

Cyprus

Cyprus has been divided since the Turkish military intervention of 1974, following an unsuccessful coup d'état directed from Greece. Since then, the Republic of Cyprus (ROC) has controlled the southern two-thirds of the country, while a Turkish Cypriot administration calling itself the "Turkish Republic of Northern Cyprus (TRNC)" controls the northern part. Only Turkey recognizes the "TRNC." The U.S. Government recognizes only the Republic of Cyprus. This report primarily discusses the area controlled by the ROC but also includes a separate section on the area administered by Turkish Cypriots.

Cyprus is a major regional financial center with a robust financial services industry and a significant amount of nonresident businesses. As with all such centers, Cyprus remains vulnerable to international money laundering activities. Fraud along with other financial crimes and narcotics trafficking are the major sources of illicit proceeds laundered in Cyprus.

A number of factors have contributed to the development of Cyprus as a financial center: the island's central location; a preferential tax regime, double tax treaties with 40 countries (including the United States, several European Union (EU) nations, and former Soviet Union nations); a labor force well trained in legal and accounting skills; a sophisticated telecommunications infrastructure; and EU membership.

Four authorities regulate and supervise financial institutions in Cyprus: the Central Bank of Cyprus, responsible for supervising locally incorporated banks and money transfer businesses; the Cooperative Societies Supervision and Development Authority (CSSDA), supervising cooperative credit institutions; the Superintendent for Insurance Control; and the Cyprus Securities and Exchange Commission. Three entities act as regulators for designated nonfinancial businesses and professions (DNFBPs): the Council of the Bar Association supervises attorneys; the Institute of Certified Public Accountants supervises accountants; and the financial intelligence unit (FIU) supervises real estate agents and dealers in precious metals and stones. The supervisory authorities may impose administrative sanctions if the legal entities or persons they supervise fail to meet their obligations as prescribed in Cyprus' anti-money laundering (AML) laws and regulations.

Cyprus currently hosts a total of 43 banks, 17 of which are incorporated locally. The remaining 26 banks are branches of foreign-incorporated banks and conduct their operations mainly with nonresidents. At the end of August 2007, the cumulative assets of all banks were U.S. \$112 billion. Under the EU's "single passport" policy, banks licensed by competent authorities in EU countries could establish branches in Cyprus or provide banking services on a cross-border basis without obtaining a license from the Central Bank of Cyprus. By the end of 2007, nine foreign banks were operating a branch in Cyprus under this arrangement.

Cyprus hosts seven licensed money transfer companies, 65 investment firms, two management firms handling "undertakings for collective investment in transferable securities" (UCITS), 40 licensed insurance companies, 400 licensed real estate agents, 2,311 registered accountants, 1,810 practicing lawyers, and around 165 cooperative credit institutions, controlling about 32 percent of total deposits. Stricter EU requirements on credit institutions have pushed cooperative credit institutions to merge on a large scale over the last three years. Their number shrank from 359 to the current 165 in less than three years, and authorities expect it to drop to just over 100 by the middle of 2008.

In recent years, Cyprus has introduced tax and legislative changes effectively abolishing all legal and substantive distinctions between domestic and offshore companies. All Cypriot companies now pay taxes at a uniform rate of 10 percent, irrespective of the permanent residence of their owners or whether they do business internationally or in Cyprus. Cyprus has lifted the prohibition from doing business domestically and companies formerly classified as offshore are now free to engage in business locally. In March 2007, Cyprus withdrew from the Offshore Group of Banking Supervisors.

The Cypriot government made this move specifically to change the focus and impression of its foreign business from “offshore” to “international.” By removing any distinction between resident and nonresident or on-shore and offshore companies, the same disclosure, reporting, tax and other laws and regulations apply equally to all registered companies. Despite these stricter standards, few of the estimated 54,000 nonresident companies established in Cyprus as of 2006 have taken themselves off the company register and the number of new nonresident companies registering in Cyprus continues to increase as a result of the low tax rate and high service quality.

Cyprus continues to revise its anti-money laundering (AML) framework to meet evolving international standards. The Prevention and Suppression of Money Laundering Activities Law criminalizes all money laundering, establishes a customer identification requirement and obligations for suspicious transaction reporting, provides for the confiscation of proceeds from serious crimes, and codifies the actions that banks, nonbank financial institutions, and obligated nonfinancial businesses must take. The AML law establishes the financial intelligence unit (FIU) and authorizes criminal (but not civil) seizure and forfeiture of assets. The definition of predicate offense is any criminal offense punishable by a prison term exceeding one year. Cypriot AML legislation addresses government corruption, provides for the sharing of assets with other governments, and facilitates the exchange of financial information with other FIUs. Cypriot authorities reportedly have full access to information concerning the beneficial owners of every company registered in Cyprus. This includes companies doing business abroad and companies with foreign beneficial owners and shareholders. Due diligence and reporting requirements extend to auditors, tax advisors, accountants, and, in certain cases, attorneys, real estate agents, and dealers in precious stones and gems. Although the professional organizations for accountants and lawyers publicize strict “know your customer” regulations, the regulatory oversight of these sectors is reportedly nearly nonexistent. Violations result in administrative fines of up to Cyprus Pounds (CP) 3,000 (approximately U.S. \$7,500). The FIU can instruct banks, financial institutions and other obligated entities to delay or prevent execution of customers’ transactions. Casinos and Internet gaming sites are not permitted, although sports betting halls are allowed.

ROC law requires all persons entering or leaving Cyprus to declare all currency, Cypriot or foreign, and gold bullion worth CP 7,300 (approximately U.S. \$18,250) or more. The Central Bank has the authority to revise this amount. On June 15 2007, EU Directive 1889/2005, went into effect. As a result, for currency worth €10,000 (U.S. \$14,620) or more, Cyprus regulates cash transactions for travelers entering its borders from countries outside the EU.

Cyprus is currently in the process of passing legislation entitled “Law for the Prevention and Suppression of Money Laundering Activities,” which was expected to pass without significant changes before the end of 2007. This legislation will consolidate and supersede existing legislation. When enacted, the draft law will encompass all recent FATF and MONEYVAL recommendations, and revises Cyprus’ AML legislation, to harmonize it with the EU’s Third AML Directive. This Directive mandated implementation by December 15, 2007. The new law provides much stricter administrative fines for noncompliance, i.e., from the current €5,130 (U.S. \$7,500) to €200,000 (U.S. \$292,400) and generally raises Cyprus’ AML standards.

The draft law also addresses: enhanced due diligence extending coverage of “politically-exposed persons” (PEPs), cross-border transactions, and transactions with customers not physically present or on behalf of third parties. The law introduces simplified due diligence for certain persons or entities deemed to be low risk as well as requirements for Unit for Combating Money Laundering (MOKAS), the Cypriot financial intelligence unit (FIU), and other supervisory authorities to collect statistical data. MOKAS must provide banks and other obligated entities with feedback in response to any STR submission. The law criminalizes the general collection of funds with the knowledge that terrorists or terrorist groups would use them for any purpose (i.e., not just for violent acts); and terrorism finance is explicitly covered by the new law (although already considered a predicate offense under existing legislation).

A second draft law, expected to pass by early 2008, regulates trust and company service providers (other than accountants and lawyers), bringing them under the supervisory authority of the Central Bank. As soon as these laws go into effect, the supervisory authorities will issue revised directives.

In October 2006, the IMF released a detailed assessment of the “Observance of Standards and Codes for Banking Supervision, Insurance Supervision and Securities Regulation.” The report noted that the Cyprus Securities and Exchange Commission (SEC) was legally unable to cooperate with foreign regulators if the SEC did not have a direct interest and that the SEC had difficulty obtaining information regarding the beneficial owners of Cypriot-registered companies. The report also noted that commitments emerging from EU accession had “placed stress on the skills and resources” of the staff of the Co-operative Societies Supervision and Development Authority (CSSDA) and the Insurance Superintendent. The SEC has drafted amending legislation to resolve these issues, expected to pass by early 2008.

In recent years the Central Bank has introduced regulations aimed at strengthening AML vigilance in the banking sector. Among other requirements, banks must ascertain the identities of the natural persons who are the “principal/ultimate” beneficial owners of all legal entities; adhere to the October 2001 paper of the Basel Committee on Banking Supervision on “Customer Due Diligence for Banks”; and pay special attention to business relationships and transactions involving persons from jurisdictions identified by the Financial Action Task Force (FATF) as deficient in their AML regime, particularly concerning counter-terror financing (CTF).

All banks must report to the Central Bank, on a monthly basis, individual cash deposits exceeding 10,000 Cypriot pounds (approximately U.S. \$22,000 in local currency) or approximately U.S. \$10,000 in foreign currency. Bank employees must report all suspicious transactions to the bank’s compliance officer, who determines whether to forward a report to the Cypriot FIU for investigation. Banks retain reports not forwarded to the FIU, which the Central Bank audits as part of its regular on-site examinations. Banks must file monthly reports with the Central Bank indicating the total number of suspicious transaction reports (STRs) submitted to the compliance officer and the number forwarded by the compliance officer to the FIU. Bank officials may be held personally liable if their institutions launder money. Cypriot law partially protects reporting individuals with respect to their cooperation with law enforcement but does not clearly absolve a reporting institution or its personnel from complete criminal or civil liability. Banks must retain client identification data, transaction records, and business correspondence for five years.

Central Bank money laundering directives place additional obligations on banks, including requirements on customer acceptance policy; and updating customers’ identification data and business profiles. Banks must have computerized risk management systems to verify whether a customer constitutes a PEP; provide full details on any customer sending an electronic transfer in excess of U.S. \$1,000; and have adequate management information systems for on-line monitoring of customers’ accounts and transactions. Cypriot banks typically use electronic risk management systems to target transactions to and from high-risk countries, as well as high-risk customers. Since the expiration of Cyprus’ Exchange Control Law, the Central Bank no longer reviews foreign investment applications for nonEU residents. Since January 1, 2007, Cyprus has begun implementing EU Directive 1781/2006 (“Information on the Payer Accompanying Transfers of Funds”), which requires full disclosure of details for electronic fund transfers in excess of €1,000 (U.S. \$1,462).

The Central Bank also requires compliance officers to file annual reports outlining measures taken to prevent money laundering and to comply with its guidance notes and relevant laws. In addition, the Central Bank has the authority to conduct unannounced inspections of bank compliance records. In July 2002, the U.S. Internal Revenue Service (IRS) officially approved Cyprus’ “know-your-customer” rules, which form the basic part of Cyprus’ AML system. As a result of the approval, banks

in Cyprus that acquire United States securities on behalf of their customers may enter into a “withholding agreement” with the IRS and become qualified intermediaries.

The Prevention and Suppression of Money Laundering Activities Law mandated the establishment of the Unit for Combating Money Laundering (MOKAS), the Cypriot financial intelligence unit (FIU). MOKAS is responsible for receiving and analyzing STRs and for conducting money laundering investigations. A representative of the Attorney General’s Office heads the unit. All banks and nonbank financial institutions, insurance companies, the stock exchange, cooperative banks, lawyers, accountants, and other financial intermediaries must report suspicious transactions to MOKAS. Sustained efforts by the Central Bank and MOKAS to strengthen reporting have resulted in a significant increase in the number of STRs being filed. Between January 1 and November 19, 2007, MOKAS received 160 STRs. In the same interval, MOKAS received 261 information requests from foreign FIUs, other foreign authorities, and INTERPOL. MOKAS cooperates closely with the U.S. in money laundering investigations.

Money laundering is an autonomous crime in Cyprus. MOKAS evaluates evidence generated by its member organizations and other sources to determine if an investigation is necessary. MOKAS has the power to administratively suspend financial transactions for an unspecified period of time. MOKAS also has the power to apply for freezing or restraint orders affecting any kind of property at a preliminary stage of an investigation. MOKAS has issued several warning notices, based on its own analysis, identifying possible trends in criminal financial activity. These notices have resulted in the closure of dormant bank accounts. MOKAS conducts AML training for Cypriot police officers, bankers, accountants, and other financial professionals, and, in conjunction with the Central Bank of Cyprus, for bankers.

During the interval from January 1 through November 19, 2007, MOKAS opened 447 cases and closed 150. Since 2000, there have been 13 prosecutions for money laundering, one of which took place in 2007. Of the 13 prosecutions, eight have resulted in convictions. In 2007, MOKAS issued one confiscation order for a total of approximately \$10.5 million. A number of other cases are pending.

Sections 4 and 8 of the Ratification Law 29 (III) of 2001 criminalize terrorist financing. The implementing legislation amends the AML law to criminalize the collection of funds in the knowledge that these would be used by terrorists or terrorist groups for violent acts. The parliament passed an amendment to the implementing legislation in July 2005 eliminating a loophole that had inadvertently excused Cypriot nationals operating in Cyprus from prosecution for terrorism finance offenses. MOKAS routinely asks banks to check their records for any transactions by any person or organization designated by foreign FIUs or the U.S. Treasury Department as a terrorist or a terrorist organization.

Under a standing instruction, the Central Bank automatically issues a “search and freeze” order for accounts matching the name of any entity or group designated by the UN 1267 Sanctions Committee or the EU Clearinghouse as a terrorist or terrorist organization. If a financial institution finds matching accounts, it will immediately freeze the accounts and inform the Central Bank. As of November 2007, no bank has reported holding a matching account. When FIUs or governments—not the UN or the EU Clearinghouse—designate and circulate the names of suspected terrorists, MOKAS has the authority to block funds and contacts commercial banks directly to investigate. To date, none of these checks have revealed anything suspicious. The lawyers’ and accountants’ associations cooperate closely with MOKAS and the Central Bank. Cyprus cooperates with the United States to investigate terrorist financing. MOKAS reports that no terrorist assets have been found in Cyprus to date and thus there have been no terrorist finance prosecutions or freezing of terrorist assets. In 2006, there was one investigation for terrorist financing involving four persons.

Cyprus believes that its existing legal structure is adequate to address money laundering through alternative remittance systems such as hawala. Cypriot authorities maintain that there is no evidence

that alternative remittance systems such as hawala operate in Cyprus. Cyprus licenses charitable organizations, which must submit copies of their organizing documents and annual statements of account to the government. The majority of charities registered in Cyprus are reportedly domestic organizations.

Cyprus is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Cyprus has signed, but not ratified, the UN Convention Against Corruption. Cyprus is a member of MONEYVAL the FATF-style regional body for Council of Europe member states. MOKAS is a member of the Egmont Group and has signed memoranda of understanding (MOUs) with 17 FIUs, although Cypriot law allows MOKAS to share information with other FIUs without benefit of an MOU. A mutual legal assistance treaty between Cyprus and the United States entered into force September 18, 2002.

