problems) a lack of reporting from nonbanking financial institutions. During 2008, FID-DANS noted that while the compliance by nonbank entities remained low, the quality of their STRs improved. As of September 2008, the FID-DANS inspected eight exchange offices, imposing fines in seven cases for a total of 20,000 BNG (approximately $13,000) for failure to identify clients or request declarations on the origin of funds, and for not filing STRs.

DANS and the Prosecution Service drafted an instruction regulating interaction mechanisms between the two entities, including elements on interaction of FID-DANS and the Prosecutors Office. The instruction also establishes a permanent Contact Group of four prosecutor sector heads within the Supreme Prosecutors Office of Cassation and four directors from DANS, including the FID Director, to coordinate and manage cooperation between the two entities. DANS also drafted another instruction regulating interaction mechanisms between DANS and the Interior Ministry. These two instructions, signed by the Chairman of DANS and the Prosecutor General and Minister of Interior, respectively, replace the prior instructions on cooperation mechanisms.

Although case law remains weak, there has been an increase in the prosecution of money laundering cases. In October 2006, the courts rendered the country's first two convictions for money laundering. Bulgaria still has failed to convict a major high-profile organized crime figure, and most money laundering cases involve relatively small amounts of money and lower level crime figures. In the first half of 2008, prosecutors worked on 106 pre-trial investigations compared to 54 for the same period of 2007, or a 51 percent increase in caseload. During this period, prosecutors filed five indictments in court (equal to the number of indictments in the first half of 2007), against eight persons (as compared to five persons in the first half of 2007). There were two convictions (as compared to four in the first half of 2007) and no acquittals. Bulgaria's location as a crossroads for the entry into Europe of southwest Asian narcotics suggests that drug monies flow as well, as do proceeds from

trafficking in persons and other crime activities. Money laundering has not figured prominently in legal cases against such perpetrators, though the Ministry of Interior is eager to strengthen its capacity in this area.

Although there are few indications of terrorist financing directly connected with Bulgaria, the possibility remains that terrorism-related funds can transit Bulgarian borders through cash couriers and other informal mechanisms. In 2008, FID-DANS received only one STR in the amount of 1,681,248 euros (approximately $2,269,685) related to possible terrorist financing. To date, no suspected terrorist assets have been identified, frozen, or seized by Bulgarian authorities. 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 authorizes the FID to use its resources and financial intelligence to combat terrorist financing along with money laundering. Bulgaria's STR reporting requirements with regard to terrorist financing are still deficient, however, lacking a reporting obligation covering funds suspected to be linked to terrorists or terrorist financing.

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, DANS, Council of Ministers, Supreme Administrative Court, Sofia City Court, and the Prosecutor General. The FID-DANS and the Bulgarian National Bank circulate the names of suspected terrorists and terrorist organizations found on the UNSCR 1267 Sanctions Committee's Consolidated List, the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224, and those designated by the relevant EU authorities.

Although alternative remittance systems may operate in Bulgaria, their prevalence 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 civil 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 Forfeiture 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. Since its establishment, the Commission has faced strong criticism and demands for its closure from both government officials who question its effectiveness and politically connected businessmen allegedly protecting their interests. Initial indications show that the Commission is starting to become effective despite the fact that the process is slow, requires preliminary criminal prosecution against the owner, and often results in assets being transferred to relatives or significantly undervalued. As of October 2008, the Commission froze five million BGN (approximately $3,300,000). During this period, the Commission noted that first instance courts in six cases (approximately 80 percent of the cases) granted claims for 2.8 million BGN (approximately $1,800,000). In one case, the Commission accepted a conviction from a U.S. federal court as the basis for asset freezing and forfeiture proceedings in Bulgaria.

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. As of October 2007, the FID had bilateral memoranda of understanding (MOU) regarding information exchange relating to money laundering

with 28 countries. The FID-DANS is authorized by law to exchange financial intelligence on the basis of reciprocity without the need of an MOU. As of October 2007, the FID-DANS sent 261 requests for information to foreign FIUs and received 54 requests for assistance from foreign FIUs.

Bulgaria participates in MONEYVAL, and the FID Director is the current Chairman of MONEYVAL. The FID-DANS is a member of the Egmont Group. Bulgaria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption.

Until December 2007, Bulgaria's legislative framework was largely viewed as consistent with international AML standards. The Act on the State Agency for National Security compromised the FID's independence and investigatory mandate. It is essential that the Government of Bulgaria rectify these shortcomings. It must clarify and strengthen the FID's inspection and sanctioning authorities. The GOB should also take steps to improve and tighten its regulatory and reporting regime, particularly with regard to nonbank sectors, bearer shares, and cash payments, including cash withdrawals and exchanges, cross border transactions, and real estate transactions. The GOB should correct the deficiencies in its STR system regarding suspected terrorist financing. 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. Interagency cooperation should be streamlined to ensure effective implementation of Bulgaria's anti-money laundering and counterterrorist financing regime, and to improve prosecutorial effectiveness in money laundering, trafficking, narcotics, and terrorist financing cases. To improve judicial review of money laundering cases, the Government should enhance the capacity of judges regarding money laundering and promote a consistent interpretation of money laundering and asset forfeiture laws. In order to remove the risk that criminal interests are able to regain possession of confiscated goods, the GOB should also clarify the authorities of the Asset Forfeiture Commission so as to provide a mechanism to manage and dispose of confiscated properties.

Burma

Burma is a major drug-producing country and its economy remains dominated by state-owned entities, including the military. Drug trafficking and human trafficking are the major sources of money laundering in Burma. Wildlife, gems, timber, and other contraband flow through Burma and are additional sources of money laundering, as is public corruption. 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. Regionally, value transfer via trade is of concern and hawala/hundi networks frequently use trade goods to provide countervaluation. 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 2008, the criminal underground faces little risk of enforcement and prosecution. Corruption in business and government is a major problem. Burma is ranked 178 out of 180 countries in Transparency International's 2008 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 Asia/Pacific Group on Money Laundering (APG)—the relevant FATF-style regional body (FSRB) continues to monitor developments there for a period of time after de-listing. In 2008, the FATF advised the GOB to enhance regulation of the financial sector, including the securities industry, and to ensure that the GOB responds adequately to any foreign requests for cooperation.

Burma underwent a mutual evaluation by the APG in July 2008. This evaluation assessed Burma's AML/CTF regime as noncompliant or only partially compliant in all but four of the FATF 49 recommendations, a clear indication that Burma remains highly vulnerable to money laundering and terrorism finance threats. Key findings in the report included the observation that Burma has no law specifically penalizing terrorism as a separate crime, and has not enacted a law specifically criminalizing terrorist financing and designating it as one of the predicate offences to money laundering. In addition, the prevalent use of the U.S. dollar in Burma makes cash courier/currency smuggling of U.S. dollars an attractive method of laundering illicit proceeds.

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 2004. 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 $75,000). Between 2004 and August 2008, more than 86,000 cash transaction reports were filed. However, the FIU lacks a separate budget and its independence is hampered by the operational role of the Central Control Board (CCB) in Suspicious Transaction Reporting (STR) processing. 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 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, 2007,

and 2008. 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 anti-money laundering (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. However, there are significant inadequacies in the Control of Money Laundering Law and regulations for a number of key preventive measures including the obligation to identify persons who either control or are the actual beneficial owners of corporations and the absence of application of customer due diligence to existing customers or to politically exposed persons (PEPs).

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. However, there is no law or regulation that requires the licensing or registration of informal money remitters (Hundi), other than as financial institutions. In March 2008, the CCB brought additional nonbank financial institutions, including the Andaman Club Resort Hotel and gems and jade trading companies (both wholesale and retail) under the AML/CTF compliance regime. However, there is no law or regulation that requires the licensing or registration of informal money remitters (Hundi), (other than as financial institutions) or to Designated Non-Financial Businesses and Professions. The Central Bank also required banks and financial institutions to maintain all records and documents related to customer accounts and transactions for a minimum of five years. Currently, there are 4 state-owned banks, 15 domestic private banks and a few nonbank financial institutions, which include a state-owned insurance enterprise, a state owned small loan enterprise, and a private owned leasing company.

The Law Relating to Forming Organizations (LRPO) governs Non-Profit Organizations (NPOs) of which there are three hundred and two registered under this law, seventy-eight of which have international connections. There has been no comprehensive review of the LRFO or the NPO sector including any review to assess the

vulnerabilities to terrorist financing, nor is there any requirement for NPOs to maintain and make their records available to public authorities.

As of August 2008, a total of 1,495 STRs had been received. In 2007, nine cases were identified as potential money laundering investigations. As of August 2008, the FIU received 444 STRs, of which seven cases were identified as potential money laundering investigations. The FIU has investigated four cases to date, two of which were sent to the courts for prosecution. According to the 2008 Asia Pacific Group on Money Laundering (APG) Mutual Evaluation Report, there has been only one conviction for money laundering itself since 2004 despite twenty-three money laundering investigations and fifty-four people having been convicted for predicate crimes under the "Control of Money Laundering Law.

The United States maintains the anti-money laundering measures it adopted against Burma in 2004, identifying 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 measures prohibit 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.

The United States also maintains other sanctions on Burma, which include bans on certain importations, new investment, and certain financial transactions, as well as a visa ban on selected individuals. Under the Block Burmese JADE (Junta's Anti-Democratic Efforts) Act of 2008, the Burmese Freedom and Democracy Act of 2003,

and several Executive Orders, the United States bans the transfer of funds and other provision of financial services to Burma by any U.S. person, freezes assets of the ruling junta and other Burmese individuals and entities, and prohibits the import of all Burmese-origin goods into the United States (with tighter restrictions on jadeite and rubies). Additional U.S. laws—such as 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, and the Tariff Act (19 USC 1307)—place further restrictions on financial transactions with Burma. Other U.S. sanctions, such as visa bans on certain individuals affiliated with the military regime, also apply to Burma.

In September 2008, the United States Government identified Burma as one of three countries in the world that had "failed demonstrably" to meet its international counternarcotics obligations. On November 13, 2008, the Office of Foreign Assets Control in the Department of the Treasury named 26 individuals and 17 companies tied to Burma's Wei Hsueh Kang and the United Wa State Army (UWSA) as Specially Designated Narcotics Traffickers pursuant to the Foreign Narcotics Kingpin Designation Act (Kingpin Act). Wei Hsueh Kang and the UWSA were designated by the president as Foreign Narcotics Kingpin on June 1, 2000 and June 2, 2003 respectively.

Burma became a member of the Asia Pacific Group on Money Laundering in 2006. The GOB is a party to the 1988 UN Drug Convention. Over the past several years, Burma has expanded its counternarcotics 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 to the UN Convention for the Suppression of the Financing of Terrorism. Burma is not a party to the UN Convention on Corruption. Burma signed the Treaty on Mutual Legal Assistance in Criminal Matters among Like-Minded ASEAN Member Countries in

January 2006, and deposited its instrument of ratification with the Attorney General of Malaysia in January 2009.

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/counterterrorist 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 financial sector, including its banks, its DNFBPs as well as its NPOs. The GOB should 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 and the FIU should become a fully funded independent agency that is allowed to function without interference. Customs should be strengthened and authorities should monitor more carefully the misuse of trade and its role in informal remittance or hawala/hundi networks. Burma should become a party to the UN Convention against Corruption. 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. Finally, the GOB should adhere to all laws and regulations that govern anti-money laundering and terrorist financing to which it is committed by virtue of its membership in the UN and the APG.

Cambodia

Cambodia is neither an important regional financial center nor an offshore financial center. The major sources of money laundering are widespread human trafficking and exploitation, drug trafficking, and corruption. Cambodia serves as a transit route for drug trafficking from the Golden Triangle to international drug markets such as Vietnam, mainland China, Taiwan, and Australia. Cambodia's fledgling anti-money laundering regime, a cash-based economy with an active informal banking system, porous borders with attendant smuggling, limited capacity of the National Bank of Cambodia (NBC) to supervise a rapidly expanding banking sector, and widespread

corruption continue to contribute to a significant money laundering risk. 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 the 2003 case involving Jemaah Islamiyah (JI). However, with the 2007 enactment of the "Law on Anti-Money Laundering and Combating the Financing of Terrorism" (AML/CTF) and the subsequent May 2008 implementing regulation, and the enactment of the "Law on Counter Terrorism" Cambodia has created a foundation to combat acts of money laundering and terrorist financing within the banking sector. Additional implementing regulations are needed to bring all designated nonfinancial businesses and professions (DNFBPs) into compliance with reporting requirements established in the AML/CTF law.

The AML/CTF law was promulgated in June 2007 and provides the framework for the Cambodian Financial Intelligence Unit (CAFIU) to exert control over banks and DNFBPs, such as casinos and realtors and entities to be designated by the CAFIU. The NBC is making strides to regulate large or suspicious financial transactions. There were two suspicious cases reported as of the third quarter of 2008 and investigations are ongoing. The Prakas (implementing regulation) on the AML/CTF law was issued on May 30, 2008, and was soon to put into force. The new Prakas places a wide range of AML/CTF obligations on banks and financial institutions that are regulated by the NBC. Since then, the CAFIU has been working with the Ministry of Interior, Ministry of Justice, and other relevant ministries to take cooperative action, ranging from identifying and reporting suspicious financial transactions, raising awareness, to lodging judicial complaints to the Ministry of Justice for court action on possible cases. The Prakas requires all reporting entities regulated by the NBC to report on a regular basis and to establish internal control systems for AML/CTF procedures to be fully compliant with the law. However, additional decrees are necessary to establish reporting procedures and formats for DNFBPs to fully implement the AML/CTF law. The Ministry of Interior has a legal responsibility for general oversight of casinos operations and providing security; however, in practice it exerts little supervision. The Ministry of Interior is authorized to investigate cases of suspicious transactions reported to it by the CAFIU.

Cambodia's banking sector is relatively small, yet rapidly expanding, with 25 commercial banks (an increase of ten in the last year); six specialized banks; 18 registered micro-finance institutions (MFIs); 3,808 money exchangers (556 in Phnom Penh and 3,252 in the provinces); and 26 registered and roughly 60 unregistered NGO credit operators. Bank operations are widely made on a cash basis and predominantly in U.S. dollars. Recently, the Royal Government of Cambodia (GOC) encouraged the use of the national currency (the riel) in lending and borrowing. Despite an increase in the use of banking and finance systems, overall lending and banking activities remain low due to lack of trust and prohibitive interest rates on loans. Increased borrowing and loans are due mainly to expansion in the construction and real estate sectors. Economists note that while a typical country would have a bank deposit to GDP ratio of roughly 60 percent, Cambodia's ratio is only 26.2 percent (August 2008), 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. In addition to banks, individual and legal persons can undertake foreign exchange provided they register with the NBC.

The NBC has regulatory responsibility for the banking sector, and it audits and inspects individual banks on-site on an annual basis to ensure full compliance with laws and regulations. Moreover, off-site investigations can be made on a daily, weekly, or monthly basis contingent upon each individual case. The AML/CTF law requires that banks and other financial institutions report transactions over 40,000,000 riel (approximately U.S. $10,000). However, large cash reporting is not yet implemented due to lack of a database within the CAFIU. While there are no reports to indicate that banking institutions themselves are knowingly engaged in money laundering, until the CAFIU was established, government audits would likely not have been 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 on average by about 41.6 per cent per year from 2004 to 2007. From January to August of 2008, deposits grew on average by 52 percent, due in part to new increased deposit requirements. 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, continues to grow.

Cambodia lacks meaningful statistics on the extent of financial crime that exists and only a few crime statistics and limited open source information is available to evaluate the major sources of illicit funds. Despite the establishment of the CAFIU, some larger-scale money laundering in Cambodia may also flow through informal banking activities and/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 across borders. The black market in Cambodia for smuggled goods, including drugs and imported substances for local production of the methamphetamine ATS, is notable. Most of the smuggling is intended to circumvent official duties and evade tax obligations and involves items such as fuel, alcohol optical disks, and cigarettes. Some government officials and their private sector associates have some control over the smuggling trade and its proceeds. Cambodia's economy is cash-based and largely dollarized, and the smuggling trade is usually conducted in U.S. dollars. Such proceeds are rarely transferred through the banking system or other financial institutions. Instead, they are readily channeled into land, housing, luxury goods or other forms of property. Cambodia's urban real estate sector, fueled by foreign investment, has witnessed rapid growth and soaring prices in recent years.

The CAFIU is under the control and financing of the NBC with a Permanent Secretariat working under the supervision of a Board of Directors composed of one senior representative each from the NBC, Council of Ministers, and the Ministries of Economy and Finance, Justice, and Interior. Under Article 5 of the Prakas on AML/CTF, banks and financial institutions are required to conduct customer due diligence when carrying out an occasional or one-off transaction that involves a sum in excess of U.S. $10,000 (or 40 million riel or foreign currency equivalent) or a wire transfer that involves a sum in excess of U.S. $ 1,000 (or 4 million riel or other equivalent foreign currency). The CAFIU has also offered "Know Your Customer" and other training to banking institutions to inform them of their obligations under the new AML/CTF regime.

The CAFIU has the authority to apply anti-money laundering requirements to DNFBPs such as casinos and other intermediaries, such as lawyers, notaries, and accountants. The major nonbank financial institutions in Cambodia are the casinos, which the

authorities have noted are particularly vulnerable to money laundering. By law, foreigners, but not Cambodian nationals, are allowed to gamble in 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 CAFIU has the authority to receive and disseminate reports, including suspicious transaction reports, on casino financial transactions and cooperate with casino regulators on AML/CTF. There are currently 27 operational licensed casinos in Cambodia, a few other licensed casinos are under construction, and there are an unrecorded number of small-sized gambling houses. Most casinos are located along Cambodia's north-west border with Thailand and along the Cambodia's southeastern border with Vietnam. However, one can also find casinos and so-called 'gambling houses' at hotels in major cities and towns. 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 or 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 NBC. 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 to seize the cash or instruments involved. Therefore, Cambodia does not at present have a system in place for effective monitoring cross border movement of cash and monetary instruments as required by international standards on AML/CTF.

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 2007 AML/CTF law, these 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 Draft Criminal Code, which is currently under consideration by the Council of Ministers, has provisions to criminalize money laundering in relation to proceeds from all serious crime.

The 2007 Law on Counter Terrorism criminalizes terrorist financing; and regulations on transactions suspected of financing terrorism are covered by the AML/CTF law. Under the 2007 Law on Counter Terrorism, the Minister of Justice may order the prosecutor to freeze property of a legal or natural person if that person 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 May 2008, the UN Counter-Terrorism Committee Executive Directorate (CTED) visited Cambodia and commended the GOC for the significant progress achieved in developing its AML/CTF regime but also noted remaining deficiencies. The CTED recommended that the CAFIU be further empowered to develop implementation and coordination procedures and undertake related training and public awareness campaigns. The CTED also recommended the development of procedures to ensure adequate AML/CTF measures, in particular for casino operations and real estate transactions.

Cambodia is a party to the UN Drug Convention, the UN Convention Against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. In June 2004, Cambodia joined the Asia/Pacific Group on Money Laundering (APG), a Financial Action Task Force (FATF) style regional body.

The Government of Cambodia (GOC) should take steps enact the Draft Criminal Code as a matter of priority so as to adopt a money laundering offence for proceeds of all serious crime. In addition, the GOC should strengthen control over its porous borders as well as increase the capability of its nascent FIU. The GOC should issue additional decrees necessary to fully implement the AML/CTF law—particularly implementing provisions relating to designated nonfinancial businesses and professions mandating compliance with reporting requirements established in the AML/CTF law. Developing the capability of its law enforcement and judicial authorities to investigate, prosecute, and adjudicate financial crimes are necessities. Establishing a national coordination group, including all relevant agencies involved in AML/CTF issues should be considered a high priority for the GOC to ensure that its AML/CTF regime comports with international standards.