Cyprus has put in place a comprehensive AML/CTF regime, which it continues to upgrade. Cyprus should ensure not only the passage, but also the full implementation, of the two laws that will tighten the current regime requirements. Cyprus should ensure that it is able to implement the law criminalizing the collection of funds with the knowledge that they will be used by terrorists or terrorist groups for any purpose, not only to commit terrorist or violent acts. Cyprus should enact provisions that allow for civil forfeiture of assets in the future.

Area Administered by Turkish Cypriots. The Turkish Cypriot community continues to lack the legal and institutional framework necessary to provide effective protection against the risks of money laundering. There are currently 24 domestic banks in the area administered by Turkish Cypriots. Internet banking is available. The offshore sector consists of 14 banks and approximately 50 companies. The offshore banks may not conduct business with residents of the area administered by Turkish Cypriots and may not deal in cash. The “Central Bank” audits the offshore entities, which must submit an annual report on their activities. However, the “Central Bank” has no regulatory authority over the offshore banks and can neither grant nor revoke licenses. Instead, the “Ministry of Finance” performs this function. A new law restricts the granting of new bank licenses to only those banks with licenses in an OECD country or a country with “friendly relations” with the “TRNC.” A new law to more closely regulate offshore banks is pending in “parliament.”

It is thought that the 18 essentially unregulated and primarily Turkish-mainland owned casinos and the 14 offshore banks are the primary vehicles through which money laundering occurs. Casino licenses are fairly easy to obtain, and background checks on applicants are minimal. A significant portion of the funds generated by these casinos reportedly change hands in Turkey without ever entering the Turkish Cypriot banking system, and there are few safeguards to prevent the large-scale transfer of cash to Turkey. Another area of concern is the approximately five hundred “finance institutions” operating in the area that extend credit and give loans. Although they must register with the “Office of the Registrar of Companies,” they remain unregulated. Some of these companies are owned by banks and others by auto dealers. Recent years have seen a large increase in the number of sport betting halls, which are licensed by the “Office of the Prime Minister.” There are currently five companies operating in this sector, with a total of 30 outlets. Four of the companies also accept bets over the Internet. Turkish Cypriot authorities deported one prominent Turkish organized crime figure, Yasar Oz, following a December 19, 2006 shootout at the Grand Ruby Casino that left two dead. As a result of this incident, the Turkish Cypriot authorities arrested seven individuals, closed the Grand Ruby and Denizkizi Casinos and deported much of their staff. Nevertheless, several other casinos are still believed to have significant links to organized crime groups in Turkey.

The fact that the “TRNC” is recognized only by Turkey limits the ability of Turkish Cypriot authorities to receive training or funding from international organizations with experience in combating money laundering. The Turkish Cypriot community is not part of any regional FATF-style

organization and thus is not subject to any peer evaluations. In 2007, FATF conducted an informal review and found numerous shortcomings in AML laws and regulations as well as insufficient resources devoted to the effort. Turkish Cypriot officials objected to the conclusions.

The offshore banking sector remains a concern. In August 2004, the U.S. Department of the Treasury's FinCEN, pursuant to Section 311 of the USA PATRIOT Act, found First Merchant Bank to be of primary money laundering concern based on a number of factors. These factors, included that it is licensed as an offshore bank in a jurisdiction with inadequate AML controls, particularly those applicable to its offshore sector; and that it is involved in the marketing and sale of fraudulent financial products and services. Other factors point to its use as a conduit for the laundering of fraudulently obtained funds; and its apparent use to launder criminal proceeds by the individuals who own, control, and operate First Merchant Bank—individuals with links to organized crime. In December 2006, the Turkish Cypriot administration ordered First Merchant Bank to cease its operations due to violations of the Turkish Cypriot "Offshore Banking Law." The bank is now only permitted to perform activities associated with closing the Bank such as the payment and collection of outstanding debts.

Turkish Cypriot authorities have begun taking limited steps to address the risk of financial crime, including enacting an anti-money laundering law (AMLL) for the area. The law aims to reduce the number of cash transactions in the area administered by Turkish Cypriots, as well as improve the tracking of any transactions above U.S. \$10,000. Under the AMLL, banks must report to the "Central Bank" any electronic transfers of funds in excess of U.S. \$100,000. Such reports must include information identifying the person transferring the money, the source of the money, and its destination. Banks, nonbank financial institutions, and foreign exchange dealers must report all currency transactions over U.S. \$20,000 and suspicious transactions in any amount. Banks must follow a know-your-customer policy and require customer identification. Banks must also submit suspicious transaction reports (STRs) to a five-member "Anti-Money Laundering Committee (AMLC)" which decides whether to refer suspicious cases to the "police" and the "attorney general's office" for further investigation. The five-member committee is composed of representatives of the "police," "customs," the "Central Bank," and the "Ministry of Finance." However, the AMLL has never been fully implemented or enforced.

In 2005, the "AMLC," which had been largely dormant for several years, began meeting on a regular basis and encouraging banks to meet their obligations to file STRs. The committee has reportedly referred several cases of possible money laundering to law enforcement for further investigation, but no cases have been brought to court and no individuals have been charged. There have been no successful prosecutions of individuals for money laundering, although one foreign bank owner suspected of having ties to organized crime was successfully extradited. There are significant concerns that law enforcement and judicial authorities lack the technical skills needed to investigate and prosecute financial crimes. The "AMLC" also complains that since foreign jurisdictions will not cooperate with them by providing evidence or appearing to testify, they have difficulty presenting cases to their court system.

Although the AMLL prohibits individuals entering or leaving the area administered by Turkish Cypriots from transporting more than U.S. \$10,000 in currency without prior "Central Bank" authorization, "Central Bank" officials note that this law is difficult to enforce. This is particularly true given the large volume of travelers to and from Turkey, especially since Turkish Cypriot authorities relaxed restrictions that limited travel across the UN-patrolled buffer zone. There is also a relatively large British population in the area administered by Turkish Cypriots and a significant number of British tourists. As a result, an informal currency exchange market has developed.

The "Ministries of Finance, Economy and Tourism" are drafting several new AML laws that they claim will, among other things, establish an FIU and provide for better regulation of casinos, currency

exchange houses, and both onshore and offshore banks. Turkish Cypriot authorities have committed to ensuring that the new legislation meets international standards. However, it is unclear if or when the new legislation will be adopted, and if it is adopted, whether it will ever be fully implemented and enforced. Work on the new bills has been ongoing for more than three years. Turkish Cypriot officials have promised FATF that the laws will pass in 2007, after which the European Commission plans to help with their implementation through selected training and funding.

The Turkish Cypriot AMLL provides better banking regulations than were previously in force, but as an AML tool it is far from adequate, and without ongoing enforcement, cannot meet its objectives. A major weakness continues to be the many casinos, where a lack of resources and expertise leave that area essentially unregulated and therefore especially vulnerable to money laundering abuse. The largely unregulated finance institutions, currency exchange houses, and offshore banking sector are also of concern. The Turkish Cypriot authorities should move quickly to enact a new anti-money laundering law, establish a strong, functioning “financial intelligence unit”, and adopt and implement a strong regulatory environment for all obliged institutions, in particular casinos, money exchange houses, and entities in the offshore sector. Turkish Cypriot authorities should take steps to enhance the expertise of members of the enforcement, regulatory, and financial communities with an objective of better regulatory guidance, the more efficient STR reporting, better analysis of reports, and enhanced use of legal tools available for prosecutions. Passage of new laws and willingness to cooperate with foreign experts for implementation will be the early tests of a change in approach to these issues.

Czech Republic

The Czech Republic is one of the most stable and prosperous of the post-Communist states of Central and Eastern Europe. However, the Czech Republic’s central location in Europe and its relatively new status as a functional market economy have left it vulnerable to money laundering. While various forms of organized crime (narcotics trafficking, trafficking in persons, fraud, counterfeit goods, embezzlement and smuggling) remain the primary source of laundered assets in the country, Czech officials and media outlets have voiced increasing concern about the ability of extremist groups and terrorists to launder or remit money within the country. Domestic and foreign organized crime groups target Czech financial institutions for laundering activity, most commonly by means of financial transfers through the Czech Republic. Banks, currency exchanges, casinos and other gaming establishments, investment companies, and real estate agencies have all been used to launder criminal proceeds. Currency exchanges in the capital and border regions are also considered to be a major problem.

The growth of the Czech Republic economy between 2000 and 2007 was supported by exports to the European Union (EU), primarily to Germany. However, despite the progressive development of modern payments techniques, the economy is still heavily cashed-based. The Czech Republic decided to adopt the single European currency (euro) in connection with its accession to the EU in 2004, and in July 2007 the Organizational Committee of National Coordination Group published “The National Changeover Plan for the Czech Republic,” which covers the technical, legislative and organizational preparation for the future introduction of the euro in Czech Republic.

Major sources of criminal proceeds include criminal offenses against property, insurance fraud, and credit fraud. Connections between organized crime and money laundering have been observed mainly in relation to activities of foreign groups, in particular from the former Soviet republics, the Balkan region, and Asia. The Czech Republic is also vulnerable to other illicit financial activities conducted through credit and loan services, money remittances (particularly in connection with the Asian community), and illegal foreign exchange business.

The Government of the Czech Republic (GOCR) first criminalized money laundering in September 1995 through additions to its Criminal Code. Although the Criminal Code does not explicitly mention

money laundering, its provisions apply to financial transactions involving the proceeds of all serious crimes. A July 2002 amendment to the Criminal Code introduces a new independent offense called “Legalization of Proceeds from Crime.” This offense has a wider scope than previous provisions and enables prosecution for laundering one’s own illegal proceeds (as opposed to those of other parties). The 2002 amendment also stipulates punishments of five to eight years imprisonment for the legalization of proceeds from all serious criminal activity and calls for the forfeiture of assets associated with money laundering. Despite some improvements, the criminalization of money laundering under Section 252a (“Legalization of Proceeds from Criminal Activity”) of the Criminal Code still does not contain a broad definition and coverage of money laundering. To date, Section 252a has mostly been applied to criminal offenses that have more to do with stolen goods than with the laundering proceeds.

The Czech anti-money laundering legislation (Act No. 61/1996, Measures Against Legalization of Proceeds from Criminal Activity) became effective in July 1996. The Anti-Money Laundering (AML) Act, which provides for the general preventive framework, was adopted in 1996 and covered only the banking sector. It has been amended several times and to comply with EU requirements. The law now requires a wide range of financial institutions, as well as attorneys, casinos, realtors, notaries, accountants, tax auditors, and entrepreneurs engaging in financial transactions, to report all suspicious transactions to the Ministry of Finance’s financial intelligence unit (FIU), known as the Financial Analytical Unit (FAU). Suspicious transactions exceeding 15,000 euros (approximately U.S. \$22,140) must be reported, and those exceeding 1,000 euros (approximately U.S. \$1,476) must be identified internally.

The GOCR recently approved a new draft law on “Measures against Legalization of Proceeds from Criminal Activity and Terrorism Financing.” This proposal implements the EU’s Third Money Laundering Directive. Legislative approval by December 15, 2007, as requested by the EU, is expected. In connection with this effort, the Czech National Bank is preparing an amendment to the foreign currency law that would introduce new regulations and licensing requirements for currency exchanges.

The Law on International Sanctions that came into force in April 2006 also represents progress by the GOCR. Under this law, the Ministry of Finance has the authority to fine institutions for failure to report accounts or other assets belonging to individuals, organizations, or countries, on which international sanctions have been imposed, or those not fulfilling other obligations set by international regulations. Earlier laws restricting financial cooperation with the Taliban (2000) and Iraq (2005) were replaced by the Law on International Sanctions.

The Czech Republic still has more than 2.6 million anonymous deposit passbooks containing 3.9 billion crowns (approximately U.S. \$200 million). Due to ongoing criticism, the Czech Republic introduced legislation in 2000 prohibiting new anonymous passbook accounts. In 2002 the Act on Banks was amended to abolish all existing bearer passbooks by December 31, 2002. In principle, bearer passbooks will be completely phased out by 2012. While account holders can still withdraw money from the accounts for another few years, the accounts do not earn interest and cannot accept deposits. In 2007, approximately 350 million crowns (approximately \$18 million) were withdrawn from these accounts. Although in general the customer identification procedures are mostly in place, full customer due diligence (CDD) requirements should be introduced in the AML Act with appropriate guidance.

Czech authorities require that financial institutions maintain transaction records for a period of ten years. Reporting requirements also apply to persons or entities seeking to enter the Czech Republic. Under the provisions of the AML Act, anyone entering or leaving the Czech Republic with more than 10,000 euros (approximately U.S. \$14,750) in cash, traveler’s checks, or other monetary instruments must make a declaration to customs officials, who are required to forward the information to the FAU.

Similar reporting requirements apply to anyone seeking to mail the same amount in cash to or from the country. In practice, the effectiveness of these procedures is difficult to assess. With the accession of the Czech Republic to the EU, nearly all customs stations on the borders were closed. Although the customs station at the Prague Airport remains operational, detecting the smuggling or transport of large sums of currency by highway is difficult.

The FAU was established in July 1996 as an administrative FIU under the umbrella of the Ministry of Finance. It has overall supervisory competence to ensure the implementation of the AML Act by all obliged entities. Since 2000 financial institutions have been required to report all suspicious transactions to the FAU. The FAU is authorized to share all information with the Czech Intelligence Service (BIS) and Czech National Security Bureau (NBU) in addition to its ongoing cooperation with the Czech Police, Customs, and counterparts abroad. The GOCR expects that this type of information sharing will improve the timeliness and nature of exchanges between the different agencies within the Czech government.

The FAU is charged with reviewing suspicious transaction reports (STRs) filed by police agencies, financial, and other institutions. It is also charged with uncovering cases of tax evasion, which is a widespread problem in the Czech Republic. The FAU has neither the mandate nor the capacity to initiate or conduct criminal investigations. Investigative responsibilities remain with the Czech National Police Unit for Combating Corruption and Financial Crimes (UOKFK) or other Czech National Police bodies. The FAU's work covers only a relatively small segment of total financial activity within the Czech Republic. Since April 2006, the FAU has had the power to fine financial institutions that fail to report accounts or other assets belonging to individuals, organizations, or countries on which international sanctions have been imposed.

The UOKFK has primary responsibility for all financial crime and corruption cases. Following the dissolution of the specialized Financial Police on January 1, 2007, the unit became the main law enforcement counterpart to the FAU and is responsible for investigations of terrorist financing cases. Following the abolition of the Financial Police, the UOKFK took over all of its ongoing cases, but the pace of investigations has slowed.