Canada

Money laundering in Canada is primarily associated with drug trafficking and financial crimes, particularly those related to fraud. According to the Canadian Security Intelligence Service (CSIS), criminals launder an estimated $5 to $17 billion each year. With $1.5 billion in trade crossing the border each day, the United States and Canadian governments share concerns about illicit cross-border movements of currency, particularly the proceeds of drug trafficking. Organized criminal groups

involved in drug trafficking also remain a challenge. CSIS estimates that approximately 950 organized crime groups operate in Canada, with approximately 80 percent of all crime groups in Canada involved in the illicit drug trade.

The Government of Canada (GOC) enacted the Proceeds of Crime (Money Laundering) Act in 2000 to criminalize money laundering, facilitate the investigation and prosecution of money laundering, and create the financial intelligence unit (FIU), known as 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 law expands the list of predicate money laundering offenses to cover all indictable offenses, including terrorism and trafficking in persons.

The PCMLTFA created a mandatory reporting system for suspicious financial transactions, large cash transactions, large international electronic funds transfers, and suspected terrorist property. Failure to file a suspicious transaction report (STR) could result in up to five years' imprisonment, a fine of approximately $2 million, or both. The law protects those filing suspicious transaction reports from civil and criminal prosecution.

The PCMLTFA requires reporting of all cross-border movement, including through the mail system, of currency and monetary instruments totaling or exceeding C$10,000 (approximately $7931), to the Canadian Border Services Agency (CBSA). Failure to report cross-border movements of currency and monetary instruments could result in seizure of funds or penalties ranging from C$250 to C$5,000 (approximately $198 to $3966). The CBSA forwards cross-border and cash seizure reports to FINTRAC. The CBSA also provides evidence to the RCMP, which investigates and brings charges. From April 2007 through March 2008, CBSA seizures totaled C$40 million (approximately $31.72 million). In the same interval, CBSA executed 130 "Level IV" seizures, which occur when a CBSA officer suspects funds are proceeds of crime or linked to terrorist activities.

In December 2006, Parliament passed Bill C-25, amending the PCMLTFA. This legislation expands the coverage of Canada's anti-money laundering (AML) and counterterrorist financing (CTF) regime and applies to banks; credit unions; life insurance companies; trust and loan companies; brokers/dealers of securities; foreign

exchange dealers; money services businesses; sellers and redeemers of money orders; accountants; real estate brokers; and casinos. In December 2008, lawyers, notaries (in Québec and British Columbia only) and dealers in precious metals and stones became subject to the PCMLTFA. However, lawyers in several provinces have successfully filed legal challenges to the applicability of the PCMLTFA to them based upon common law attorney-client privileges, so lawyers are not completely covered by the AML provisions.

Bill C-25 enhances client identification and record-keeping by requiring greater scrutiny of correspondent banking relationships; enhanced monitoring of politically exposed persons; expanded record keeping and due diligence requirements for real estate agents and brokers; mandatory risk assessments to mitigate high risk activities for money laundering and terrorist financing; originator information for outgoing international wire transfers; and information on the beneficial owners of corporations. The Bill mandates that FINTRAC create a national registry for money service businesses, and establish a system to render administrative monetary penalties for noncompliance effective December 2008. FINTRAC's administrative monetary penalties regime provides for fines of up to C$1,000 ($793) for a minor violation, up to C$10,000(approximately $7931) for a serious violation, and as much as C$500,000 ($396,445) for a very serious violation.

In February 2008, the Financial Action Task Force (FATF) adopted a mutual evaluation report (MER) of Canada. The report stated that although Canada has strengthened its overall AML/CTF regime, shortcomings still existed, including the scope and coverage of the AML/CTF requirements applicable to designated nonfinancial business and professions. The report also cited concern regarding FINTRAC's effectiveness communicating relevant information to law enforcement authorities. The mutual evaluation on-site assessment visit took place after the passage of Bill C-25, but before Canada could implement all related measures. In June 2008, Canada implemented the bill, resulting in a somewhat stronger comportment with international standards. As a result of the implementation of the bill, authorities introduced a risk-based approach, required new client identification and recordkeeping requirements for real estate agents and brokers, and established a national registry of money service businesses to ensure sector compliance and transparency. Bill C-25

also permits FINTRAC to include additional information in the intelligence product that it can disclose to law enforcement and national security agencies.

While Canada's Office of the Superintendent of Financial Institutions (OSFI) and other federal and provincial regulatory agencies supervise institutions for safety and soundness, FINTRAC is the sole authority with the mandate to ensure compliance with the PCMLTFA and associated regulations. FINTRAC recently revised regulations and guidelines explaining the PCMLTFA and its requirements to incorporate the most recent implementation of Bill C-25 effective June 2008. The guidelines provide an overview of FINTRAC's mandate and responsibilities, and include background information about money laundering and terrorist financing. The guidelines also provide an outline of requirements for maintaining a compliance regime, record-keeping, client identification, and reporting transactions.

Operational since 2001, FINTRAC is an independent agency with regulatory and FIU functions. FINTRAC has a staff of approximately 320 employees that work as analysts, compliance officers, and information technology specialists. FINTRAC receives and analyzes reports from regulated entities as mandated by the PCMLTFA, and disseminates its findings—disclosures—to law enforcement and intelligence agencies. 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 requires an MOU in order to exchange information and has signed 53 MOUs with foreign counterparts. From April 2007 to the end of March 2008, Canada sent 62 case disclosures to partner FIUs.

FINTRAC received over 21 million reports from reporting entities between April 2007 and the end of March 2008. These reports included more than 50,000 STRs more than 5.5 million cash transaction reports, in excess of 50,000 cross-border reports, and more than 16 million electronic funds transfer reports (which includes funds that enter and exit the country). FINTRAC may only disclose information related to money laundering or terrorist financing offenses. FINTRAC produced a total of 210 case disclosures between 2007 and 2008. Of the 210 case disclosures, 171 were suspected money laundering, 29 were suspected terrorist activity, and 10 involved suspected money laundering, terrorist financing, and/or threats to the security of Canada.

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. 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. From April 2007 through the end of March 2008, FINTRAC conducted 277 examinations with national and provincial regulatory agencies conducing 257 examinations for their respective sectors. FINTRAC identified and disclosed five cases of noncompliance for further law enforcement investigation and prosecution. OSFI completed 13 AML on-site compliance examinations of financial institutions. The Department of Finance has established a public/private sector advisory committee and is now coordinating a National Risk Assessment. In May 2008, the OSFI held an information session on the risk-based approach.

Although all Canadian police forces can investigate money laundering and terrorist financing offenses, the Royal Canadian Mounted Police (RCMP), in particular its Integrated Proceeds of Crime Initiative (IPOC) Units, and the provincial law enforcement authorities in Ontario (the Ontario Provincial Police) and Québec (Sûreté du Québec) undertake virtually all money laundering and terrorist financing investigations. In 2007, the RCMP opened 73 money laundering cases, and opened seven in the first four months of 2008; most have not concluded. The RCMP also seized approximately $8.9 million and forfeited $283,000 in 2007. In the first half of 2008, RCMP seized approximately $484,000.

The attorney general of Canada (through public prosecution offices) and provincial attorney generals prosecute money laundering and terrorist financing cases. In 2007, authorities charged targets with 150 possession of proceeds of crime charges, three specifically for money laundering, and in the first four months of 2008 registered four such charges, none specific to money laundering. In 2007 prosecutors obtained five convictions of the original 150 and none in 2008.

The PCMLTFA enables Canadian authorities to identify, deter, disable, prosecute, convict, and punish terrorist groups. The PCMLTFA expands FINTRAC's mandate to include counterterrorist financing and allow disclosures to CSIS of information related

to financial transactions relevant to threats against Canadian security. The GOC also designates suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list. Financial institutions must freeze the assets of those designated. The PCMLTFA also prohibits fundraising for these organizations. There are currently more than 500 individuals and entities associated with terrorist activities designated by the GOC. Investigations indicate that terrorist cells generate funds locally through drug trafficking and various fraud schemes, and terrorist groups employ identical methods to money launderers including bulk cash smuggling; the use of the formal banking sector; money exchange/transfer services; and emerging technology such as internet transfer systems. To deter the exploitation of nonprofit and charitable organizations by terrorists, the 2001 reforms criminalize knowingly collecting or providing funds to carry out terrorism. They also denied or removed special charitable status from nonprofits supporting terrorism; and facilitated freezing and seizing their assets.

Canada has longstanding agreements with the U. S. on law enforcement cooperation, including treaties on extradition and mutual legal assistance, as well as an asset sharing agreement. Recent cooperation concerns focus on the inability of U.S. 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 between the CBSA and the U.S. Department of Homeland Security's Immigration and Customs Enforcement (ICE) on exchange of cross-border currency declarations expanded the extremely narrow disclosure policy. However, the scope of the exchange remains restrictive. To remedy this, the CBSA is developing an information-sharing MOU with the United States related to its Cross-Border Currency Reporting Program.

Canada is a party to the UN 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.

Canada is a member of the FATF as well as the Asia/Pacific Group on Money Laundering (APG), and is a supporting nation of 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 is a

member of the Egmont Group, which maintains its Secretariat in Toronto. The GOC is contributing approximately $5 million over a five-year period to help establish the Secretariat.

The Government of Canada has demonstrated a strong commitment to combat money laundering and terrorist financing both domestically and internationally. In 2008, the GOC continued to make strides in enhancing its AML/CTF regime, and reducing its vulnerability to money laundering and terrorist financing. The GOC should continue to 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. FINTRAC should maintain its new registry of money services bureaus, making use of the registry and executing compliance examinations. The GOC should also continue to improve the communication between FINTRAC and law enforcement authorities. The GOC should ensure effective reporting of cross-border reports to FINTRAC and increase efforts to share information in this regard with U.S. counterparts.

Cayman Islands

The Cayman Islands, a United Kingdom (UK) Caribbean overseas territory, continues to make strides in strengthening its anti-money laundering and counterterrorist 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 and drug trafficking. Due to their status as a zero tax regime, the Cayman Islands is also considered attractive to those seeking to evade taxes in their home jurisdiction.

The Cayman Islands is home to a well-developed offshore financial center that provides a wide range of services, including banking, structured finance, and investment funds, various types of trusts, and company formation and management. As of December 2008, there are approximately 278 banks, 159 active trust licenses, 773 captive insurance companies, seven money service businesses, and more than 62,572 exempt companies licensed or registered in the Cayman Islands. At the end of June 2008, there were 10,037 hedge funds registered, up from 9,413 at the end of 2007, according to the Cayman Islands Monetary Authority (CIMA). 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. As an offshore financial center with no direct taxes and a strong reputation for having a stable legal and financial services infrastructure, the Cayman Islands is attractive to businesses based in the United States and elsewhere for legal purposes but also equally attractive to criminal organizations seeking to disguise the proceeds of illicit activity.

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.

The Proceeds of Crime Law 2008 (POCL) came into effect in September 2008. The law repeals and replaces the Proceeds of Criminal Conduct Law (2007 revision). The POCL introduces the concept of criminal property (includes terrorist property) that constitutes a person's benefit (directly or indirectly) from criminal conduct; tax offenses are not included. No longer applicable to an indictable offense, the term criminal conduct was also amended to cover any offense. Extraterritorial and appropriate ancillary offenses are covered in domestic legislation and criminal liability extends to legal persons. The POCL also consolidates the law relating to the confiscation of the proceeds of crime and the law relating to mutual legal assistance in criminal matters. The penalties for money laundering are $5000 Cayman Island (KYD) dollars (approximately $6,125) fine and/or imprisonment for two years for summary conviction, and a fine and/or imprisonment for 14 years on conviction on indictment.

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 counterterrorist 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 Money Laundering (Amendment) Regulations 2008, which came into force on October 24, 2008. A 2007 amendment to the Money Laundering Regulations brought dealers of precious metals and stones under the definition of relevant financial businesses, and they were 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.

Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing (Guidance Notes) are issued by the CIMA and were last amended in December 2008. The amendments, among other things, require institutions to keep appropriate evidence of client identification, account opening or new business documentation. Adequate records identifying relevant financial transactions should be kept for a period of five years following the closing of an account, the end of the transaction or the termination of the business relationship. This includes records pertaining to inquiries about complex, unusual large transactions, and unusual patterns of transactions. The amendments also address correspondent banking and enhanced due diligence procedures. Financial institutions are prohibited from correspondent relationships with shell banks. In addition, financial institutions must satisfy that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

The CIMA conducts on-site and off-site examinations of licensees. These examinations include monitoring for compliance with the POCL and the CIMA's Guidance Notes. Additional requirements of 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 KYD $15,000 (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.

Tipping off provisions were broadened through the POCL and include situations where an individual knows or suspects that criminal conduct is about to take, is presently taking, or has taken place. The penalties for tipping off were increased to a KYD $5000 fine and/or imprisonment for two years for summary conviction, and a fine and/or imprisonment for five years on conviction on indictment.

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. From June 2007 through June 2008, the FRA reviewed 247 cases and made 70 disclosures to domestic and foreign law enforcement and regulatory agencies. The majority of reports filed were related to suspicious financial activity, fraud, and money laundering. Under the PCCL, the FRA has the authority to require all obligated entities to provide additional information related to a SAR. The FRA can request a court order to freeze bank accounts if it suspects the account is linked to money laundering or terrorist financing. The FRA is an active member of the Egmont Group and has Memoranda of Understanding in place with Australia, Canada, Chile, Guatemala, Indonesia, Mauritius, Nigeria, Thailand, and the United States.

The Financial Crime Unit (FCU) of the Royal Cayman Islands Police Service (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. In July 2008, the FCU arrested an individual in connection with the collapse of

the Grand Island Fund following serious irregularities in the fund's trading activities. The collapse of the fund is believed to involve millions of dollars. The FCU investigation is ongoing.

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 KYD $15,000 (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 the 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. The POCL provides the Attorney-General with the ability to issue restraint orders once an investigation has begun without the need to bring charges within 21 days. Confiscation orders may also now be made by the Attorney-General upon conviction in either Summary or Grand Courts. The legislation also permits the Attorney General to bring civil proceedings for the recovery of the proceeds of crime. 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 (TUNMOTO). 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 (MLAT) 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. Many U.S. investigations involve, at some stage, a defendant who has secreted funds in the Caymans, often in accounts held by offshore trust entities. Although generally helpful when receiving formal MLAT requests from the U.S. for assistance, the Cayman Islands has not been proactive with regard to money laundering prosecutions based on its own investigations.

The Cayman Islands is a member of the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body. In November 2007, CFATF conducted its third mutual evaluation of the Cayman Islands. The evaluation found the Cayman Islands to be compliant or largely compliant with 38 of the Forty-Nine Financial Action Task Force recommendations and noted that a strong culture of compliance exists within the AML/CTF regime. However, recommendations to address remaining weaknesses were identified. Over the course of 2008, the Cayman Islands revised legislation in accordance with most of the recommendations made in the report including the following: The Proceeds of Crime Law (POCL) was enacted in June 2008; The Money Laundering (Amendment) Regulations 2008 became enforceable in October 2008; The Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing (GN) was revised and issued in September 2008.

In March 2008, the United Kingdom published The Foreign and Commonwealth Office: Managing Risk in the Overseas Territories. In terms of AML/CTF, the Foreign and Commonwealth Office indicated that regulatory standards in most Territories are not up to those of the Crown Dependencies (Jersey, Guernsey and the Isle of Man) and that a lack of capacity has reduced the ability of Territories to investigate and prosecute money laundering. However, the report noted that only the Cayman Islands has, so far achieved successful prosecutions of local participants for offshore money laundering offenses. This trend will hopefully continue in the future, as it sets a model for other offshore financial sectors in the Caribbean basin. There have been only five money laundering convictions in the Cayman Islands since 2003, which is not a large

amount considering the size of the Caymans' financial sector and the volume of offshore entities holding assets there.

In July 2008, the U.S. Government Accountability Office (GAO) issued a report entitled: "Cayman Islands: Business and Tax Advantages Attract U.S. Persons and Enforcement Challenges Exist." The report was conducted in response to a Congressional inquiry regarding offshore tax evasion; the business activities of U.S. taxpayers involving a corporate service provider in the Cayman Islands; the extent, motives, and tax implications of these activities; and the extent that the U.S. government has examined these activities.

The report found that U.S. persons who conduct financial activity in the Cayman Islands commonly do so to gain business advantages, such as facilitating U.S.-foreign transactions or to minimize or obtain tax advantages; while much of this activity is legal, some is not. In June 2008, two former Bear Stearns hedge fund managers were arrested and indicted in the U.S. on conspiracy and fraud charges related to the collapse of two Cayman Islands funds they oversaw. A companion civil suit to recover over $1.5 billion in losses was filed against four individuals and companies in the Cayman Islands. The report did highlight the cooperation between U.S. agencies and its Cayman counterparts in investigating money laundering, financial crimes, and tax evasion. In general, U.S. officials said that cooperation with its Cayman counterparts has been good and that compliance problems are not more prevalent than elsewhere offshore.

The Government of the Cayman Islands bolstered its AML/CTF regime in 2008, to be in accordance with international standards. However, for a jurisdiction with one of the largest and most developed offshore sectors, the Cayman Islands should continue to strengthen and implement its AM.L/CTF regime to include ensuring the new provisions related to AML/CTF requirements for dealers in precious metals and stones. Additionally, the disclosure/declaration system for the cross-border movement of currency should be fully implemented. The Cayman Islands also should work to fully develop its capacity to investigate and prosecute money laundering and terrorist financing cases.

Chile

Chile has a large and well-developed banking and financial sector. Systemic vulnerabilities in Chile's anti-money laundering and combating the financing of terrorism (AML/CTF) regime include stringent bank secrecy laws that emphasize privacy rights impede Chilean efforts to identify and investigate money laundering and terrorist financing, as well as relatively new regulatory institutions in which oversight gaps remain. The Government of Chile (GOC) is actively seeking to turn Chile into a global financial center, but not an offshore financial center. Chile has Free Trade Agreements with 55 countries and is negotiating four more. Increased trade and currency flows, combined with an expanding economy, could attract illicit financial activity and money laundering. Given Chile's extensive trading partnerships and long and somewhat porous borders, its largely unregulated free trade zones are additional vulnerabilities. Illicit proceeds from limited drug trafficking and domestic consumption are laundered in the country.

Chile criminalized money laundering under Law 19.366 of 1995, Law 19.913 of 2003, and Law 20.119 of 2006. Law 19.913 identifies predicate offenses for money laundering, which include narcotics trafficking, terrorism in any form and the financing of terrorist acts or groups, illegal arms trafficking, kidnapping, fraud, corruption, child prostitution, 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.

Chile's financial intelligence unit (FIU) is the Unidad de Análisis Financiero (UAF), created by Law 19.913. The UAF is an autonomous agency affiliated with the Ministry of Finance and has a staff of 32—an increase from 21 personnel in 2007. It does not have criminal investigative or regulatory responsibilities. Law 19.913 requires mandatory reporting of suspicious transactions to the UAF, but does not establish specific parameters to determine irregular or suspicious activity. The UAF may access any government information (police, taxes, etc.) not covered by secrecy or privacy laws. The UAF can issue general instructions, such as requiring obligated entities to report any transactions by persons suspected of terrorist financing.

Financial institutions subject to suspicious transaction reporting requirements include banks, savings and loan associations, 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, and sports clubs. 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) (450 UF is approximately $15,000). 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 six 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. The UAF had received 1,312 CTRs through June 2008, and 311 STRs through September 2008.

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. Since the beginning of 2008, a new pilot system that allows for better management of information by the UAF was put in place. The system allows Customs to file its reports directly from the place where the activity being reported is taking place. At this point, the system is fully operational at the Santiago Airport's Customs and in the process of being implemented in the rest of the country.

Law 20.119 authorizes the UAF to impose sanctions on obligated entities if they fail to comply with requirements to establish an AML/CTF system or report suspicious cash transactions. The sanctions range from warning letters to fines. In 2008, the UAF identified 35 cases where entities failed to comply with ALM/CTF requirements or report suspicious cash transactions. The UAF levied fines in 29 of the 35 cases. Of these 35 cases, nine involved factoring companies and eight involved currency exchange houses.