The number of STRs transmitted to the FAU has been growing. There were 3,404 suspicious transactions reported in 2005 and 3,480 in 2006. From January through October 2007, there were 1,729 reports of suspicious transactions. This upward trend is interpreted as evidence of the active participation of concerned entities in the anti-money laundering regime. Conversely, the number of inquiries evaluated and forwarded to law enforcement bodies have decreased compared to 2005. In 2005, the FAU forwarded 208 reports to the police and only 137 in 2006. From January through October 2007, the number of reports forwarded to the police was 82; in 25 cases, the payments were temporarily frozen. The abolition of the Financial Police and the transfer of its cases to the Unit Combating Corruption and Financial Crimes caused temporary difficulties in communication between the FAU and the Police. It is not clear whether every case transferred to law enforcement was investigated. Cooperation with foreign counterparts remains good. In 2005, the FAU received 130 assistance requests from abroad and sent 69 requests abroad. In 2006, it received 128 and sent 77. During the first nine months of 2007, the FAU received 102 requests and sent out 49 requests.

From January to June 2007, the Police investigated eight individuals, but did not seize any related funds. This is a significant decrease from 2006, when the police investigated 11 offenders and seized 373 million crowns (approximately \$20 million). The decrease can be partially explained by the abolition of the specialized Financial Police.

The Czech Republic saw its first convictions of individuals attempting to legalize proceeds from crime only in 2004. In 2005, there were 23 alleged offenders prosecuted and three were convicted. In 2006, there were 33 were prosecuted, and five convicted. In the first half of 2007, only six people were prosecuted and two convicted. The sentences were low and included suspended sentences or fines. An

ongoing issue in criminal prosecutions is that law enforcement agencies must prove that the assets in question were derived from criminal activity. The accused is not obligated to prove that the property or assets were acquired legitimately.

While the institutional capacity to detect, investigate, and prosecute money laundering and financial offenses has increased in recent years, both the FAU and the Police face staffing challenges. The Financial Action Task Force (FATF) and the Council of Europe's FATF-style regional body (MONEYVAL) have both emphasized the need for the Czech Republic to increase the FAU's staff. Given the scope of its responsibilities, the FAU remains a relatively small organization. The Police face even bigger challenges due to recent changes in police retirement rules and the perceived lack of political support for independent police work. Many senior and experienced police officers are reportedly leaving or are considering early retirement. These departures will affect not only the UOKFK, but the Organized Crime Unit and other critical police organizations as well. The dissolution of the Financial Police, which was created in 2004 in response to EU recommendations and had a good track record of investigating and prosecuting money laundering and terrorist finance cases, has also had a negative impact on police work on financial crimes.

Czech laws facilitate the seizure and forfeiture of bank accounts. A financial institution that reports a suspicious transaction has the authority to freeze the suspect account for up to 24 hours. However, for investigative purposes, this time limit can be extended to 72 hours to give the FAU sufficient time to investigate whether there is evidence of criminal activity. Currently, the FAU is authorized to freeze accounts for 72 hours. If sufficient evidence of criminal activity exists, the case is forwarded to UOKFK, which has another three days to gather the necessary evidence. If the UOKFK is able to gather enough evidence to start prosecution procedures, then the account can stay frozen for the duration of the investigation and prosecution. If, within the 72-hour time limit, the UOKFK fails to gather sufficient evidence to convince a judge to begin prosecution, the frozen funds must be released. These time limits do not apply to accounts owned by suspected terrorists and terrorist organizations, or by other individuals and organizations covered under the Law on International Sanctions.

Although Czech law authorizes officials to use asset forfeiture, it is still not widely used. It was introduced into the criminal system in 2002 and allows judges, prosecutors, or the police (with the prosecutor's consent) to freeze an account or assets if evidence indicates that the contents were used or will be used to commit a crime, or if the contents are proceeds of criminal activity. In urgent cases, the police can freeze the account without the previous consent of the prosecutor, but within 48 hours must inform the prosecutor, who then confirms the freeze or releases the funds. An amendment to the 2004 Law on the Administration of Asset Forfeiture in Criminal Procedure implemented provisions and responsibilities overseeing the administration and storage of seized property and appoints the police as administrators of seized assets.

A 2006 amendment to the Czech Criminal Procedure Code and Penal Code brought several positive changes to the asset forfeiture and seizure law. The law, as amended, now allows for the freezing and confiscation of the value of any asset (including immovable assets) and is not limited to property. These provisions allow the police and prosecutors to seize assets gained in illicit activity previously shielded by family members. The law allows for the seizure of substitute asset values as well as asset values not belonging to the criminal.

The National Drug Headquarters (NDH) cooperates with the UOKFK on drug-related cases. However, as a result of the abolition of the Financial Police the NDH conducts its basic financial investigations alone and, if needed, contacts the UOKFK. In the first ten months of 2007, the NDH confiscated 1.9 million crowns (approximately U.S. \$108,000), 44 thousand euros (approximately U.S. \$65,000), and other assets valued at 1.8 million crowns (approximately U.S. \$103,000).

In November 2004, the Czech Government amended the Criminal Code and enacted new definitions for terrorist attacks and terrorist financing. A penalty of up to 15 years' imprisonment can be imposed

on those who support terrorists financially, materially, or by other means. In addition to reporting all suspicious transactions possibly linked to money laundering, concerned institutions are now required to report all transactions suspected of being tied to terrorist financing. An amendment to the anti-money laundering law in 2000 requires financial institutions to freeze assets that belong to suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committees consolidated list.

The Czech Republic ratified the UN International Convention for the Suppression of the Financing of Terrorism in October 2005. Subsequently, the GOOCR adopted the National Action Plan for the Fight against Terrorism for 2005-2007. This document covers topics such as police work and cooperation, protection of security interests, enhancement of security standards, and customs issues. The fight against terrorist financing is one of the major priorities contained in the plan.

Although the terrorist finance threat in the Czech Republic is considered to be modest, some law enforcement officials believe that the presence of third-country remuneration networks operating in the country (“hawala” shops) could translate into a greater possibility of financing terrorist activities. The Czech Republic has specific laws criminalizing terrorist financing and legislation permitting rapid implementation of UN and EU financial sanctions, including action against accounts held by suspected terrorists or terrorist organizations. A governmental body called the Clearinghouse was established in 2002 to streamline the collection of information from institutions to enhance cooperation and response to a terrorist threat. The Clearinghouse meets only in cases of necessity. It has not met thus far in 2007. The FAU is currently distributing lists of designated terrorists to relevant financial and governmental bodies. Czech authorities have been cooperative in the global effort to identify suspect terrorist accounts, and adoption of the Law International Sanctions has made their work easier. Several cases have been detected, and payments to suspected organizations were not permitted. No sanctions have been imposed.

The Czech Republic has signed memoranda of understanding on information exchange with 23 countries, and, most recently, signed a new agreement with Paraguay. The Czech Republic formalized an agreement with Europol in 2002. The FAU has been a member of the Egmont Group since 1997 and is authorized to cooperate and share information with all of its international counterparts, including those that are not part of the Egmont Group. The Czech Republic participates in MONEYVAL. The most recent mutual evaluation of Czech Republic was conducted by the MONEYVAL in 2006. The mutual evaluation report (MER) was adopted by the MONEYVAL at its 24th plenary meeting in December 2007.

The Czech Republic is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The Czech Republic is also a party to the World Customs Organization’s Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offenses as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

The United States and the Czech Republic have a Mutual Legal Assistance Treaty (MLAT), which entered into force on May 7, 2000, as well as an extradition treaty that has been in effect since 1925. In May 2006, the United States and the Czech Republic signed a supplemental extradition treaty and a supplemental MLAT to implement the U.S.-EU Agreements on these subjects; however, these instruments have not yet been ratified.

The Government of the Czech Republic has made progress in its efforts to strengthen its money laundering regime. The GOOCR cooperates to a large extent with foreign counterparts in the field of anti-money laundering and counter-terrorist financing. However, the incomplete Czech legal framework on seizure and confiscation is a major limitation to its international cooperation, and its staffing problems could be an obstacle to timely and effective collaboration. Czech authorities are using a risk-based approach when determining priorities and imposing obligations on obliged entities.

However, there is a tendency to rely on assumptions rather than on assessments, and as a result there is a lack of unanimity on sectors exposed to and used for money laundering purposes. The Czech Republic should approve already-drafted amendments to its existing money laundering legislation by to implement the European Union's Third Money Laundering Directive. The GOCR should also ratify the UN Convention against Transnational Organized Crime and UN Convention against Corruption.

Dominica

The Commonwealth of Dominica initially sought to attract offshore dollars by offering a wide range of confidential financial services, low fees, and minimal government oversight. A rapid expansion of Dominica's offshore sector without proper supervision made it attractive to international criminals and vulnerable to official corruption. In response to international criticism, Dominica enacted legislation to address many of the deficiencies in its anti-money laundering and counter-terrorist financing regime.

Dominica's financial sector includes one offshore bank, approximately 12,787 international business companies (IBCs) (an increase from 11,452 in 2006), 20 insurance agencies, six money remitters, one building and loan society, and three operational Internet gaming companies. However, reports indicate more Internet gaming sites may exist. There are no free trade zones in Dominica.

Under Dominica's Economic Citizenship Program, individuals can purchase citizenship and obtain passports for approximately U.S. \$75,000 for an individual and U.S. \$100,000 for a family of up to four persons. There is no residency requirement and passport holders may travel to Commonwealth countries without a visa. An application for economic citizenship must be made through a government approved local agent and requires a fee for due diligence or background check purposes. An in-person interview is also required. Dominica's Economic Citizenship Program does not appear to be adequately regulated. In the past, subjects of United States criminal investigations have been identified as exploiting this program. In 2007, 15 individuals acquired economic citizenship.

Under common banking legislation enacted by its eight member jurisdictions, the Eastern Caribbean Central Bank (ECCB) acts as the primary supervisor and regulator of onshore banks in Dominica. The ECCB, in conjunction with the Financial Services Unit (FSU), supervises Dominica's offshore bank. The ECCB assesses applications for offshore banking licenses, conducts due diligence checks on applicants, and provides a recommendation to the Minister of Finance. Offshore banks are required to have a physical presence and are forbidden from opening client accounts before verifying the beneficial owner of the bearer shares and/or companies. The Minister of Finance is required to seek advice from the ECCB before exercising his powers with respect to licensing and enforcement.

The ECCB also conducts on-site inspections for anti-money laundering compliance of onshore and offshore banks in Dominica. Inspections of offshore banks are conducted by the ECCB in collaboration with the FSU. The Offshore Banking (Amendment) Act No. 16 of 2000 prohibits the opening of anonymous accounts, prohibits IBCs from direct or indirect ownership of an offshore bank, and requires disclosure of beneficial owners and prior authorization to changes in beneficial ownership of banks. All offshore banks are required to have available for review on-site books and records of transactions. Per the Banking Act, which went into effect in Dominica in 2006, the ECCB is able to share information directly with foreign regulators through a memorandum of understanding (MOU).

The International Business Companies Act (IBCA) enacted in 1996 and amended in 2000, requires that bearer shares be kept with an approved fiduciary, who is required to maintain a register with the names and addresses of beneficial owners. Additional amendments to the Act in September 2001 require previously issued bearer shares to be registered. Dominica permits "shelf companies" or ready made offshore companies. Shelf companies have already been incorporated with a nominee director and nominee shareholder, and are for sale for immediate use. IBCs are not required to have a physical

presence and are restricted from conducting local business activities. Internet gaming entities must register as IBCs.

The IBCA empowers the FSU to perform regulatory, investigatory, and enforcement functions over IBCs. The FSU also supervises, regulates, and inspects Dominica's registered agents and conducts on-site visits to ensure that the companies are operating in compliance with requirements imposed by law. The FSU staff consists of a manager, two professional staff (supervisors/examiners), and one administrative assistant.

Amendments to the Money Laundering Prevention Act (MLPA) No. 20 of December 2000 adopted in 2001 criminalize the laundering of proceeds from any indictable offense. The law applies to narcotics-related money laundering and all hybrid or indictable offenses as predicate offenses for money laundering, whether committed in Dominica or elsewhere. The MLPA overrides secrecy provisions in other legislation and requires financial institutions to keep records of transactions for at least seven years. The MLPA also requires persons to report cross-border movements of currency that exceed U.S. \$10,000 to the financial intelligence unit (FIU). The MLPA requires a wide range of financial institutions and businesses, including any offshore institutions, to report suspicious transactions simultaneously to the MLSA and the FIU. Additionally, financial institutions are required to report any transaction over U.S. \$5,000.

The MLPA establishes the Money Laundering Supervisory Authority (MLSA) and authorizes it to inspect and supervise nonbank financial institutions and regulated businesses for compliance with anti-money laundering legislation. The MLSA is also responsible for developing anti-money laundering policies, issuing guidance notes, and conducting training. The MLSA consists of five members: a former bank manager, the FSU manager, the Deputy Commissioner of Police, a senior State Attorney, and the Deputy Comptroller of Customs.

The 2001 Money Laundering Prevention Regulations apply to all onshore and offshore financial institutions including banks, trusts, insurance companies, money transmitters, regulated businesses, and securities companies. The regulations specify know-your-customer requirements, record keeping, and suspicious transaction reporting procedures, and require compliance officers and training programs for financial institutions. The regulations require that the true identity of the beneficial interests in accounts be established, and mandate the verification of the nature of the business and the source of the funds of the account holders and beneficiaries. Reporting entities are protected by law with respect to their cooperation with law enforcement entities. Anti-Money Laundering Guidance Notes, also issued in 2001, provide further instructions for complying with the MLPA and provide examples of suspicious transactions to be reported to the MLSA and the FIU.

The FIU, established under the MLPA, became operational in August 2001. The FIU's staff consists of a certified financial investigator and a director. The FIU analyzes suspicious transaction reports (STRs) and cross-border currency transactions reports, forwards appropriate information to the Director of Public Prosecutions, and works with foreign counterparts on financial crimes cases. The FIU has access to records of financial institutions and other government agencies with the exception of the Inland Revenue Division. In 2007, the FIU received 17 STRs. The FIU is closely examining the relationship between narcotics proceeds and money laundering in Dominican financial institutions. However, Dominica believes most of the money laundering cases under investigation involves external proceeds from fraudulent investment schemes.

The MLPA provides for the freezing of assets for seven days by the FIU, after which time a suspect must be charged with money laundering or the assets released. All assets that can be linked to any individual or legitimate business under investigation can be seized or forfeited, providing that the amount seized or forfeited does not exceed the total benefit gained by the subject from the crime committed. The court can order the confiscation of frozen assets. Pursuant to the MLPA, tangible confiscated assets such as vehicles or boats are forfeited to the state. Intangible assets such as cash or

bank accounts are split between the forfeiture fund and the government-consolidated fund by 80 and 20 percent, respectively. In 2006, \$55,481 was frozen but subsequently the matter was discontinued by the Director of Public Prosecutions and the funds returned. No statistics are currently available on the amount of assets frozen or seized in 2007.

There are no known convictions on money laundering charges in Dominica and there were no arrests or prosecutions for money laundering or terrorist financing in 2007. In 2006, a French national was arrested for attempting to obtain a line of credit through fraudulent wire transfers; he had been under investigation since 2004 for misappropriation of funds from Guadeloupe nationals. Since 2003, Dominica has collaborated closely with U.S. and foreign law enforcement agencies in a widespread money laundering case involving a European fraudulent investment scheme proceeds in one of the now closed offshore banks in Dominica.

In 2003, Dominica enacted the Suppression of Financing of Terrorism Act (No. 3 of 2003), which provides authority to identify, freeze, and seize terrorist assets, and to revoke the registration of charities providing resources to terrorists. The MLSA and the Office of the Attorney General supervise and examine financial institutions for compliance with anti-money laundering and counter-terrorist financing laws and regulations. The Government of the Commonwealth of Dominica (GOCD) circulates pertinent terrorist lists to financial institutions. To date, no accounts associated with terrorists or terrorist entities have been found in Dominica. There were no terrorist-related assets frozen, forfeited, or seized in 2007. The GOCD has not taken any specific initiatives focused on alternative remittance systems.

In 2000, a Mutual Legal Assistance Treaty between Dominica and the United States entered into force. However, in 2007, Dominica has not been cooperative in meeting mutual legal assistance requests. The GOCD also has a Tax Information Exchange Agreement with the United States but Dominica has not responded to more than two dozen requests from the USG for information regarding a potential money laundering case involving both countries. The MLPA authorizes the FIU to exchange information with foreign counterparts. Cash smuggling reports are not shared with foreign governments.

Dominica is a member of the Caribbean Financial Action Task Force (CFATF). The GOCD is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Dominica's FIU became a member of the Egmont Group in June 2003. Dominica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and to the Inter-American Convention against Terrorism. The GOCD has neither signed nor ratified the UN Convention against Corruption or the UN Convention against Transnational Organized Crime.

The Government of the Commonwealth of Dominica should fully implement and enforce the provisions of its legislation and provide additional resources for regulating offshore entities, including immobilizing the bearer shares of current "shell companies". It should stringently regulate Internet gaming entities. Dominica should take measures to update its anti-money laundering regulations and guidance notes to reflect current international standards. In addition, Dominica should conduct awareness training for financial institutions, specifically banks, to ensure their understanding and compliance of STR reporting requirements. The GOCD should either commit to engage in scrupulous due diligence on Economic Citizenship applicants, or eliminate the program. Per its agreements with the United States Government (USG), Dominica should make efforts to share information with the USG in an effective and timely manner as stipulated under the terms of its MLAT and Tax information Exchange Agreement. The GOCD should also become a party to the UN Convention against Corruption and the UN Convention against Transnational Organized Crime.

Dominican Republic

As a major transit country for drug trafficking, the Dominican Republic remains vulnerable to money laundering. Financial institutions in the Dominican Republic engage in currency transactions involving international narcotics trafficking proceeds that include significant amounts of U.S. currency or currency derived from illegal drug sales in the United States. The smuggling of bulk cash by couriers and the use of wire transfer remittances are the primary methods for moving illicit funds from the United States into the Dominican Republic. Once in the Dominican Republic, currency exchange houses, money remittance companies, real estate and construction companies, and casinos facilitate the laundering of these illicit funds.

Money laundering in the Dominican Republic is criminalized under Act 17 of 1995 (the 1995 Narcotics Law) and Law No. 72-02 of 2002. Under these laws, the predicate offenses for money laundering include illegal drug activity, trafficking in human beings or human organs, arms trafficking, kidnapping, extortion related to recordings and electronic tapes, theft of vehicles, counterfeiting of currency, fraud against the state, embezzlement, and extortion and bribery related to drug trafficking. Law 183-02 also imposes financial penalties on institutions that engage in money laundering, although the Government of the Dominican Republic (GODR) is in the process of amending the law to add a parallel structure of criminal penalties. Law No. 78-03 permits the seizure, conservation and administration of assets that are the product or instrument of criminal acts pending judgment and sentencing. The 1995 Narcotics Law allows preventive seizures and criminal forfeiture of drug-related assets, and authorizes international cooperation in forfeiture cases.

While narcotics-related investigations have been initiated under the 1995 Narcotics Law, and substantial currency and other assets have been confiscated, there have been only four successful money laundering prosecutions under this law. In August 2006, the Attorney General's office created a financial crimes unit to actively pursue financial crimes and money laundering investigations to aid in prosecutors' ability to obtain money laundering convictions. Since 2006, there have been 25 investigations and seven cases brought to court, one of which is the Banco Intercontinental (BANINTER) case.

The 2003 collapse of BANINTER revealed 14 years of double-bookkeeping designed to hide sweetheart loans, embezzlement, and money laundering. Subsequent state reimbursement of depositors resulted in costs of approximately 2.3 billion dollars. With the fraud-based collapse of Banco Mercantil and Banco Nacional de Credito (BANCREDITO) that same year, total bank fraud-based losses to the Dominican government approached \$3 billion in 2003. These frauds gutted the Dominican economy, almost tripled national indebtedness, and caused a massive devaluation of the Dominican peso. The GODR negotiated an International Monetary Fund (IMF) standby loan in August 2003 to help cover the costs of the failures. The IMF insisted on extensive changes in laws and procedures to improve banking supervision. Though legislative changes have been made, full implementation of IMF requirements lags.

By the end of 2007, the prosecutor's investigations were essentially completed in the BANCREDITO case, although none of the convictions—which are currently under appeal—were for money laundering. Preparations for a case against Banco Mercantil officials have been hampered since February as the Supreme Court has not yet resolved related jurisdictional issues. In the BANINTER case, which concluded in November 2007, convictions and significant sentences were entered for bank president Ramon Baez Figueroa and bank vice-president Marcos Baez Coco for violation of banking and monetary laws, although both were acquitted of money laundering. Dominican economist and entrepreneur Luis Alvarez Rentá, a U.S. citizen, was convicted of criminal money laundering in connection with the collapse and sentenced to ten years in prison. These convictions, criticized by civil society, the media, and jurists as internally inconsistent, are nevertheless a significant challenge to impunity for the country's elite. The convictions are currently under appeal.

Under Law No. 72-02 and Decree No. 288-1996, numerous financial and nonfinancial institutions are subject to anti-money laundering provisions. Obligated entities include banks, currency exchange houses, stockbrokers, securities brokers, the Central Bank, cashers of checks or other types of negotiable instruments, issuers/sellers/cashers of travelers checks or money orders, credit and debit card companies, remittance companies, offshore financial service providers, casinos, real estate agents, automobile dealerships, insurance companies, and certain commercial entities such as those dealing in firearms, metals, archeological artifacts, jewelry, boats, and airplanes. The law mandates that these entities must report suspicious transactions as well as all currency transactions exceeding U.S. \$10,000, and maintain records for a minimum of five years. Moreover, the legislation requires individuals to declare cross-border movements of currency that are equal to or greater than the equivalent of U.S. \$10,000 in domestic or foreign currency.

In 1997 the Unidad de Inteligencia Financiera (UIF) was established as the financial intelligence unit (FIU) of the Dominican Republic, with the responsibility of receiving financial disclosures and suspicious transaction reports (STRs) from reporting entities in the financial sector. In 2002, Law 72-02 created the Unidad de Análisis Financiero (Financial Analysis Unit, or UAF) that reports to the National Anti-Money Laundering Committee, and has the mandate to receive financial disclosures and STRs from both financial and nonfinancial reporting entities, as well as present leads to the prosecutors' office. According to the GODR, the UAF, which became operational in 2005, has replaced the UIF as the FIU of the Dominican Republic. As a result, the UIF, which became a member of the Egmont Group in 2000, lost its membership in November 2006 as it is no longer the legally recognized FIU of the Dominican Republic. The UAF anticipates applying for Egmont membership once a full transition of FIU functions and responsibilities are complete and the GODR has formally criminalized terrorist financing, as the criminalization of terrorist financing is now a requirement for all new members of the Egmont Group.

Although the UAF is now recognized as the GODR's financial intelligence unit, it appears that there is still confusion among obligated entities regarding their reporting requirements. In 2007, rather than reporting directly to the UAF, reporting entities filed 824 STRs with the UIF. The UIF then reported the STRs to the UAF. The majority of the reports the UAF received in 2007 are believed to have been transferred from the UIF.

Further confounding the duality of FIU functions in the Dominican Republic is the proposed creation of an offshore financial center with its own agency equivalent to an FIU. In 2006, legislation was introduced by the GODR to allow for the creation of an Independent Financial Center of the Americas (IFCA), which would not be subject to the regulatory authority of GODR banking supervisors. To reassure international concerns regarding the IFCA's susceptibility to abuse by money launderers and terrorist financiers, as well as the GODR's inability to ensure that the IFCA complies with anti-money laundering and counter-terrorist financing standards, the creators of the IFCA have proposed establishing their own FIU to report to the UAF and exchange information with other FIUs. However, an FIU must by definition be a single, national entity. Although proposed amendments to the draft legislation suggest changing the name of the IFCA's FIU-equivalent agency to avoid confusion, it would still serve as a filter for STRs that should be sent to the UAF, which is not permissible under the international standards of the Egmont Group and Financial Action Task Force.

Although terrorist financing is not a crime in the Dominican Republic, the GODR continues to support U.S. Government efforts to identify and block terrorist-related funds. While no assets have been identified or frozen, the GODR's efforts to identify and block terrorist-related funds continue through orders and circulars issued by the Ministry of Finance and the Superintendence of Banks that instruct all financial institutions to continually monitor accounts. The GODR has not enacted specific legislation that would criminalize the financing of terrorism and provide reporting entities with a legal basis to carry out counter-terrorist financing prevention programs.

According to U.S. law enforcement officials, cooperation between law enforcement agencies on drug cases, human trafficking, and extradition matters remains strong. In 2007, GODR and U.S. law enforcement were able to work together to intercept and disrupt bulk cash smuggling organizations operating in the airports and seaports of the Dominican Republic. Law enforcement in the Dominican Republic is also actively targeting commercial flights and vessels that operate to drug source countries to disrupt the illicit money flow back to narcotics traffickers.

The United States continues to encourage the GODR to join a mutual legal assistance treaty with the Organization of American States (OAS) and sign related money laundering conventions. The Dominican Republic is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The Dominican Republic is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. The GODR has signed, but has not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism.

The GODR is enhancing its anti-money laundering regime; however, additional improvements are needed, particularly with regard to combating terrorist financing. Legislative and oversight provisions are being put in place in the formal financial sector, but there exists a lack of coordination among the various entities tasked with anti-money laundering activities. Weak implementation of anti-money laundering legislation leaves the Dominican Republic vulnerable to criminal financial activity. The Government of the Dominican Republic should enhance supervision of the nonfinancial sector, and ensure this sector's compliance with reporting requirements. The GODR should bolster the operational capacity of the fledgling UAF and ensure a full transition of FIU functions. Provisions should be put in place to ensure that the International Financial Center of the Americas is not susceptible to money laundering and terrorist financing activity, and the establishment of a FIU-equivalent within the IFCA should be prohibited. The GODR should formally criminalize the financing of terrorism and ratify the International Convention for the Suppression of the Financing of Terrorism.

Ecuador

With a dollar economy geographically situated between two major drug producing countries, Ecuador is highly vulnerable to money laundering, although it is not an important regional financial center. Because thus far only a few major banks have active money laundering controls in place, and because a large number of transactions take place through unregulated money exchange and remittance companies, there is no reliable way to judge the magnitude of such activity in the country. In addition to concerns about illicit transactions through financial institutions, there is evidence that money laundering is taking place through trade and commercial activity. Large amounts of unexplained currency entering and leaving Ecuador indicate that transit and laundering of illicit cash are also significant activities. Though smuggled goods are regularly brought into the country, there is no evidence that they are significantly funded by drug proceeds.

Ecuador's financial sector consists of 29 banks, 13 investment companies, two formal exchange houses, 28 cooperatives, 39 insurance companies, two stock exchanges, and eight mutual funds. Several Ecuadorian banks maintain offshore offices. The Superintendence of Banks and Insurance is responsible for oversight of both offshore and onshore financial institutions. Regulations are essentially the same for onshore and offshore banks, with the exception that offshore deposits no longer qualify for the government's deposit guarantee. Anonymous directors are not permitted. Licensing requirements are the same for offshore and onshore financial institutions. However, offshore banks are required to contract external auditors pre-qualified by the Superintendence of Banks. These private accounting firms perform the standard audits on offshore banks that would generally be undertaken by the Superintendence in Ecuador. Bearer shares are not permitted for banks or

companies in Ecuador. Small local credit unions are numerous and are regulated only by the Ministry of Social Affairs

Law 2005-13 of October 2005 criminalizes money laundering in Ecuador. The law criminalizes the laundering of illicit funds from any source and penalizes the undeclared entry of more than \$10,000 in cash or other convertible assets. Prior to the passage of Law 2005-13, the Narcotics and Psychotropic Substance Act of 1990 (Law 108) criminalized money laundering activities only in connection with illicit drug trafficking. The new law criminalizes money laundering in relation to any illegal activity, including drug trafficking, trafficking in persons and prostitution. Money laundering is penalized by a prison term of one to nine years, depending upon the amount laundered, as well as a monetary fine. However, it is unclear if a conviction is required for the predicate offense to prosecute for money laundering, and money laundering is only considered to be a crime if the amount of funds laundered exceeds U.S. \$5,000.

Law 2005-13 established the National Council Against Money Laundering, headed by the Procurador General (solicitor general) and includes representatives of all government entities involved in fighting money laundering, such as the Superintendence of Banks and the National Police. Law 2005-13 also establishes Ecuador's financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), under the purview of the Council. Regulations for application of the law and establishment of the FIU were published in April 2006 under Decree 1328. The first UIF director was appointed in November 2006 but quickly resigned. A second director was appointed in December 2006 and currently leads the UIF. During 2007, the UIF acquired office space, hired 17 personnel, and set up computer systems. The UIF became operational on December 1, 2007. In the month of December, the UIF received 61 suspicious transaction reports (STRs) from obligated entities, and referred 20 suspicious transactions to the judicial police and Attorney General's Office for review. Although now operational, the director is still seeking technical support and improved software to improve the analytical capacity of the unit.

All entities that fall under the 1994 Financial System Law, including banks, savings and credit institutions, investment companies, stock exchanges, mutual funds, exchange houses, credit card administrators, money transmitters, mortgage companies, insurance companies and reinsurance companies, are required to report all "unusual and unjustified" transactions to the UIF within 48 hours. Financial institutions under the supervision of the Superintendence of Banks and Insurance currently report suspicious transactions to the Superintendence. Obligated entities are also required to establish "know-your-client" provisions, report cash transactions over \$10,000, and maintain financial transaction records for ten years. Any person entering Ecuador with \$10,000 or more in cash must file a report with the customs service; however, this requirement is currently not being enforced. Entities or persons who fail to file the required reports or declarations may be sanctioned by the Superintendence of Banks. The UIF may request information from any of the obligated entities to assist in its analysis of suspicious transactions, and cases that are deemed to warrant further investigation will be sent to the Public Ministry. The UIF is also empowered to exchange information with other financial intelligence units on the basis of reciprocity.