The UAF continues to develop its capabilities. In 2008, it created a compliance division to ensure that required entities meet reporting requirements. The compliance division will initially focus on currency exchange houses. The Association of Banks and Financial Institutions, the Superintendence of Banks and Financial Institutions (SBIF), and the UAF provide training and resources to required reporting entities. In 2008, the UAF organized several money laundering seminars for compliance officers at banks and currency exchange houses. The UAF also issued instructions to customs agents and real estate agents that emphasized the importance of "know your customer" (KYC) requirements.

The SBIF supervises and regulates banks in Chile. 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 KYC standards and other money laundering controls for checking accounts. 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.

Chile's gaming industry is supervised by the Superintendence of Casinos (SCJ). The SCJ is responsible for drafting regulations about casino facilities and managing the development of the industry. Online gambling is prohibited except for the Internet purchase of lottery tickets from one of Chile's two lotteries. Sixteen 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 new casinos to operate in Chile after

participating in an international and domestic bidding process to assign permits during 2005 and 2006. Eight new casinos opened in 2008. Six more are expected to open in 2009, bringing the total number of casinos to 22. The SCJ screened applications for the new casino licenses with the support of domestic and international police and financial institutions. Chilean law, however, limited 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 (approximately $15,000) and to designate a compliance officer. According to the GOC, the UAF issued a regulation jointly with the SCJ, which verifies that to date 100 percent of operational casinos have: a compliance officer; an AML/CTF manual; and on site supervision and enforcement. In addition, the UAF instructed casinos to identify, know, and maintain records on all customers—Chileans and foreigners—who carry out any cash transaction over $3,000; this is a reduction in the cash transaction threshold from $10,000. The SCJ also requires the casinos to prepare and submit for approval manuals detailing their AML/CTF plan The SCJ is actively 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.

While the regulatory and oversight system established by Chile for banks, financial institutions, and the gaming industry provides a foundation to combat money laundering, there are weaknesses. For example, there is no common definition for "suspicious activity" among financial institutions. The UAF publishes a list of warning signs to help reporting entities identify suspicious activity, but financial institutions are given wide latitude to police themselves regarding activities that could be considered suspicious. Another weakness is the absence of regulatory oversight for nonbank financial institutions such as money exchange houses and cash couriers. There are more than 60 money exchange houses in Santiago and 125 registered with the UAF throughout the country. While money exchange houses must register with the UAF, they are not supervised by any regulatory body. Non-bank 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. This sector appears particularly vulnerable to abuse by money launderers.

The Public Ministry directs the investigation and prosecution of money laundering cases. When the UAF receives a STR or a CTR, it analyzes the information and determines if an account or a case requires further investigation. If a case requires further investigation, the UAF passes the information to the Public Ministry. 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. Through September, the UAF referred 47 cases to the Public Ministry.

The Public Ministry's unit for money laundering and economic crimes proactively investigates potential crimes and seeks opportunities to enhance its capabilities. Public prosecutors in all regions have received training on money laundering. The money laundering unit has also developed reference materials for prosecutors, including a manual that provides practical steps to investigate assets in order 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 (PDI) and the uniformed national police (Carabineros) work in conjunction with the Public Ministry on money laundering investigations. The PDI has an economic crimes division and a unit dedicated to money laundering investigations. They also cooperate with U.S. and regional law enforcement in money laundering investigations. In 2004, this cooperation resulted in the break-up of an international money laundering ring that involved smugglers in Colombia, Chile and the United States.

The Public Ministry and police are competent and professional, but there are several factors that limit their ability to successfully investigate and prosecute money laundering cases. The units in charge of money laundering investigations and prosecutions are new and do not have extensive experience. There is a shortage of qualified investigators to pursue cases, and some institutional resistance to the idea that money laundering is worth prosecuting. Regulations also restrict information

sharing among different agencies. Under the current money laundering laws, the UAF is prohibited from giving information directly to the PDI or Carabineros. The UAF is only permitted to share information with the Public Ministry and foreign FIUs. The PDI or Carabineros must request financial information from the Public Ministry, which in turn requests it from the UAF. The UAF responds with all available information, which the Public Ministry gives to the PDI or Carabineros, but this process costs valuable time.

The most significant obstacle to money laundering investigations is bank secrecy. Article 154 of the General Banking Law places all types of bank deposits and obligations under banking secrecy, and only allows banking institutions to share information about such transactions with the depositor or creditor (or an authorized legal representative). Law 707 states that banks may not share information about the movement and balances in a current account with a third party. Due to these legal restrictions, banks do not share information with prosecutors without a judicial order. Some banks and their compliance officers aggressively apply rigorous, international AML/CTF standards, but they are restricted to simply reporting suspicious activity and then waiting for the appropriate court authorization to release any private information. Other banks are slow to reply to judicial court orders to provide prosecutors with additional information. Police and prosecutors complain they lose valuable time waiting at least a month (but usually more) for some banks to provide 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 STR 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. 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 always received permission to examine an account when requested, but it has only made requests when it was confident the judge would comply. The system does not 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 under review 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 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. 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. 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 also 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. The GOC seized just over $2 million in assets in 2008.

The GOC pursued 14 money laundering cases in 2008. Eleven cases were tied to drug trafficking, two of which were by-products of public corruption cases, and one derived from a prostitution case. The public corruption and prostitution cases are the first money laundering cases to be prosecuted that are not tied to drug trafficking. One

case has led to a conviction and the other 13 cases are awaiting trial. The majority of the accused are being held in pre-trial detention. In the case that led to a conviction, the prosecution charged a Chilean member of an international criminal organization with drug trafficking and money laundering. The criminal organization included members from Mexico and Colombia. The defendant concealed illicit proceeds from drug sales and invested the money in various businesses. The defendant was sentenced to 10 years in prison; the case is noteworthy because of its complexity and international connections. While the GOC pursued two money laundering cases tied to public corruption in 2008, public corruption does not contribute significantly to money laundering in Chile. There is no indication that financial institutions engage in currency transactions involving international narcotics proceeds from significant amounts of U.S. currency or currency derived from drug sales in the United States. Most money laundering cases have been connected to domestic drug dealing. Detection methods, particularly when not tied to drug trafficking, are still weak. It is difficult to determine if other crimes, such as smuggling of goods, are connected to money laundering or if trade-based money laundering occurs. Given Chile's extensive trading partnerships, long borders, and advanced financial system, it is possible that criminal organizations, in addition to drug smugglers, use Chile as a money laundering location.

Chile has free trade zones in Iquique and Punta Arenas. The Iquique free trade zone is the larger of the two and has over 1,600 companies conducting retail and wholesale operations. It is located in northern Chile and has an extension in Arica, near Chile's border with Peru. Punta Arenas is located in southern Chile and is relatively small compared to Iquique. The physical borders of both free trade zones are porous and largely uncontrolled. All companies in the free trade zones are reporting entities and are required to report any suspicious activity to the UAF. It is nearly impossible to determine the extent of money laundering in the free trade zones. Detection methods are weak and Chilean resources to combat the issue are limited. Iquique is 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. Police investigative efforts suggest possible criminal links between Iquique and the Tri-Border Area involving both terrorist financing of Hezbollah and Hamas and money laundering.

Laws 18.314 and 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 SBIF 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. To date, the GOC has not identified any terrorist assets belonging to individuals or groups named on the list. 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 GAFISUD, which was released in December 2006, the Finance Ministry initiated discussions with the SBIF 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 Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Chile is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and GAFISUD. During the GAFISUD Plenary XIV, Chile's Mutual Evaluation Report was approved. According to the GAFISUD procedures, the report was approved and a process of "intensive monitoring" was established. This was a result of low ratings on compliance with key FATF Recommendations. In the case of Chile, the evaluators rated Chile "partially compliant" on FATF Recommendation 5, which relates to customer due diligence and record keeping, and rated Chile "not compliant" on FATF Special Recommendation IV, which centers on reporting of terrorist-related suspicious transactions. The UAF is a member of the Egmont Group of FIUs 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 occurs, including the exchange of sensitive financial information with Financial Crimes Enforcement Network (FinCEN), the UAF's counterpart in the United States, through the Egmont Secure Web. The U.S. Government (USG) and GOC continue their judicial and investigative cooperation via the Inter-American Convention on Mutual Assistance in Criminal Matters. In 2008, the Carabineros joined the U.S. Federal Bureau of Investigation's (FBI) South American Fingerprint Exchange project that allows Chile and the USG to share fingerprint records of criminals. In addition, the FBI signed Memorandum of Cooperation agreements with the Carabineros, PDI, the Public Ministry, and the Customs agency for increased cooperation on transnational criminal investigations. As a result, there has been a significant increase in the amount of interaction and information exchange between the USG and GOC. 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.

Chile's anti-money laundering efforts continue to mature. The investigation and prosecution of three money laundering cases that are not tied to drug trafficking is an important step for the GOC. At the same time, the GOC can still do more to investigate complex money laundering schemes, such as trade-based money laundering. The UAF and the Public Ministry signed a collaboration agreement in October 2008 that aims to improve communication and cooperation between organizations. Given the current legal structure that separates reporting suspicious activity from investigating and prosecuting suspicious activity, it is essential that these institutions establish procedures to quickly and effectively share information and resources. The GOC should also expand the list of predicate crimes for money laundering to include all serious crimes, such as trafficking in persons and intellectual property rights violations, as well as establish regulatory control over nonbank institutions such as money exchange houses and charities. The GOC should ensure

the passage of the draft law currently pending 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 (AML) and counterterrorist financing (CTF) measures including legislative reform, strengthening enforcement mechanisms, and implementing international cooperation initiatives. 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, corruption, and other financial crimes are major sources of laundered funds. Most money laundering cases currently under investigation involve funds obtained from corruption and bribery. Proceeds of tax evasion, recycled through offshore companies, often return to China disguised as foreign investment and, as such, receive tax benefits. Chinese officials have noted that most acts of corruption in China are closely related to economic activities that accompany illegal money transfers. Observers register increasing concern regarding underground banking and trade-based money laundering.

The People's Bank of China (PBOC), China's central bank, maintains primary authority for AML/CTF coordination. The PBOC shares some AML 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 (MPS) has both an Anti-Money Laundering (AML) Division and an Anti-Terrorism Bureau, which lead anti-money laundering and counterterrorist finance-related law enforcement efforts.