Some existing laws may conflict with the detection and prosecution of money laundering. For example, the Bank Secrecy Law severely limits the information that can be released by a financial institution directly to the police as part of any investigation, and the Banking Procedures Law reserves information on private bank accounts to the Superintendence of Banks. In addition, the Criminal Defamation Law includes sanctions for banks and other financial institutions that provide information about accounts to police or advise the police of suspicious transactions if no criminal activity is ultimately proven. The law also does not provide safe harbor provisions for bank compliance officers.

Many of these obstacles can be overcome by a judge properly issuing an appropriate warrant. Also, the UIF is entitled by law to obtain information from the Superintendence of Banks and individual financial institutions, as an exception to the Banking Secrecy Law, and can provide this information to

the judicial police when part of an investigation. However, this contradictory legal framework may impede cooperation between other Government of Ecuador (GOE) agencies and the police, and cooperation to date has fallen short of the level needed for effective enforcement of money laundering statutes.

Ecuador's first major money laundering case began in August 2006 with the arrest of approximately a dozen alleged members of a Colombian money laundering operation and the seizure of a large number of assets in Ecuador. The suspects were linked to accused drug trafficker Hernan Prada Cortes, who had acquired many Ecuadorian businesses and real properties in the names of other persons since 2000, and was recently extradited to the United States from Colombia. Two of the ten individuals detained in 2006 were released due to insufficient evidence, while the other eight remain in detention and pending trial. The prosecution of this case has been delayed, in part, pending additional evidence that is expected from the Prada trial in the United States. There have been a total of three money laundering cases initiated by prosecutors since the passage of Law 2005-13, and no convictions to date.

Ecuador's legal system provides for asset forfeiture upon conviction; however, civil forfeiture is not permitted. The National Council Against Money Laundering is responsible for administering the freezing and seizure of funds that are identified as originating from illicit sources. A special fund for forfeited assets will be set up in the Central Bank, and these assets will be distributed among government entities responsible for combating money laundering. No statistics are available on the amount of assets seized or frozen by the GOE in 2007.

Terrorist financing has not been criminalized in Ecuador. The Ministry of Foreign Affairs, Superintendence of Banks and the Association of Private Banks formed a working group in December 2004 to draft a law against terrorist financing. In 2006, the draft law passed its first debate in Congress, but since then the draft has seen no revisions and is awaiting further debate. With the Congress in recess and the transition to a Constituent Assembly, there has been little opportunity to address the issue.

The Superintendence of Banks has cooperated with the U.S. Government in requesting financial institutions to report transactions involving known terrorists, as designated by the United States as Specially Designated Global Terrorists pursuant to Executive Order 13224, or as named on the consolidated list maintained by the United Nations 1267 Sanctions Committee. No terrorist finance assets have been identified to date in Ecuador. The Superintendence would have to obtain a court order to freeze or seize such assets, in the event they were identified in Ecuador. No steps have been taken to prevent the use of gold and precious metals to launder terrorist assets. Currently, there are no measures in place to prevent the misuse of charitable or nonprofit entities to finance terrorist activities.

Ecuador is a member of the Financial Action Task Force for South America (GAFISUD), and held the GAFISUD presidency in 2007. The GOE underwent a mutual evaluation by GAFISUD in September 2007, and the mutual evaluation report was accepted by the GAFISUD plenary in December 2007. The evaluation team found the GOE to be noncompliant or only partially compliant with 48 of the 49 Financial Action Task Force Recommendations on money laundering and terrorist financing. The mutual evaluation report noted the lack of a counter-terrorist financing law and the lack of successfully prosecuted money laundering cases, but recognized that the UIF is making some progress.

Ecuador is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. The GOE is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Ecuador and the United States are parties to a bilateral Agreement for the Prevention and Control of Narcotics Related Money Laundering that entered into force in 1993 and a 1994 Agreement to Implement the United Nations Convention against Illicit

Trafficking in Narcotic Drugs and Psychotropic Substances of December 1988, as it relates to the transfer of confiscated property, securities and instrumentalities. There is also a Financial Information Exchange Agreement (FIEA) between the GOE and the U.S. to share information on currency transactions. The UIF has signed memoranda of understanding with the FIUs of Argentina, Brazil, Bolivia, Chile, Colombia, Panama, and Peru for the exchange of information.

The Government of Ecuador has made progress in combating money laundering in recent years with the passage of anti-money laundering legislation and the establishment of an operational financial intelligence unit. However, the GOE should fully implement the existing legislation and ensure that reporting requirements are enforced. Ecuador is one of only two countries in South America that is not a member of the Egmont Group of FIUs, and the GOE should ensure that the UIF becomes fully functional and meets the standards of the Egmont Group and the Financial Action Task Force. Ecuador still needs to criminalize the financing of terrorism, which is a prerequisite for membership in the Egmont Group and is necessary to fully comply with international anti-money laundering and counter-terrorist financing standards. The GOE should address items that were not accounted for in its money laundering legislation, including the abolition of strict bank secrecy limitations and any potential sanctions for financial institutions that report suspicious transactions. The GOE should also amend its current legislation so that the laundering of funds under U.S. \$5,000 is considered to be a money laundering offense, and clarify whether a conviction for a predicate offense is required before prosecutors may charge an individual with money laundering.

Egypt, The Arab Republic of

Egypt is not considered a regional financial center or a major hub for money laundering. Egypt still has a large informal cash economy, and many financial transactions do not enter the banking system. As part of its on-going economic reform plan, the Government of Egypt (GOE) continued financial sector reform in 2007. Few money laundering cases have made it to court in the last several years. Illegal dealings in antiquities, corruption, misappropriation of public funds, smuggling, and the use of alternative remittance systems, such as hawala, increase Egypt's vulnerability to money laundering.

While there is no significant market for illicit or smuggled goods in Egypt, there is evidence that arms are being smuggled across Egypt's border with Gaza. The funding source is unclear, as is the destination of the proceeds. Other than arms smuggling, authorities say that the under-invoicing of imports and exports by Egyptian businessmen is still a relatively common practice. The primary goal for businessmen who engage in such activity is reportedly to avoid taxes and customs fees. Customs fraud and invoice manipulation are also found in regional value transfer schemes. The number of businesses and individuals filing tax returns as a result of June 2005 tax cuts continue to rise. Nevertheless, a large portion of Egyptian economy remains undocumented and tax evasion is commonplace.

At present, money laundering and terrorist financing are officially reported as not widespread. The few cases of money laundering that have been detected involved laundering of money through the formal banking sector. However, informal remittance systems are widespread in Egypt, and are a potential means for laundering funds. Nevertheless, Egyptian authorities claim these systems do not operate in Egypt, and therefore make no effort to detect, monitor and regulate them. Due to lack of regulation and investigations, it is unclear if and to what extent money laundering is actually occurring through these systems. Expatriate Egyptian workers frequently use informal underground remittance systems due to cost and unfamiliarity with official banking procedures. Western Union and Moneygram, the two formal cash transfer operators in Egypt, are also widely used and managers have petitioned the Central Bank to expand their operations. The Central Bank has not yet approved the requests. Reports on the number of Egyptian expatriate workers are contradictory, but the figure generally stated is 5

million. The latest figures from the Central Bank indicate that overseas workers remitted U.S. \$6.321 billion in fiscal year 2006-2007.

Egypt does not have a high prevalence of financial crimes, such as counterfeiting or bank fraud. There is no evidence that Egyptian financial institutions engage in currency transactions involving international narcotics-trafficking proceeds. The Anti-Money Laundering (AML) Law No. 80 of 2002 criminalizes laundering of funds from narcotics trafficking, prostitution and other immoral acts, terrorism, antiquities theft, arms dealing, organized crime, and numerous other activities. The law did not repeal Egypt's existing law on bank secrecy, but it did provide the legal justification for providing account information to responsible civil and criminal authorities. The law established the Egyptian Money Laundering Combating Unit (EMLCU) as Egypt's financial intelligence unit (FIU), which officially began operating on March 1, 2003, as an independent entity within the Central Bank. The administrative regulations of the EMLCU provide the legal basis by which the EMLCU derives its authority, spelled out the predicate crimes associated with money laundering, established a Council of Trustees to govern the EMLCU, defined the role of supervisory authorities and financial institutions, and allowed for the exchange of information with foreign competent authorities.

The Central Bank's Supervision Unit shares responsibility with the EMLCU for regulating banks and other financial institutions and ensuring compliance with AML law. Under the AML law, banks are required to keep all records for five years, and numbered or anonymous financial accounts are prohibited. The Central Bank also requires banks to maintain internal systems enabling them to comply with the AML law and has issued an instruction to banks requiring them to examine large transactions. In addition, banks are required to submit quarterly reports demonstrating compliance with AML regulations. Reporting of suspicious transactions is required by banks and nonbank financial institutions.

The Central Bank and EMLCU undertook frequent compliance assessments of all banks operating in Egypt. The assessments consisted of questionnaires and on-site visits to check AML compliance systems. Where deficiencies were found, banks were notified of corrective measures to be undertaken with a deadline for making the necessary changes and follow-up visits to reassess compliance. Sanctions for noncompliance include issuing a warning letter; imposing financial penalties; forbidding banks to undertake certain activities; replacing the board of directors; and revoking the bank's license. The Central Bank also monitors bureaux de change and money transmission companies for foreign exchange control purposes, giving special attention to those accounts with transactions above certain limits. The Capital Market Authority (CMA), which is responsible for regulating the securities markets, also conducts inspections of firms and independent brokers and dealers under its jurisdiction. Inspections are aimed at explaining and discussing AML regulations and obligations, as well as evaluating the implementation of systems and procedures, including checking for an internal procedures manual and ensuring the appointment of compliance officers.

In 2006, an independent insurance regulatory authority was established and charged with supervising insurance companies for compliance with AML laws and regulations. The General Authority for Free Zones and Investment (GAFI) regulates activity in free zones and Special Economic Zones (SEZ). The Ministry of Communication and Information Technology regulates the Postal Authority and the financial services it offers. Egypt allows gambling in casinos located in international hotels, but only foreigners are allowed to enter the casinos. All cash transactions at casinos are performed by licensed banks subject to AML controls. Individuals acting as financial intermediaries, such as lawyers, accountants, and cash couriers, are not currently subject to AML controls, although EMLCU officials have indicated that the law will soon be amended to cover the activities of these individuals. The AML law protects institutions and individuals who cooperate with law enforcement officials.

The executive regulations of the AML law lowered the threshold for declaring foreign currency at borders from the equivalent of U.S. \$20,000 to U.S. \$10,000. The declaration requirement was also

extended to travelers leaving as well as entering the country. However, enforcement of this provision is not consistent. The Customs Authority also signed an agreement with the EMLCU to share information on currency declarations. Authorities claim that the terrorist attacks of the past several years have given extra impetus to law enforcement agencies to thoroughly scrutinize currency imports/exports. As an example, there have been reports that Hamas ministers in the last Palestinian cabinet were crossing the Egypt-Gaza border with large amounts of cash. Egyptian Customs Authorities now pass all reports of foreign currency declarations at the border to the EMLCU and also alert the European Union border guards of individuals crossing the border with large amounts of cash.

Egypt is not an offshore financial center. Offshore banks, international business companies, and other forms of exempt or shell companies are not permitted in the country. Egypt has nine public free zones, 250 private free zones, and one SEZ. Public free zones are outside of Egypt's customs boundaries, so firms operating within them have significant freedom with regard to transactions and exchanges. The firms may be foreign or domestic, may operate in foreign currency, and are exempt from customs duties, taxes, and fees. Private free zones are usually limited to a single project such as mixing, repackaging, assembling and/or manufacturing for re-export. The SEZs allow firms operating in them to import capital equipment, raw materials, and intermediate goods duty-free and to operate tax-free. All banks and nonfinancial institutions operating in such zones are subject to Egypt's AML law provisions (AML).

The EMLCU, Egypt's FIU, is an independent entity within the Central Bank. The EMLCU has its own budget and staff and also has the full legal authority to examine and analyze all Suspicious Transaction Reports (STRs). Investigations are conducted by law enforcement agencies, including the Ministry of Interior, the National Security Agency, and the Administrative Control Authority. The EMLCU shares information with these agencies. The unit handles implementation of the AML law, which includes publishing the executive directives. The EMLCU takes its direction from a six-member council, the Council of Trustees, which is chaired by the Assistant Minister of Justice for Legislative Affairs. Other members of the Council include the Chairman of the CMA, the Deputy Governor of the Central Bank, a Sub-Minister (Under Secretary) from the Ministry of Social Solidarity, a representative from the Egyptian Banking Federation, and an expert in financial and banking affairs. In June 2004, the EMLCU was admitted to the Egmont Group of FIUs.

The Executive Director of the EMLCU is responsible for the operation of the FIU and the implementation of the policies drafted by the Council of Trustees. His responsibilities include: proposing procedures and rules to be observed by different entities involved in combating money laundering; presenting these rules and procedures to the Chairman of the Council of Trustees; reviewing the regulations issued by supervisory authorities for consistency with legal obligations and ensuring that they are up to date; ensuring the capability and readiness of the unit's database; exchanging information with supervisory entities abroad; acting as a point of contact within the GOE; preparing periodic and annual reports on the operational status of the unit; and taking necessary action on STRs recommended to be reported to the Office of Public Prosecution.

In 2002, the GOE passed the Law on Civil Associations and Establishments (Law No. 84 of 2002), which governs the procedures for establishing nongovernmental organizations (NGOs), including their internal regulations, activities, and financial records. The Law places restrictions on accepting foreign donations without prior permission from the proper authorities. Both the Ministry of Social Solidarity and the Central Bank continually monitor the operations of domestic NGOs and charities to prevent the funding of domestic and foreign terrorist groups.

Although the AML law does not specifically allow for seizure and confiscation of assets from money laundering, the Penal Code authorizes seizure of assets related to predicate crimes, including terrorism. All assets are subject to seizure, including moveable and immovable property, rights and businesses. Assets can only be seized with an order from the Public Prosecutor, and the agency responsible for

seizing the assets depends on the predicate crime. Typically, the Central Bank seizes cash and the Ministry of Justice seizes real assets. Confiscated assets are given to the Ministry of Finance, and the executive regulations of the AML law allow for sharing of confiscated assets with other governments. The Public Prosecutor's office is currently engaged in negotiations to enhance cooperation with other governments on asset seizure and confiscation.

Because of its own historical problems with domestic terrorism, the GOE has sought closer international cooperation to counter terrorism and terrorist financing. The GOE has shown a willingness to cooperate with foreign authorities in criminal investigations, whether they are related to terrorism or narcotics.