China has criminalized money laundering under three separate articles of the Penal Code. China introduced Article 349 of the Penal Code in December 1990 to criminalize the laundering of proceeds generated from drug-related offenses, and amended Articles 191 and 312 of the Penal Code in June 2006. Article 191 expands the criminalization of money laundering to additional categories of predicate offences: narcotics trafficking, smuggling, organized crime, terrorism, embezzlement and bribery, financial fraud and disrupting the financial management order. The Article 191 amendments to seven predicate offenses, including fraud, bribery, and embezzlement, narcotics trafficking, organized crime, smuggling, and terrorism. Article 312 criminalizes money laundering on the basis of an all-crimes approach, and criminalizes complicity in concealing the proceeds of criminal activity. The Financial Action Task Force (FATF) 2007 mutual evaluation report (MER) identified several deficiencies in China's criminalization of money laundering. These included the failure to fully cover the sole and knowing acquisition and use; criminalize self-laundering; provide for corporate criminal liability for article 312 and 349 offences; and adequately criminalize terrorist financing as a money laundering predicate offense.

Chinese authorities are in the process of addressing several of these deficiencies. China has interpreted its Penal Code to extend the all-crimes offence set out in article 312 to the sole and knowing acquisition and use of proceeds—a judicial interpretations which is poised to become law after undergoing a third reading by the Legal Affairs Committee of the National People's Congress (LAC/NPC). Chinese authorities are amending the Penal Code to provide for corporate criminal liability. A draft Penal Code amendment (Amendment 7) extending corporate criminal liability to article 312 (the all-crimes money laundering offence) passed its first reading at the end of August 2008 but must still undergo second and third readings.

A new anti-money laundering (AML) law, which covers AML/CTF preventative measures for the entire financial system, took effect January 1, 2007. The law extends AML/CTF obligations to the securities and insurance sectors, requires financial institutions to maintain thorough account and transaction records and reports of large and suspicious transactions, and explicitly prohibits financial institutions from opening or maintaining anonymous accounts or accounts in fictitious names. The PBOC remains the primary regulator for AML/CTF purposes for all financial institutions,

including insurance and securities, although other regulators (CBRC, CSRC and CIRC) have a role in formulating the requirements, primarily in relation to systems and controls. To implement the new AML Law, PBOC issued "Rules for Anti-Money Laundering by Financial Institutions" (AML Rules) (effective January 1, 2007); "Administrative Rules for Reporting of Large-Value and Suspicious Transactions by Financial Institutions" (LVT/STR Rules) (effective March 1, 2007); and "Administrative Rules for Financial Institutions on Customer Identification and Record Keeping of Customer Identity and Transaction Information (CDD Rules) (effective August 1, 2007). The AML 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. . Under the new regulatory framework, all financial institutions—securities, insurance, trust companies and futures dealers—must manage their own AML mechanisms and 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, banks must report any cash deposit or withdrawal of over renminbi RMB 200,000 (approximately $27,000) or foreign-currency withdrawal of over $10,000 in one business day to the PBOC's financial intelligence unit (FIU). Banks must report either electronically within five days or in writing within 10 days. They must also report money transfers exceeding RMB 2 million (approximately $274,000) between companies in one day or between an individual and a company greater than RMB 500,000 (approximately $68,500). All financial institutions must submit monthly reports describing 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 revocation of their licenses or forced suspension of business operations.

The new CDD Rules require all financial institutions to identify and verify their customers, including the beneficial owner, (although this requirement may be limited to the natural person who ultimately controls—as opposed to owns—a customer), and extend requirements relating to the identification of legal persons to all financial institutions. Banks must identify and verify customers when carrying out occasional

transactions over 10,000 RMB or 1,000 U.S. $ equivalent, or when providing cash deposit or case withdrawal services over 50,000 RMB or 10,000 U.S. $ equivalent. Similar provisions cover a range of cash and other transactions for the insurance sector. All securities transactions must be funded through a custodian bank account subject to CDD. The CDD Rules call for risk-based CDD and monitoring, and introduce specific requirements for financial institutions in relation to foreign Politically Exposed Persons (PEPs), including the requirement to obtain approval from senior management before opening an account and determine the source of funds.

According to Article 16 of China's AML Law, when establishing business relationships, financial institutions must require prospective customers to show a valid identification card or other identification document issued by a reliable independent source. For example, when opening an account, customers who are residents of China must produce an official or temporary identification card, or in the case of military unit servicemen or armed police, an army or police identification card. The financial institution must verify the customer's identity documents by examining their authenticity and keep records of the information contained therein. Financial institutions may also verify the customer's identity through the State Administration of Industry and Commerce (SAIC) or through public security departments. To remedy deficiencies in regulators' ability to obtain information, the PBOC 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.

Because of the country's size, the Chinese authorities have evolved a decentralized system of AML/CTF supervision, with general oversight being exercised from PBOC head office in Beijing. The supervisory program includes both onsite and offsite monitoring (based on submission by financial institutions of periodic reports). The frequency of onsite inspections for particular institutions is risk-based. The overall adequacy and effectiveness of China's AML supervisory system is improving, but problems remain, particularly with respect to the usefulness of the offsite process. According to the PBOC 2007 China Anti-Money Laundering Report, examiners executed on-site inspections of 4,533 financial institutions to determine compliance with the AML rules. Of the inspected institutions, 350 received financial sanctions for

violating the regulations. The fines totaled RMB 26.52 million (approximately $3.9 million). Of the 350 institutions incurring penalties, 341 were banking financial institutions, 4 were in the securities and futures sector, and the other 5 were in the insurance sector. Of the 350, 347 institutions failed to verify customer identification or report large-value or suspicious transactions, and 3 failed to set up an AML internal control system. Fifty-five percent of the sanctioned institutions were State-owned and joint-stock commercial banks, and 98 percent were Chinese-funded. More recent data is not available.

The AML Law provides for the PBOC's AML authorities, roles and functions, including its FIU. China's FIU is divided into two units within the single overarching authority of the PBOC: China Anti-money Laundering Monitoring & Analysis Center (CAMLMAC) and the Anti-Money Laundering Bureau (AMLB). The heads of CAMLMAC and the AMLB both report to a single deputy governor.

CAMLMAC, established in April 2004, specializes in data collection, processing and analysis, as well as international cooperation. It receives and analyzes STRs and LVTs, and is the central point of contact for foreign FIUs. Established in October 2003, the AMLB organizes and coordinates China's anti-money laundering affairs, and executes administrative investigation, dissemination and policy oversight. Although CAMLMAC and the AMLB work together to conduct follow-up analysis on LVTs and STRs, the AMLB conducts the majority of the additional analysis and dissemination functions.

According to the PBOC, authorities in 2007 discovered 89 cases of money laundering involving RMB 28.8 billion (approximately $4.17 billion). In the first half of 2008, the PBOC sanctioned 12 financial institutions involved in money laundering, with fines totaling RMB 2.25 million (approximately $329,000), The PBOC has also helped police solve 42 money laundering cases involving about RMB 84.4 billion (approximately $12.4 billion).

The Ministry of Public Security (MPS), China's main law enforcement body, follows up on STRs and guides and coordinates public security authorities across China in money laundering investigations. The AML Division of the MPS Economic Crime Investigation Department (ECID) handles the majority of responsibilities related to the seizing, freezing and confiscation of criminal proceeds. The Anti-Terrorism Bureau of the MPS investigates 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 Procurator (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 the SPP and the SPC can issue judicial interpretations. Law enforcement agencies have authority 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 records held by financial institutions. Reportedly, however, law enforcement and prosecutorial authorities focus on pursuing predicate offences, to the exclusion of AML/CTF.

China has implemented a cross-border currency disclosure system using risk-based targeting operated by the General Customs Administration (GCA). All travelers must declare cross-border transportation of cash exceeding RMB 20,000 for local currency (approximately $2,930) or of foreign currency. There is no requirement for bearer negotiable instruments. However, a FATF follow up report states: " China has finished drafting new Administrative Rules on Management of AML Information of Cross-Border Transportation of Cash and Bearer Negotiable Instruments (informal name). The draft is now being circulated among relevant competent authorities for comment. The main issues that are still being debated relate to: (1) reconciling the FATF definition of bearer negotiable instruments with related definitions in existing Chinese legislation; (2) ensuring that the new Rules do not conflict with existing currency-control legislation; and (3) setting the declaration threshold." China prohibits cross-border transportation of RMB through the mail 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 created loopholes for money laundering activity. Authorities do not appear to effectively use captured data for money laundering or terrorist financing investigations.

Only banks have the authority to provide money or value transfer services in China, and may not have agents that offer such services. Article 174 of the Penal Code states that it is a criminal offense to operate an illegal financial institution or provide financial services illegally in China. Although China has had some success at combating illegal underground banking, the country'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 adept at 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. The prevalence of counterfeit identity documents and underground banks, which in some regions reportedly account for over one-third of lending activities, further hamper AML efforts. Authorities have expressed concern that criminal or terrorist groups could exploit underground banking mechanisms to bypass law enforcement.

The extent of the linkages between underground banking and the large expatriate Chinese community remains unknown. Traditionally, money changers, gold shops, and trading companies operate "flying money" or fei-chien networks. The international Chinese underground banking system depends on close associations and family ties 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 participate in the trade of Chinese-manufactured counterfeit goods, in violation of intellectual property rights. Reportedly, 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 address online fraud, the PBOC has tightened regulations governing electronic payments. PBOC rules prohibit consumers from making online purchases of more than RMB 1,000 (approximately $137) in any single transaction or more than RMB 5,000 (approximately $688) in a single day. Enterprises are limited to electronic payments of no more than RMB 50,000 (approximately $6,900) in a single day. In March 2007, Chinese regulators announced additional online restrictions regarding the use of "virtual money" (online credits sold by websites to customers to pay for games and

other web-based services) amidst rumors that criminals were using the credits to launder money.

Terrorist financing is criminalized in Article 120bis of the Penal Code. The MER found that China did not adequately criminalize the sole collection of funds in a terrorist financing context. Through a judicial interpretation of the Penal Code, China has clarified that the terrorist financing offence covers the sole and knowing collection of terrorist funds and has defined "funds" to conform to the definition set forth in the Vienna Convention. These judicial interpretations will likely become law after undergoing a third reading by the Legal Affairs Committee of the National People's Congress (LAC/NPC).

China's primary domestic concerns with terrorist financing focus on the western Xinjiang Uighur Autonomous Region. 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. However, according to the MER, China has not implemented UNSCR 1267 and UNSCR 1373 in a manner that meets the specific requirements of FATF Special Recommendation III.

China is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN 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 $9.1 billion) involved. In late 2004, China joined the Eurasian Group on combating money laundering and financing of terrorism (EAG)—a FATF-style regional body. China became a member of the FATF in June 2007.

The Government of China has 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 take steps to develop a viable AML/CTF regime consistent with international standards. 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. Authorities should assess the application of sanctions for noncompliance with identification, due diligence and record-keeping requirements to ensure that they have a genuinely dissuasive effect. China should ensure that its judicial interpretations that clarify and strengthen its AML/CTF regime become codified in law. In addition to strengthening its counterterrorism finance regime, Chinese law should ensure that it defines the term "terrorist activities" consistently 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 take steps to effectively implement the UNSCRs and strengthen its mechanisms for freezing terrorist assets. Chinese law enforcement authorities should examine domestic and home-grown ties to the international network of Chinese expatriate brokers and traders that often link to underground finance, trade fraud, and trade-based money laundering activities.

Colombia

The Government of Colombia (GOC) is a regional leader in the fight against money laundering. Nevertheless, the laundering of money from Colombia's illicit cocaine and heroin trade continues to penetrate its economy and affect its financial institutions. In

addition to drug-related money laundering, laundered funds are also derived from commercial smuggling for tax and import duty evasion, kidnapping for profit, arms trafficking, and terrorism connected to violent paramilitary groups and guerrilla organizations. Further, money laundering is carried out to a large extent by U.S. Government-designated terrorist organizations. 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, including exchange houses, 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; the trade of counterfeit items in violation of intellectual property rights is an ever increasing method to launder illicit proceeds. Colombian money is also laundered through offshore centers, generally relating to transactions involving drug-related proceeds. Casinos and free trade zones in Colombia present opportunities for criminals to take advantage of inadequate regulation and transparency. Although corruption of government officials remains a problem, its scope has decreased significantly in recent years.

Colombia's economy is robust and diverse. It is fueled by significant export sectors that ship goods such as coal, petroleum products, textiles and apparel, flowers, and coffee to the United States and beyond. While Colombia is not a regional financial center, the banking sector is mature and well regulated. Comprehensive anti-money laundering regulations, as well as international cooperation on anti-money laundering, have allowed the government to refine and improve its ability to combat financial crimes and money laundering. The GOC and U.S. law enforcement agencies closely monitor transactions that could disguise terrorist finance activities. The United States 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 applies to most money laundering activities resulting from Colombia's drug trade.

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 44 techniques for laundering money. Colombia also appears to be a significant destination and transit location for bulk shipment of narcotics-related U.S. currency and European Union euros. Local currency exchangers registered to conduct exchange house transactions, convert narcotics currency to Colombian pesos and then ship U.S. dollars and euros to Europe, 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 narcotics traffickers have also been known to coerce local businessmen into purchasing properties, including real property, in “straw” (or nominee) names, which are then leased to unsuspecting tenants. Colombian authorities have had difficulty in prosecuting such schemes for money laundering, and in confiscating such properties under Colombia’s extincion de dominio nonconviction based forfeiture law regime. Colombian authorities have also noted increased body smuggling (carrying currency on a person) of U.S. and other foreign currencies, an increase in the number of shell companies operating in Colombia, and rising laundering threats in the real estate and cargo transport sectors. 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. In November 2008, several pyramid schemes collapsed, and the largest alleged scheme was shut down by the Colombian government, under charges of illegal enrichment and suspected money laundering.

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 law enacted 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 15 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.

Terrorist financing is an autonomous crime in Colombia. Law 1121 of 2006 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 law allows the UIAF to receive STRs regarding terrorist financing, and freeze terrorists' assets immediately after their designation. In addition, banks are 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 in 2007 from 45 to 65 positions and authorized the creation of new subdivisions for Information Management and Legal Affairs.

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 Financial Superintendent. In 2007, the Financial Superintendent issued a circular that requires entities under its authority to implement a new consolidated risk-based monitoring system (called SARLAFT) that includes risk prevention and control measures based on international standards. In June 2008, the Financial Superintendent issued a circular effective October 2008 further tightening financial reporting requirements for the financial, insurance, and securities sectors with strict deadlines for submitting regular transaction reports.

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 Mexico, and 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, money 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 $5,000. The UIAF requires exchange houses to provide data on all transactions above $200. Between October 2007 and September 2008, 7,980 suspicious transaction reports (STRs) were filed, with 34 percent of STRs deemed by UIAF to merit further investigation by their analysis unit. The Colombian Fiscalia (National Prosecutor's Office) reported 48 convictions for money laundering in 2008.

In 2006, the UIAF inaugurated a new centralized data network connecting 15 governmental entities as well as the private banking 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 2008, the UIAF's database contained over 709 million transaction and activity reports. Between October 2007 and September 2008, the UIAF provided authorities with 604 financial intelligence reports pertaining to 6,231 individuals, 842 businesses, and approximately $3 billion in transactions. During the same period, UIAF responded to 3,067 information requests from national authorities and 499 requests from Egmont Group members, reducing its response time from an average of eight to three days. The UIAF has also increased its staff from 45 to 65 members, which allows for more and better analysis of financial information.

Given concerns about bulk cash smuggling, the GOC requires individual cash transactions above $5,000 or combined monthly transactions above $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 $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.

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. Provisional use has caused some liability issues in Colombia when properties have to be returned for various reasons prior to a final forfeiture.

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 2007, 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 require an evaluation of an asset's worth prior to seizure, and made other significant changes to the manner in which seizures for forfeiture is 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. The GOC aggressively pursues the seizure of assets obtained by drug traffickers through their illicit activities. In 2008, new regulations were also enacted which permit the DNE to make "interlocutory" sales of assets in some instances, if the values of the properties will deteriorate before final forfeiture can be obtained.

For the last five 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 drug cartels' business empires, including the Rodriguez Orejuela brothers, the Grajales family, and Juan Carlos Ramirez Abadia ("Chupeta"). The Cali and Norte Valle drug cartels, as well as their leaders and associated front persons and businesses, have been named by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) as Specially Designated Narcotics Traffickers (SDNTs), pursuant to Executive Order 12978. The Executive Order imposes financial sanctions against designated targets in order to attack the financial empires built by significant 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 2008, the Colombian National Police and Colombian Prosecutor's Office seized over 400 assets, including businesses and properties, tied to major Colombian drug trafficker Juan Carlos Ramirez Abadia, bringing the total value of seized cash and assets to nearly $1 billion. These assets included office buildings, a resort hotel, night clubs, and an amusement park. OFAC added additional businesses and front men tied to Chupeta's financial empire to its SDNT list, including a regulated Colombian money exchange business, CAMBIOS Y CAPITALES S.A. These joint actions to seize assets and apply

financial sanctions have affected the Colombian drug cartels' abilities to use many of their assets derived from their narcotics trafficking activities and have assisted the Colombian government to pursue major cases to seize narcotics-related assets.

In 2008, 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 Titan, which resulted in 113 arrests for money laundering and drug trafficking world wide. Extradition requests to the United States are pending in many of the arrests for Operation Titan and Agents were able to make a direct connection between a traditional Colombian Drug Trafficking and Money Laundering Organization and Middle Eastern money launderers tied to Hezbollah.

The U.S. Department of Homeland Security's Immigration and Customs Enforcement (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.

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 STRs.

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), the GOC's participation in GAFISUD-sponsored events is limited, and the GOC does not have a voice at GAFISUD plenary meetings. According to GOC officials, new legislation is required to authorize the GOC to pay its membership dues; past dues had been paid without legal authorization. In April 2008 the Colombian Congress passed Law 1186 to authorize future payments to GAFISUD. However, at the time of this report, the Constitutional Court had referred the legislation back to the Congress for republication before final constitutional approval—a process expected to take several months. A Mutual Evaluation (ME) by GAFISUD of Colombia was conducted during June 30 to July 9, 2008. Overall, Colombia's AML/CTF regime complies with the FATF 40 Recommendations and the Nine Special Recommendations.

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, and in August 2008, proposed concluding a regional memorandum of understanding with 11 Caribbean Basin countries as well as promoted the incorporation of money laundering and terrorism financing provisions into the Cartagena Declaration of the Regional Counternarcotics, Security and Cooperation Summit. The GOC also issued presidential joint statements with Paraguay and Honduras in 2008 to strengthen cooperation between respective FIUs. In 2008, UIAF organized nine international workshops, which trained more than 220 officials from Ecuador, Peru, Bolivia, and Paraguay. The GOC is a party to the1988 UN Drug

Convention, the UN 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 2008, the Government of Colombia made additional progress in the development of its financial intelligence unit, regulatory framework and interagency cooperation within the government. The further strengthening and broadening of financial reporting requirements reinforce efforts to fight terrorism and financial crime. International cooperation with the U.S. and other countries has led to several high-profile seizures and prosecutions. The transition to a new criminal procedure provides potential for improved use of undercover and other critical investigative techniques, as well as increasing the possibility of plea bargaining and the use of confidential investigations. However, this new system is still being learned. Greater focus and priority toward money laundering investigations, including increased resources, are needed to ensure greater progress. 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, Colombia's Trade Transparency Unit, and 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 the 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 counterterrorist 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. Although Comoros lacks homegrown narcotics, the islands are used to transit drugs, mainly from Madagascar. The presidency of the Union rotates

between the three islands. An ongoing struggle for influence between the Union and the island presidents continued into 2008.

Comoros is not a principal financial center for the region. An anti-money laundering (AML) law addressing many of the primary AML issues of concern was passed by Presidential Decree in 2004. However, the 2004 law does not meet international standards. Also, while legally applicable to all three islands, the AML law was not enforced on Anjouan prior to March 2008. In addition, Comoran authorities lack the capacity to effectively implement and enforce the2004 AML law, as the three islands in the Comoros retain a great deal of autonomy, particularly with respect to their security services, economies, and banking sectors.