In January 2005, the National Committee for Combating Money Laundering and Terrorist Financing was established to formulate general strategy and coordinate policy implementation among the various responsible agencies of the GOE. The committee includes representatives from the Ministries of Interior, Foreign Affairs, Social Affairs, Justice, and the National Security Agency, in addition to the EMCLU. The same agencies sit on a National Committee for International Cooperation in Combating Terrorism, which was established in 1998.

The GOE is in the process of replacing its original counter-terrorism law, an emergency law enacted in 1981 that is due to expire in spring of 2008, with a new comprehensive law. It will reportedly include specific measures against terrorist financing. Currently, article 86 of the Egyptian Penal Code criminalizes the financing of terrorism.

The United States and Egypt have a Mutual Legal Assistance Treaty. Egyptian authorities have cooperated with U.S. efforts to seek and freeze terrorist assets. Egypt also has agreements for cooperation on AML issues with the UK, Romania, Zimbabwe, and Peru. The Central Bank circulates to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. No related assets were identified, frozen, seized, or forfeited in 2007.

Egypt is a founding member of the Middle East and North Africa Financial Action Task Force (MENAFATF) and follows that organization's recommendations on anti-money laundering and counter-terrorist financing. There is no information available on Egypt's mutual evaluation by MENAFATF. Egypt is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption.

The Government of Egypt will not have a successful anti-money laundering and terrorist finance regime until it has successful prosecutions and convictions. Improved investigative capacity in financial crimes is a prerequisite. Egypt should consider ways of improving the EMLCU's feedback on STRs to reporting institutions. It should improve its enforcement of cross-border currency controls, specifically allowing for seizure of suspicious cross-border currency transfers. Egyptian law enforcement and customs authorities should examine and investigate trade-based money laundering, informal value transfer systems, and customs fraud. The GOE should ensure that its updated law against terrorism specifically addresses the threat of terrorist financing, including asset identification, seizure and forfeiture.

El Salvador

Located on the Pacific coast of the Central American isthmus, El Salvador has one of the largest and most developed banking systems in Central America. Its most significant financial contacts are with neighboring Central American countries, as well as with the United States, Mexico, and the Dominican Republic. The growth of El Salvador's financial sector, the increase in narcotics

trafficking, the large volume of remittances through the formal financial sector and alternative remittance systems, and the use of the U.S. dollar as legal tender make El Salvador vulnerable to money laundering. In 2007, approximately \$3.5 billion in remittances were sent to El Salvador through the financial system. Most were sent from Salvadorans working in the United States to family members. The quantity of additional remittances that flow back to El Salvador via other methods such as visiting relatives, regular mail and alternative remittance systems is not known.

Most money laundering is conducted by international criminal organizations. These organizations use bank and wire fund transfers from the United States to disguise criminal revenues as legitimate remittances to El Salvador. The false remittances are collected and transferred to other financial institutions until sufficiently laundered for use by the source of the criminal enterprise, usually a narcotics trafficking organization. One such case was investigated jointly by the Drug Enforcement Administration (DEA) and the Government of El Salvador (GOES) beginning in 2005. Two individuals were arrested. One Panamanian national was subsequently found guilty of money laundering in 2006, and a Salvadoran pled guilty in 2007. It is estimated that between U.S. \$7 million and U.S. \$11 million were laundered through local Western Union branch remittances.

Decree 498 of 1998, the “Law Against the Laundering of Money and Assets,” criminalizes money laundering related to narcotics trafficking and other serious crimes, including trafficking in persons, kidnapping, extortion, illicit enrichment, embezzlement and contraband. The law also establishes the financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), within the Attorney General’s Office. The UIF has been operational since January 2000. The National Civilian Police (PNC) and the Central Bank also have their own anti-money laundering units.

Under Decree 498, financial institutions must identify their customers, maintain records for a minimum of five years, train personnel in identification of money and asset laundering, establish internal auditing procedures, and report all suspicious transactions and transactions that exceed approximately U.S. \$57,000 to the UIF. Entities obligated to comply with these requirements include banks, finance companies, exchange houses, stock exchanges and exchange brokers, commodity exchanges, insurance companies, credit card companies, casinos, dealers in precious metals and stones, real estate agents, travel agencies, the postal service, construction companies, and the hotel industry. The law includes a safe harbor provision to protect all persons who report transactions and cooperate with law enforcement authorities, and also contains banker negligence provisions that make individual bankers responsible for money laundering at their institutions. Bank secrecy laws do not apply to money laundering investigations.

In 2007, the GOES investigated 27 cases of suspected money laundering. GOES law enforcement arrested five individuals suspected of engaging in money laundering and financial crime, and prosecutors obtained convictions for four of those individuals in 2007. There were also two notable high-profile financial crime cases in 2007. In the first, a former National Legislative Assembly Deputy facing public corruption and money laundering charges fled to the United States and was later apprehended in Anaheim, California, and held on immigration charges. In the second high-profile case, a fugitive financier wanted on charges of defrauding Salvadoran investors in a case dating back to 2005 was arrested in Miami, Florida, and held pending resolution of a Salvadoran government extradition request.

The GOES has begun to more aggressively investigate private companies and financial service providers involved in suspicious financial activities. Despite demonstrating a greater commitment to pursue financial crimes, the GOES still lacks sufficient prosecutorial and police resources to adequately investigate and prosecute financial crimes. The GOES has established a secure computerized communication link between the Attorney General’s office and the financial crimes division of the National Civilian Police. In addition to providing communication, the system has a software component that filters, sorts, and connects financial and other information vital to money

laundering investigations. The system, which became operational in 2006, is expected to enhance investigative capabilities. The UIF recently undertook an effort to establish a closer information sharing relationship with the Superintendent of the Salvadoran Financial System (SSF), as well as to formally incorporate the SSF into the existing secure computerized communication link.

To address the problem of international transportation of criminal proceeds, Decree 498 requires all incoming travelers to declare the value of goods, cash, or monetary instruments they are carrying in excess of approximately U.S. \$11,400. Falsehood, omission, or inaccuracy on such a declaration is grounds for retention of the goods, cash, or monetary instruments, and the initiation of criminal proceedings. If, following the end of a 30-day period, the traveler has not proved the legal origin of said property, the Salvadoran authorities have the authority to confiscate the assets. In 2007, eight individuals were detected carrying undeclared cash at the international airport or at international border crossings, and a total of U.S. \$1.2 million was confiscated from these individuals.

The GOES has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related and other assets of serious crimes. Forfeited money laundering proceeds are deposited in a special fund used to support law enforcement, drug treatment and prevention, and other related government programs, while funds forfeited as the result of other criminal activity are deposited into general government revenues. Law enforcement agencies are allowed to use certain seized assets while a final sentence is pending. In practice, however, forfeited funds are rarely channeled to counternarcotics operations. There exists no legal mechanism to share seized assets with other countries. Salvadoran law currently provides only for the judicial forfeiture of assets upon conviction, and not for civil or administrative forfeiture. A draft law to reform Decree 498 to provide for civil forfeiture of assets, currently in the national legislature, has run into resistance from businessmen and others who are fearful that a civil asset forfeiture regime could lead to a crackdown on tax evaders, or possibly be misused for political purposes. In 2007, the GOES froze U.S. \$57,853 in bank deposits related to money laundering and financial crime investigations.

The GOES passed counterterrorism legislation, Decree No. 108, in September 2006. Decree No. 108 further defines acts of terrorism and establishes tougher penalties for the execution of those acts. Article 29 of Decree No. 108 establishes the financing of terrorism as a criminal offense, punishable by a prison term of 20 to 30 years and a monetary fine ranging from \$100,000 to \$500,000. The law also granted the GOES the legal authority to freeze and seize suspected assets associated with terrorists and terrorism. However, provisions to improve supervision of cash couriers, wire transfers, and financing of nongovernmental organizations (NGOs) that were included in an early draft were not included in the final law.

The GOES has circulated the names of suspected terrorists and terrorist organizations listed on the United Nations (UN) 1267 Sanctions Committee consolidated list to financial institutions. These institutions are required to search for any assets related to the individuals and entities on the consolidated list. There is no evidence that any charitable or nonprofit entity in El Salvador has been used as a conduit for terrorist financing.

El Salvador has signed several agreements of cooperation and understanding with financial supervisors from other countries to facilitate the exchange of supervisory information, including permitting on-site examinations of banks and trust companies operating in El Salvador. El Salvador is also a party to the Treaty of Mutual Legal Assistance in Criminal Matters signed by the Republics of Costa Rica, Honduras, Guatemala, Nicaragua, and Panama. Salvadoran law does not require the UIF to sign agreements to share or provide information to other countries. The GOES is party to the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, which provides for parties to cooperate in tracking and seizing assets. The UIF is also legally authorized to access the databases of public or private entities. The GOES has cooperated with foreign

governments in financial investigations related to narcotics, money laundering, terrorism, terrorist financing and other serious crimes.

El Salvador is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). The UIF has been a member of the Egmont Group since 2000. The GOES is party to the OAS Inter-American Convention against Terrorism, the UN International Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. El Salvador is also a signatory to the Central American Convention for the Prevention and Repression of Money Laundering Crimes Related to Illicit Drug Trafficking and Related Crimes.

The Government of El Salvador made advances in 2007 in terms of improvements in the operational capabilities of the UIF. To build upon this progress, however, El Salvador should continue to expand and enhance its anti-money laundering and counter-terrorist financing policies, and strengthen its ability to seize and share assets. The GOES should ensure the passage of the civil forfeiture legislation that is currently under consideration by the legislature. Remittances remain an important sector of the Salvadoran economy, and as such should be carefully supervised. The GOES should improve supervision of cash couriers and wire transfers as outlined in the Financial Action Task Force Nine Special Recommendations on terrorist financing. The GOES should also ensure that sufficient resources are provided to the overburdened Attorney General's office, as well as to the financial crime and narcotics divisions of the National Civilian Police.

France

France remains an attractive venue for money laundering because of its sizable economy, political stability, and sophisticated financial system. Narcotics trafficking, human trafficking, smuggling, and other crimes associated with organized crime are among its vulnerabilities.

The Government of France (GOF) first criminalized money laundering related to narcotics trafficking in 1987. Law 96-392 criminalizes the laundering of proceeds of all crimes. In 2004, the French Supreme Court ruled that joint prosecution of individuals was possible on both money laundering charges and the underlying predicate offense. Prior to this judgment, the money laundering charge and the predicate offense were considered the same offense and could only be prosecuted as one offense. French law has obliged institutions to combat money laundering since 1990. Entities obliged to file suspicious transaction reports (STRs) include those within a variety of financial and nonfinancial sectors, including banks, insurance companies, casinos, and lawyers.

Under Article 324 of the Penal Code, money laundering carries a penalty of five years imprisonment and a fine of 375,000 euros (approximately U.S. \$547,500). With aggravating circumstances such as habitual or organized activity or connection with narcotics trafficking (Article 222-38), the penalty increases to ten years imprisonment and a fine of 750,000 euros (approximately U.S. \$1,095,000). Legal procedure for criminal conspiracy applies to money laundering crimes.

As a member of the European Union (EU), France is obligated to implement all three EU money laundering directives. In late 2005, the EU adopted the Third Money Laundering Directive (2005/60/EC), which mandated an implementation deadline of December 15, 2007.

France has developed the Liaison Committee against the Laundering of the Proceeds of Crime, which is comprised of representatives from reporting professions and institutions, regulators, and law enforcement authorities. The Committee's purpose is to share information with regulated entities and to make proposals to improve the anti-money laundering (AML) system. The Justice Ministry and the French financial intelligence unit (FIU), known as the Unit for Treatment of Intelligence and Action Against Clandestine Financial Circuits or TRACFIN, co-chair this group.

The Banking Commission supervises fiduciary institutions and conducts regular audits of credit institutions. The Insurance and Provident Institutions Supervision Commission reviews insurance brokers. The Financial Market Authority monitors the reporting compliance of the stock exchange and other nonbank financial institutions. The Central Bank (Banque de France) oversees management of the records required to monitor banking transactions. Bank regulators and law enforcement can access the French Tax Administration's database to obtain information on the opening and closing of accounts. Information is available for depository accounts, transferable securities, and other properties, including cash assets. These records are important tools in the French arsenal for combating money laundering and terrorist financing.

France's FIU, TRACFIN, is responsible for analyzing suspicious transaction reports (STRs) filed by obliged entities. TRACFIN may exchange information with foreign counterparts that observe similar rules regarding reciprocity and confidentiality of information. TRACFIN works closely with the Ministry of Interior's Central Office for Major Financial Crimes (OCRGDF), which is the main point of contact for Interpol and Europol in France. TRACFIN can obtain information from senior police officers and central or local governments. The State Prosecutor informs the FIU of final court orders relating to suspicious transactions that have been reported.

TRACFIN received 12,047 STRs in 2006. The banking sector submits approximately 81 percent of STRs. The FIU referred 411 cases to the judicial authorities in 2006.

French law requires two types of reports, in addition to STRs, to be submitted to the FIU. An entity must file a report with TRACFIN when the identity of the principal or beneficiary remains unclear despite due diligence. There is no threshold limit for such reporting. Entities must also file reports when a financial entity acting in the form, or on behalf, of any asset management instrument, when legal or beneficial owners are unknown, carries out a transaction on a third party's behalf. The reporting obligation can also be extended by decree to transactions carried out by financial entities, on their own behalf or on behalf of third parties, with natural or legal persons, including their subsidiaries or establishments that are domiciled, registered, or established in any country or territory included on the Financial Action Task Force (FATF) list of noncooperative countries or territories.

Law No. 96-392 of 1996 instituted procedures for seizure and confiscation of the proceeds of crime. French law permits seizure of all or part of property. In cases of terrorist financing, France has promulgated an additional penalty of confiscation of the total assets of the terrorist offender. Authorities can freeze accounts and financial assets through both administrative and judicial measures.

Since 1986, French counter-terrorism legislation has provided for the prosecution of those involved in terrorist financing under the more severe offense of complicity in the act of terrorism. To strengthen this provision, France introduced several new characterizations of offenses, pointedly including terrorist financing. The offense of financing terrorist activities (Article 421-2-2 of the Penal Code) is defined according to the UN International Convention for the Suppression of the Financing of Terrorism and can result in ten years' imprisonment and a fine of 225,000 euros (approximately U.S. \$328,500). Since 2001, TRACFIN has referred 92 cases of suspected terrorist financing to the judicial authorities for prosecution. TRACFIN participates in the "Cell for the fight against the financing of terrorism," an informal group created within the French Ministry of the Economy, Finance, and Industry to gather information to fight terrorist financing.