In 2007 Comore and Moheli held free elections. However, Colonel Mohamed Bacar refused to hold elections in Anjouan. In June 2007, Anjouan, under the leadership of Colonel Mohamed Bacar, de facto seceded from the Union. Union President Ahmed Abdallah Mohamend Sambi and his cabinet were unable to govern Anjouan. On March 25, 2008, a joint Union of the Comoros and African Union military force removed Colonel Bacar and restored Union legal authority and order.

Both Moheli, pursuant to the International Bank Act of 2001, and Anjouan, pursuant to the Regulation of Banks and Comparable Establishments of 1999, licensed more than 300 offshore banks. Neither island required applicants for banking licenses to appear in person to obtain their licenses. Anjouan required 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) to obtain an offshore license and accepted faxed copies of the required documents. In addition to licensing shell banks, Anjouan sold the right to issue bank licenses. All of the shell banks and other entities were located offshore and had no permanent presence in the Comoros. Neither jurisdiction had the expertise or resources to effectively regulate an offshore banking center. Anjouan delegated most of its authority to operate and regulate the offshore business to private, non-Comoran domiciled parties.

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, licensed insurance companies, internet casinos, and international business companies (IBCs). Moheli claims to have licensed over 1200 IBCs. Moheli law permits bearer shares of

IBCs. Anjouan also allows trusts, and will register aircraft and ships without requiring an inspection of the aircraft or ship in Anjouan.

The Union Central Bank retains a French financial professional as "Financial Controller," and corresponds with French commercial banking authorities. Central Bank Governor Abdoulbastoi sent the United States a comprehensive report on Union Government policies and actions with regard to Anjouan illicit banking activities. The Union Central Bank published informational circulars intended to warn members of the international financial system against dealings with banks "licensed" by Anjouan. The circulars explained that offshore and onshore financial institutions operating within the jurisdiction of the Union of the Comoros must abide by the provisions of legislation No. 80-7 of May 3, 1980, which requires that a financial institution operating in the Union of the Comoros receive prior authorization from the Union Finance Minister upon recommendation from the Comoros Central Bank. Therefore, offshore banks operating in the autonomous islands of the Union of the Comoros without prior authorization from the Union Finance Minister were operating illegally. Because the involved computer servers and illicit "entities" are located outside the Comoros, the GOC lacks the jurisdiction and capacity to act beyond the announcements and warnings regarding the illegal entities.

Citing the law conferring sole authority for granting banking licenses on the Union Central Bank, the Governor asked financial authorities in France, Belgium, and the United States to prohibit all activities within their jurisdictions by Anjouan-registered entities. Union President Sambi also requested international assistance in closing any shell banks or illicit financial entities that operate within the Comoros without legitimate approval. The Governor repeated an earlier request to U.S. and European authorities for help closing all websites associated with Anjouan. The government also issued numerous public announcements warning the public against Anjouan financial entities. A regularly-updated circular lists the 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 Ex-Im Bank, a Tanzanian entity, opened in 2008.

Since Bacar fled to Benin and is no longer in power in Anjouan, Union authorities report that these illicit activities have ceased in Anjouan. During 2008, Comoros closed many of the illegitimate financial institutions, and Moheli and Anjouan no longer issue banking licenses to offshore entities. Current legal licensing authority rests with the Union Finance Minister and Union Central Bank Governor, and the Anjouan and Moheli counterparts are under Union control. However, the already established offshore entities remain outside Union control. The entity to which the Anjouan authorities sold licensing authority may still be issuing licenses in the name of Anjouan. The Comoran government has solicited the law enforcement authorities in the United Kingdom and France to locate and arrest the perpetrators, who were reportedly in Europe.

In early 2007, Union Vice President Idi Nadhoim hosted a World Bank- Bank of France seminar on policies to combat money laundering and terrorist finance. Union Central Bank officials, commercial banks, and operators participated.

As of December 2008, the Union had a draft of a new AML law before the Parliament. Until that law is promulgated, Comoros will use its 2004 federal-level AML law, based on the French model. The 2004 law 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 $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 Comoran francs 5 million (approximately $12,500); and criminalizes the provision of material support to terrorists and terrorist organizations. In addition, there is a suspicious activity filing requirement in the Union's AML law, and reports go to the Central Bank, as stipulated in the law. Comoros does not have an operational financial intelligence unit (FIU).

Foreign remittances from Comorans living abroad in France, Mayotte (claimed by France) and elsewhere remain the most important influx of funds for most Comorans. A 2008 African Development Bank report estimated total annual remittances at $100 million, with two-thirds arriving via informal means. In 2006, Western Union established a presence in Comoros to capture part of this market, but most Comorans continue to prefer to use informal sectors.

As mentioned above, Union authorities have limited ability to implement AML laws in Anjouan and Moheli due to the islands' degree of autonomy. 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 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). However, 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 to bring AML enforcement under Union government jurisdiction. These efforts include the drafting of the new AML legislation currently under consideration by Parliament and the prosecution of corrupt former officials. A grossly inadequate budget, dysfunctional ministries, and a nonfunctioning judiciary limit effectiveness. The lack of capacity severely hinders progress on AML issues, despite apparent high-level political support.

France, the former colonial power, maintains substantial influence and activity in Comoros and, where possible, has bypassed the Union and island governments to prosecute suspected money launderers or shell banks under French law.

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 is a member of the free-trade area of the Common Market for Eastern and Southern Africa (COMESA). It has obtained observer status in the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. The Comoros is moving toward full membership in ESAAMLG, which will commit Comoros to adherence to the FATF's international standards. Comoros has agreed to an on-site visit by ESAAMLG, scheduled to take place in early 2009, and a mutual evaluation visit by the IMF, scheduled for May 2009.

The Government of the Union of the Comoros (GOC) should ensure that the draft anti-money laundering legislation meets international standards, and pass the legislation, which will apply to the three islands that comprise the federal entity. Authorities should ensure that their activities relating to the implementation of the law, when promulgated, take place in all three islands. Authorities should establish an FIU with jurisdiction over the entire country and prohibit bearer shares. Authorities should circulate the list of individuals and entities that are included on the United Nations 1267 Sanctions Committee's consolidated list to Comoran banks. With a total annual operating budget of the Union Finance Ministry less than $100,000, Comoran authorities should ensure that resources target FIU development and regulatory and law enforcement capacity.

V. Statistical Tables

COLOMBIA STATISTICS (1998-2008)									
	2008	**2007**	**2006**	**2005**	**2004**	**2003**	**2002**	**2001**	**20**
Coca									
Net Cultivation[1] (ha)		167,000	157,200	144,000	114,000	113,850	144,450	169,800	136
Aerial Eradication (ha)	133,496	153,133	171,613	138,775	136,555	132,817	122,695	84,251	47,
Manual Eradication (ha)	95,732	66,396	42,111	31,285	10,991				
HCl (Cocaine): Potential[1,2] (mt)		535	550	525	415	445	585	700	530
Opium Poppy									
Net Cultivation[1] (ha)		1,000[3]	2,300	N/A[4]	2,100	4,400	4,900	6,540	5,0
Aerial Eradication (ha)[5]			232	1,624	3,060	2,994	3,371	2,583	9,2
Manual Eradication (ha)	381	375	1929	497	1,497				
Heroin: Potential[1] (mt)		1.9	4.6		3.8	7.8	8.5	11.4	8.7
Seizures									
Coca Base/Paste (mt)	41	60.6	48.1	43.8	28.3	31.1	30.0	26.7	0.0
Cocaine HCl (mt)	182.8	130.7	130.2	179.0	138.6	114.0	94.0	57.3	69.

Combined HCl & Base (mt)	223.8	191.3	178.3	222.8	166.9	145.1	124.0	84.0	69.
Heroin	0.64	0.6	0.5	0.7	0.7	0.5	0.8	0.8	0.6
Arrests/Detentions	54,041	59,652	64,123	82,236	63,791		15,868	15,367	8,6
Labs Destroyed									
Cocaine HCl	301	240	205	137	150	83	129		
Base	3,238	2,875	1,952						
Heroin	4	1	9	6	8	3	3	6	13

[1] A 2008 USG estimate for net cultivation, and consequently production, was not available in time for this report.

[2] Estimates of Colombian potential pure-cocaine production for 1999-2006 were revised based on the results of coca-leaf yield studies completed in 2007 and early 2008.

[3] Only a partial survey was completed in 2007.

[4] Cloud cover in key opium poppy growing areas of Colombia precluded an opium estimate in 2005.

[5] Aerial eradication of poppy was discontinued in April 2006 in order to put all aerial assets against coca cultivation.

Comoros

I. Summary

The Union of the Comoros is composed of three islands in the Indian Ocean (Grande Comore, Anjouan, and Moheli) and claims a fourth, Mayotte, (which France currently governs). Until March 25, 2008, renegade Colonel Mohamed Bacar was the illegitimate leader of Anjouan, having declared himself island president (governor) in June, 2007.

II. Status of Country

The Comoros is a transit country for illegal drugs and possibly a source; particularly in Anjouan during the Bacar regime.

III. Country Actions against Drugs in 2008

On October 26, 2008, Comoran authorities seized 200 kilograms of marijuana at the port of Moroni and arrested a customs official suspected of being implicated in the transshipment of these illicit drugs.

Drug Flow/Transit. There is evidence that drugs transit Comoros, but the quantities are unlikely to be large.

Agreements and Treaties. The 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.

IV. U.S. Policy Initiatives and Programs

Comoran police participate in the International Law Enforcement Academy (ILEA) training program and Comoran army and gendarmes in International Military Education and Training (IMET). Comoran security forces are inadequate to provide border security and prevent drug trafficking. The U.S. will continue to offer Comoran law enforcement training opportunities at ILEA to improve enforcement capacity.

---

[1] These numbers track closely with USG estimates of 200,000 ha for 2007 and 160,000 for 2008. In this section of the INCSR we provide the UN figures because those figures are used by the international donor community, including the United States, to coordinate assistance, including under the Good Performer Initiative that provides assistance to provinces that have dramatically reduced poppy cultivation. For USG estimates, please refer to page 34.