The Government of France (GOF) moved to strengthen France's anti-terrorism legal arsenal with the Act of 23 January 2006, authorizing video surveillance of public places, including nuclear and industrial sites, airports, and railway stations. The Act requires telephone operators and Internet café owners to keep extensive records, allows greater government access to e-communications, and opens flight passenger lists and identification information to access by counter-terrorism officials. The Act stiffens prison sentences for directing a terrorist enterprise to 30 years and extends the possible period of detention without charge. The Act permits increased surveillance of potential targets of terrorism. It

empowers the Minister of the Economy to freeze the funds, financial instruments and economic resources belonging to individuals committing or attempting to commit acts of terrorism, and belonging to companies directly or indirectly controlled by these individuals. By granting explicit national authority to freeze assets, the Act closes a potential loophole concerning the freezing of a citizen's assets as oppose to a resident EU-member citizen's assets. Adopted in January 2006, it entered into force by presidential decree in April 2007.

French authorities have moved rapidly to identify and freeze financial assets of organizations associated with Al-Qaida and the Taliban under United Nations Security Council Resolution 1267. France takes actions against other terrorist groups through the EU-wide "clearinghouse" procedure. Within the Group of Eight, France has sought to support and expand efforts targeting terrorist financing. France has worked to engage and improve the AML and counter-terrorist financing (CTF) capabilities of some African countries by offering technical assistance. On the operational level, French law enforcement cooperation targeting terrorist financing continues to be strong.

The United States and France entered into a mutual legal assistance treaty (MLAT) in 2001. Through MLAT requests and by other means, the French have provided large amounts of data to the United States in connection with terrorist financing. TRACFIN is a member of the Egmont Group and Egmont Committee and has information-sharing agreements with 30 foreign FIUs.

France is a member of the Financial Action Task Force (FATF). It is a Cooperating and Supporting Nation to the Caribbean Financial Action Task Force (CFATF) and an Observer to the Financial Action Task Force of South America (GAFISUD). France is a party to the 1988 UN Drug Convention; the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the UN Convention against Transnational Organized Crime; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention against Corruption.

The Government of France has established a comprehensive anti-money laundering regime and is an active partner in international efforts to control money laundering and the financing of terrorism. France should continue its active participation in international organizations, and its outreach to lower-capacity recipient countries, to combat the domestic and global threats of money laundering and terrorist financing. France should ensure that the promulgating regulations for compliance with the Third Money Laundering Directive are fully effective, and that the supervisory authorities are well-equipped to handle their new duties. The GOF should enact a compulsory written cash declaration regime at its airports to ensure that travelers entering and exiting France and the EU provide, in writing, a record of their conveyance of currency or monetary instruments that can be saved and shared.

Germany

Germany is one of the largest financial centers in Europe. Most of the money laundering that occurs in Germany relates to white-collar crime. Although not a major drug producing country, Germany continues to be a consumer and a major transit hub for narcotics. Organized criminal groups involved in drug trafficking and other illegal activities are an additional source of money laundering in Germany. Germany is not an offshore financial center.

In 2002, the Federal Republic of Germany (FRG) enacted a number of laws to improve law enforcement's ability to combat money laundering and terrorist financing. The measures brought German laws into line with the first and second European Union (EU) Money Laundering Directives, which mandate suspicious activity reporting by a variety of entities, including notaries, accountants, tax consultants, casinos, luxury item retailers, and attorneys.

Money Laundering and Financial Crimes

In May 2002, the German banking, securities, and insurance industry regulators merged into a single financial sector regulator known as the Federal Financial Supervisory Authority (BaFIN). Germany's anti-money laundering (AML) legislation requires that BaFIN maintain a centralized register of all bank accounts with electronic access to all key account data held by banks in Germany. Banks cooperate with German authorities. Many have independently developed risk assessment software to screen potential and existing clients and their financial activity, and to monitor transactions for suspicious activity.

Germany's Money Laundering Act, amended by the Act on the Improvement of the Suppression of Money Laundering and Combating the Financing of Terrorism of August 8, 2002, criminalizes money laundering related to narcotics trafficking, fraud, forgery, embezzlement, and membership in a terrorist organization. It also increases due diligence and reporting requirements for banks and financial institutions and requires financial institutions to obtain customer identification for transactions conducted in cash or precious metals exceeding 15,000 euros (approximately U.S. \$22,000). The legislation mandates more comprehensive background checks for owners of financial institutions and tighter rules for credit card companies. Banks must report suspected money laundering to the FIU as well as to the State Attorney (Staatsanwaltschaft).

The Federal Interior Ministry has drafted new legislation to implement the third EU Money Laundering Directive. The legislation is expected to be adopted in mid-2008. In addition to requiring that EU member states implement the Financial Action Task Force's (FATF) 40 Recommendations, the directive contains further provisions on customer due diligence and other internal risk-management measures to prevent money laundering and terrorist financing. The new regulations will apply to banks, insurance companies, and a number of professional groups (e.g., financial services providers, lawyers, notaries public, tax advisors, and other business operators). The directive calls for improved integrity and transparency to help prevent financial crime and improve information exchange between the public and private sectors. According to the draft legislation, suitable control structures must ensure that proper, accurate and current information is available about the contracting party, to ensure transparency. The EU requirement also expands reporting requirements to encompass transactions that support the financing of terrorism. The EU regulation on wire transfers (EC 1781/2006) entered into force on January 1, 2007.

As of June 15, 2007, travelers entering Germany from a nonEU country or traveling to a nonEU country with 10,000 euros (approximately U.S. \$14,500) or more in cash must declare their cash in writing. The definition of "cash" includes currency, checks, traveler's checks, money orders, bills of exchange, promissory notes, shares, debentures, and due interest warrants (coupons). The written declaration must also include personal data, travel itinerary and means of transport as well as the total amount of money being transported, where the money originated from, what it is to be used for, who the owner of the money is and who is the payee. If authorities doubt the information given, or if there are other grounds to suspect money laundering or the funding of a terrorist organization, the cash will be placed under customs custody until the matter has been investigated. Penalties for nondeclaration or false declaration include a fine of up to one million euros (U.S. \$1.46 million). During the period between January and September 2007 the Federal Customs Criminal Office identified 998 cases of individual cross-border cash movements that required further clarification and review. In December 2007 the new Schengen countries were enveloped within EU borders, making it possible to travel across Europe from Estonia through Germany to Portugal without border controls.

Germany established a single, centralized, federal financial intelligence unit (FIU) within the Federal Office of Criminal Investigation (Bundeskriminalamt or BKA). Staffed with financial market supervision, customs, and legal experts, the FIU is responsible for analyzing cases, responding to reports of suspicious transactions, and developing and maintaining a central database of this information. Another unit under the BKA, the Federal Financial Crimes Investigation Task Force, houses twenty BKA officers and customs agents.

Information for 2007 was unavailable, but in 2006, obligated entities filed 10,051 suspicious transaction reports (STRs) pursuant to the Money Laundering Act. According to the German Financial Intelligence Unit's (FIU's) 2006 annual report, 80 percent of the STRs filed pursuant to the Money Laundering Act and other notifications of money laundering activity forwarded to the FIU in 2006 cited fraud, including "phishing" and the use of "financial agents", as a possible criminal offense from the perspective of the reporting party. The individuals recruited in phishing schemes may be liable for money laundering penalties as well as for the illegal provision of financial services. Document forgery and tax offenses were the next most frequently cited offenses.

In 2006, approximately fifty-seven percent of the persons cited in German STRs were German nationals. Of the forty-three percent of the STRs that referenced nonGerman nationals, suspects with Turkish citizenship comprised the greatest proportion followed by Russian, Chinese, Italian and Kazakh. The 2006 statistics on STRs concerning transfers of assets to and from foreign countries displayed a number of significant trends. Russia and the Ukraine were the top two destinations for asset transfers that generated STRs. The United States is the eighth most frequently listed destination for asset transfers that are cited by STRs. When entities file STRs on transfers of assets from foreign countries, the USA is the most frequently cited source nation.

As with other crimes, actual enforcement of money laundering laws under the German federal system takes place at the state (sub-federal) level. Each state has a joint customs/police/financial investigations unit (GFG), which works closely with the federal FIU. The State Attorney can order a freeze of accounts when warranted.

As an EU member, Germany complies with a recent EU regulation requiring accurate originator information on funds transfers for transfers into or out of the EU. However, this does not place Germany into compliance with FATF Special Recommendation Seven (SR VII) on Terrorist Financing, which governs wire transfers. SR VII requires such information on all cross-border transfers, including transfers between EU member countries.

Germany moved quickly after September 11, 2001, to identify and correct the weaknesses in its laws that had permitted terrorists to live and study in Germany. One reform package closed loopholes that had permitted members of foreign terrorist organizations to engage in fundraising in Germany (e.g., through charitable organizations), which extremists had exploited to advocate violence. Subsequently, Germany increased its law enforcement efforts to prevent misuse of charitable entities. Germany has used its *Vereingeseetz*, or Law on Associations, to take administrative action to ban extremist associations that "threaten the democratic constitutional order."

A second reform package enhances the capabilities of federal law enforcement agencies and improves the ability of intelligence and law enforcement authorities to coordinate efforts and to share information on suspected terrorists. The law also provides Germany's internal intelligence service with access to information from banks and financial institutions, postal service providers, airlines, and telecommunication and Internet service providers. Another proposed counterterrorism reform, will further streamline and simplify security agencies' access to German financial, travel, and telephone records. In 2002, the FRG also added terrorism and terrorist financing to its list of predicate offenses for money laundering, as defined by Section 261 of the Federal Criminal Code. The Criminal Code allows prosecution of members in terrorist organizations based outside Germany.

An amendment to the Banking Act institutes a broad legal basis for BaFIN to order frozen assets of EU residents suspected as terrorists. Authorities primarily concentrate on financial assets. BaFIN's system allows immediate identification of financial assets that can be potentially frozen, and German law enforcement authorities can freeze accounts for up to nine months. However, unless the assets belong to an individual or entity designated by the UNSCR 1267 Sanctions Committee, the FRG cannot seize money until authorities prove in court that the funds were derived from criminal activity or intended for terrorist activity.

Germany participates in United Nations and EU processes to monitor and freeze the assets of terrorists. The names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanctions Committee's consolidated list and those designated by EU or German authorities are regularly disseminated to German financial institutions. A court can order the freezing of nonfinancial assets. Germany and several other EU member states have taken the view that the EU Council Common Position requires, at a minimum, a criminal investigation to establish a sufficient legal basis for freezes under the EU Clearinghouse process. Proceeds from asset seizures and forfeitures go into the federal government treasury.

Since 1998, the FRG has licensed and supervised money transmitters, shut down thousands of unlicensed money remitters, and issued AML guidelines to the industry. German law considers the activities of alternative remittance systems such as hawala to be banking activities. Accordingly, German authorities require bank licenses for money transfer services, thus allowing authorities to prosecute unlicensed operations and maintain close surveillance over authorized transfer agents.

German law enforcement authorities cooperate closely at the EU level, such as through Europol. Germany has mutual legal assistance treaties (MLATs) with numerous countries. Germany exchanges law enforcement information with the United States through bilateral law enforcement agreements and informal mechanisms. United States and German authorities have conducted joint investigations. The U.S. and Germany signed a Mutual Legal Assistance Treaty in Criminal Matters on October 14, 2003. On July 27, 2006, the U.S. Senate ratified the MLAT and the German legislative bodies approved the implementing legislation in July and September 2007. Germany published the implementing legislation in the Federal Gazette on November 2, 2007, and the MLAT will come into effect once the parties formally exchange the instruments of ratification. Additionally, the U.S. and Germany signed bilateral instruments to implement the U.S.-EU Extradition and Mutual Legal Assistance Agreements on April 18, 2006. These instruments, as well as the underlying U.S.-EU Agreements, have not yet been ratified. German authorities cooperate with U.S. authorities to trace and seize assets to the full extent allowed under German laws. German law does not currently permit the sharing of forfeited assets with other countries.

Germany is a member of the FATF, the EU and the Council of Europe. The FIU is a member of the Egmont Group. Germany is party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Germany has signed, but not yet ratified, the UN Convention against Corruption.

The Government of Germany's AML laws and its ratification of international instruments underline Germany's continued efforts to combat money laundering and terrorist finance. Germany should amend its wire transfer legislation to ensure that origination information applies to all cross-border transfers, including those within the EU. It should also amend legislation to waive the asset freezing restrictions in the EU Clearinghouse for financial crime and terrorist financing, so that the freezing process does not require a criminal investigation as well as amend its legislation to allow asset sharing with other countries. Germany should ratify the UN Convention against Corruption.

Ghana

Ghana is not a regional financial center, but due to continuing turmoil in the region, Ghana's financial sector is likely to become more important regionally as it develops. Most of the money laundering found in Ghana involves narcotics and public corruption. Ghana is a significant transshipment point for cocaine and heroin. Police suspect that criminals use nonbank financial institutions, such as foreign exchange bureaus, to launder the proceeds of narcotics trafficking. Criminals can also launder their illicit proceeds through investment in banking, insurance, real estate, automotive import, and general import businesses. Reportedly, donations to religious institutions have been used as a vehicle to launder money. The number of "advance fee" or 419 fraud letters, known as Sakawa in Ghana, that

originate from Ghana continues to increase, as do other related financial crimes, such as use of stolen credit and ATM cards.

Informal activity accounts for about 45 percent of the total Ghanaian economy. Ghana's 2000 census found that 80 percent of employment was in the informal sector. Only a small percentage of the informal economy, however, relies on the banking sector. Because some traders smuggle goods to evade tax and import counterfeit goods, black market activity in smuggled goods is a concern. In most cases the smugglers bring the goods into the country in small quantities, and Ghanaian authorities have no indication that these smugglers have links to criminals who want to launder money gained through narcotics or corruption.

Ghana has designated four free trade zone areas, but the Tema Export Processing Zone is currently the only active free trade zone. Ghana also licenses factories outside the free zone area as free zone companies. Free zone companies must export at least 70 percent of their output. Most of the companies produce garment and processed foods. The Ghana Free Zone Board and the immigration and customs authorities monitor these companies. Immigration and customs officials do not suspect that trade-based money laundering (TBML) schemes are a major problem in the free trade zones. Although the Government of Ghana (GOG) has instituted identification requirements for companies, individuals, and their vehicles in the free zone, monitoring and due diligence procedures are lax.

The GOG has developed new laws to stimulate financial sector growth, including the revision of the banking law to strengthen the operational independence of the Central Bank (Bank of Ghana). The government is promoting efforts to model Ghana's financial system on that of the regional financial hub in Mauritius. In line with this, the GOG passed the Banking (Amendment) Act, 2007 Act 738, on June 18, 2007. The law establishes the basis for the provision of international financial services in Ghana and requires the Bank of Ghana to authorize offshore banks. Prior to this law, the Bank of Ghana licensed only reputable and internationally active banks. On September 7, 2007, Barclays Bank of Ghana Ltd., a subsidiary of Barclays Bank PLC, UK became the first to start operating as an offshore bank. The Bank of Ghana is in the process of drafting regulations for offshore banks.

Nearly six years after drafting began, the Parliament passed the Anti-Money Laundering (AML) Bill on November 2, 2007. The President signed it on January 22, 2008, and it was gazetted on January 25, 2008. The law covers obliged institutions and their reporting and disclosure requirements; the role of supervisory authorities; preventive measures; customer identification and record keeping requirements; and rules for suspicious transaction reporting. Ghana has bank secrecy laws, but allows the sharing of information with relevant law enforcement agencies. Law enforcement officials can compel disclosure of bank records for drug-related offenses. Bank officials have protection from liability when they cooperate with law enforcement investigations. The new AML law requires banks and individuals to report suspicious transactions.

The banking sector lacks a strong regulatory framework to prevent money laundering and report suspicious transactions, although entities recognize the importance of such a framework. The Bank of Ghana allows two types of foreign currency bank accounts: the foreign exchange (FE) account and the foreign currency (FC) account. The FE account is tailored to foreign currency sourced within Ghana while the FC account targets transfers from abroad. Bank of Ghana regulations instituted in December 2006 under the Foreign Exchange Act allow U.S. \$10,000 per year to be transferred from an FE account without documentation and approval from the Bank of Ghana. The regulations also allow import transactions of up to \$25,000 without initial documentation for FE accounts. There are no limits on the number of such transactions made on each account or on the number of such accounts that an individual can hold. The law does not permit foreign exchange bureaus to make outward transfers. Local banks strictly follow "know your customer" rules. Ghana has no effective system to obtain data on an individual's dealings with all the banks in Ghana.

Ghana has a cross-border currency reporting requirement. However, Ghanaian authorities have difficulty monitoring cross-border movement of currency.

The new AML bill calls for establishment of a Financial Intelligence Unit (FIU), overseen by the Minister of Finance. Ghana plans to fund the FIU through government grants and donations. The FIU will not investigate crime but will gather and analyze intelligence to help in identifying proceeds of unlawful activity and the perpetrators of the crimes. The FIU will have the authority to obtain information from other government regulatory authorities and from financial institutions. The GOG made no arrests, nor did it pursue any prosecutions related to money laundering or terrorist finance in 2007.

The Narcotic Drug Law of 1990 provides for the forfeiture of assets upon conviction of a drug trafficking offense. A February 2007 court order compelled authorities to release seized assets in a 1991 landmark narcotics trafficking case which resulted in a ten-year jail sentence of the convict, and return the assets to the owners. The ex-convict had appealed the seizure, arguing that the assets did not belong to him. The draft Proceeds of Crime Bill, pending since 2006, contains provisions dealing with pre-emptive measures, confiscation and pecuniary penalty orders, search and seizure, and restraining orders and realization of property. The draft Proceeds of Crime bill will merge with the existing Serious Fraud Office Law, 1993 (Act 466). The Serious Fraud Office, established by this law, investigates corruption and crimes that have the potential to cause economic loss to the state.

Ghana has not yet criminalized the financing of terrorism, as required by United Nations Security Council Resolution 1373. A draft Anti-Terrorism Bill, incorporating terrorist financing provisions, came before Parliament in 2005. The Bill is under examination by members of the Constitutional, Legal, and Parliamentary Affairs Committee and the Defense and Interior Committee. The draft bill addresses terrorist acts, support for terrorist offenses, specific entities associated with acts of terrorism, and search, seizure, and forfeiture of property relating to acts of terrorism. The Central Bank has circulated the list of individuals and entities on the UNSCR 1267 Sanctions Committee's consolidated list to local banks, but no Ghanaian entities have identified assets belonging to any of the designees.

Although current Ghanaian law does not allow for the sharing of seized narcotics assets with other governments, the Narcotic Drug Law of 1990 includes provisions for the sharing of information, documents, and records with other governments. It also provides for extradition between Ghana and foreign countries for drug-related offenses. The United States has not requested financial investigative assistance from Ghanaian authorities.

Ghana is a member of the Inter-Governmental Action Group Against Money Laundering and Terrorist Financing in West Africa (GIABA), a regional body modeled after the Financial Action Task Force (FATF). Ghana has bilateral agreements for the exchange of money laundering-related information with the United Kingdom, Germany, Brazil, and Italy. Ghana is a party to the twelve UN conventions on terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism. Ghana is a party to the 1988 UN Drug Convention, and the African Union Convention on Preventing and Combating Corruption. In June 2007, Ghana ratified the UN Convention against Corruption. Ghana has not signed the UN Convention against Transnational Organized Crime. Ghana has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision."

Although the Government of Ghana (GOG) became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002, it has not criminalized terrorist financing. It should do so. The GOG should move swiftly to implement the AML Bill, and should expand the list of predicate crimes to comply with international standards. The GOG should issue promulgating regulations, improve capacity among the agencies impacted, and establish its FIU. The GOG should make every effort to pass asset seizure and forfeiture legislation that comports with international standards as soon as possible. Once the laws are in place, Ghana should take the necessary steps to promote public awareness and understanding of financial crime, money laundering and financing of

terrorist activities. The GOG should reconsider establishing the offshore center altogether. Ghana should immediately release regulations and guidance for its new offshore entities, and draft legislation to ensure that offshore entities are treated identically to the onshore sector under the AML Bill. Additionally, the GOG should require that the true names of all offshore entities are held in a registry, accessible to law enforcement. The GOG should increase cooperation and information sharing with other governments. Ghana should also become a party to the UN Convention against Transnational Organized Crime.

Gibraltar

Gibraltar is an overseas territory of the United Kingdom. A November 2006 referendum resulted in constitutional reforms transferring powers exercised by the U.K. government to Gibraltar. Gibraltar is a significant international financial center with strong ties to London, the Channel Islands, Israel, Cyprus, and other financial centers. Located at the southern tip of Spain, near the north coast of Africa, Gibraltar is adjacent to known drug-trafficking and human smuggling routes. It is also a retail banking centre for northern European expatriates with property in southern Spain. All of these factors reportedly contribute to money laundering and terrorist financing vulnerabilities in Gibraltar.

Gibraltar was one of the first jurisdictions to introduce and implement money laundering legislation that covered all crimes. The Gibraltar Criminal Justice Ordinance to Combat Money Laundering, which related to all crimes, entered into effect in 1996. The Drug Offenses Ordinance (DOO) of 1995 and Criminal Justice Ordinance of 1995, amended in June 2007 as the Criminal Justice Act, criminalize money laundering related to all crimes. The laws mandate reporting of suspicious transactions by any obliged entity or individual therein. The DOO obliges banks, mutual savings companies, insurance companies, financial consultants, postal services, exchange bureaus, attorneys, accountants, financial regulatory agencies, unions, casinos, charities, lotteries, car dealerships, yacht brokers, company formation agents, dealers in gold bullion, and political parties.

Authorities issued comprehensive anti-money laundering (AML) Guidance Notes, which have the force of law, to clarify the obligations of Gibraltar's financial service providers. Gibraltar issued its most recent Guidance Notes in December 2007 with amendments based on the Criminal Justice (Amendment) Act 2007 and Terrorist (Amendment) Act 2007. The 2007 Guidance Notes apply to banks and building societies, the Gibraltar Saving Bank, investment business and controlled activities, life insurance companies, currency exchangers/bureaux de change, and money transmission/remittance offices. In transposing the EU's Third Money Laundering Directive to include nonfinancial sectors, Gibraltar extended the Criminal Justice Act.

Gibraltar established the Financial Services Commission (FSC), the unified regulatory and supervisory authority for financial services, under the FSC Ordinance (FSCO) 1989. Required by statute to match the supervisory standards of the United Kingdom, the FSC is the supervisory body for banks and building societies, investment businesses, insurance companies, and controlled activities, which include investment services, company management, professional trusteeship, insurance management and insurance intermediation. The main legal instruments governing the regulation and supervision of the financial system, in addition to the FSCO, are: the Banking Ordinance (1992) that provides powers to license and supervise banking and other deposit-taking business in Gibraltar; the Insurance Ordinance (1987) that provides powers to regulate and restrict the conduct of the business of insurance; and the Financial Services (Collective Investment Schemes) Ordinance that provide for the licensing and supervision of investment business.

Legislation requires that all businesses establish the beneficial owner of any companies or assets before undertaking a relationship or incorporating any company or asset. Onshore and offshore banks are subject to the same legal and supervisory requirements. Institutions must retain financial records for at least five years from the date of completion of the business. If the obligated institution has

submitted a suspicious transaction report (STR) to the Gibraltar financial intelligence unit (FIU) or when it knows that a client or transaction is under investigation, it is required to maintain any relevant record even if the five year interval has expired. If a law enforcement agency investigating a money laundering case cannot link the funds passing through the financial system with the original criminal money, then the funds cannot be confiscated.

The Financial Services Commission Act 2007 (FSCA) became effective in May 2007. This act repeals and replaces the Financial Services Commission Act of 1989. With this legislation, the FSC modernized and restructured itself. One of the most significant changes arising from the FSCA is in respect to the appointment of members of the Commission, who will be selected by the minister with responsibility for financial services (presently the Chief Minister) from a short list of three suitable persons provided to him by existing members. The FSC has also received expanded statutory functions. The FSC now holds formal licensing, supervisory, and regulatory powers over all firms authorized under the Supervisory Acts. The FSC authority also ensures compliance with legislation, rules and guidance notes in general as well as those specific to combating financial crime. The FSC is now able to issue Rules and Guidance, which enables the FSC to draft practical guidance for compliance with legislative measures, and regulatory expectations to supplement legislative provisions. As a safeguard against inappropriate or overregulation, the rules and guidance undergo a public consultation process and are subject to final veto of the Minister.

The Government of Gibraltar (GOG) permits Internet gaming that is subject to a licensing regime. Gibraltar has guidelines for correspondent banking, politically exposed persons (PEPs), bearer securities, and “know your customer” (KYC) procedures. In 2006, Gibraltar underwent a mutual evaluation by the International Monetary Fund (IMF). The IMF rated Gibraltar “largely compliant” or “better” with 32 of the Financial Action Task Force’s (FATF’s) 40 Recommendations and nine Special Recommendations.

In 1996, Gibraltar established the Gibraltar Coordinating Center for Criminal Intelligence and Drugs (GCID) to receive, analyze, and disseminate financial information and disclosures filed by obliged institutions. The GCID serves as Gibraltar’s FIU (GFIU) and is a sub-unit of the Gibraltar Criminal Intelligence Department. The GCID consists mainly of police and customs officers but is independent of law enforcement. The GFIU has responded to over 40 international requests for information and has initiated ten requests to counterpart FIUs. The GFIU receives approximately 100 STRs per year.

Gibraltar’s 2001 Terrorism (United Nations Measures) (Overseas Territories) Order criminalizes the financing of terrorism. The Order requires banks to report any knowledge that a present, past or potential client or customer is a terrorist, or receives funds in relation to terrorism, or makes funds available for terrorism. Gibraltar also addresses terrorist financing through the Terrorism Ordinance (2005).

Application of the 1988 U.S.-UK Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking was extended to Gibraltar in 1992. The DOO of 1995 provides for mutual legal assistance with foreign jurisdictions on matters related to narcotics trafficking and related proceeds. Gibraltar has passed legislation to update mutual legal assistance arrangements with its EU and Council of Europe partners. Gibraltar is a member of the Offshore Group of Banking Supervisors (OGBS) and the International Organization of Securities Commissions (IOSC). The GFIU is a member of the Egmont Group. The GOG has implemented the 1988 UN Drug Convention.

The Government of Gibraltar should continue its efforts to implement a comprehensive anti-money laundering and counter-terrorist financing (AML/CTF) regime. The criminal laws on money laundering should be consolidated, and powers presently available only in drug-related money laundering cases should be extended to money laundering cases involving the proceeds of other crimes. The GOG should introduce legislative provisions to its asset seizure and confiscation regime

allowing authorities to confiscate assets, including cash, even without a link to the original criminal proceeds. Gibraltar needs to conduct risk assessment of those designated nonfinancial businesses and professions that are unsupervised and determine and extend the necessary authority to conduct AML/CTF compliance examinations of these entities.

Greece

Greece is becoming a regional financial center in the rapidly developing Balkans as well as a bridge between Europe and the Middle East. Anecdotal evidence of illicit transactions suggests an increase in financial crimes in the past two years. Greek law enforcement proceedings indicate that Greece is vulnerable to narcotics trafficking, trafficking in persons and illegal immigration, prostitution, cigarette, and other forms of smuggling, large scale tax evasion, serious fraud or theft, and illicit gambling activities. The widespread use of cash facilitates a gray economy and tax evasion. Due to the gray economy, it is difficult to determine the amount of smuggled goods in the country. Crimes are often carried out by criminal organizations from Southeastern Europe and the Balkans.

U.S. law enforcement agencies believe that criminally derived proceeds are not typically laundered through the Greek banking system. Instead, they are most commonly invested in real estate, the lottery, and a growing stock market. U.S. law enforcement agencies also believe Greece's geographic location has led to a moderate increase in cross-border movements of illicit currency and monetary instruments due to the increasing interconnection of financial services companies operating in Southeastern Europe and the Balkans. Reportedly, currency transactions involving international narcotics-trafficking proceeds do not appear to include significant amounts of U.S. currency.

The June 2007 Financial Action Task Force (FATF) mutual evaluation report (MER) of Greece found its legal requirements in place to combat money laundering and terrorist financing generally inadequate to meet the FATF standards. The report articulated concerns about the overall effectiveness of the AML/CTF system, including inadequate customer identification preventative systems, lack of adequate legal systems to prevent money laundering and terrorist financing, and a lack of adequate preventive measures and regulatory oversight. Of the FATF 40 Recommendations and Nine Special Recommendations on Terrorist Financing, Greece received 12 ratings of "largely compliant" or better and 13 ratings of "noncompliant." Of the 5 core FATF recommendations (Recommendations 1, 5, 10, and 13, SR II and IV), Greece's Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) regime was only deemed "partially compliant".

The Government of Greece has criminalized money laundering through a series of laws that have expanded the list of predicate offenses for money laundering that now includes terrorist financing, trafficking in persons, electronic fraud, and stock market manipulation. However evidence indicates that the ML provisions have not been effectively implemented. The laws also empower supervisory authorities to block transactions when money laundering is suspected and authorizes the financial intelligence unit (FIU) director to temporarily freeze assets without a court order. With its Act 25779/2006, the Bank of Greece has applied the main provisions of the Third European Union (EU) Money Laundering Directive to all financial institutions. The Greek government anticipates it will take steps to formally transpose the Directive into national law in 2008.

The Bank of Greece (BOG), through its Banking Supervision Department and the Ministry of National Economy and Finance, through its Capital Market Commission, supervise and monitor credit and financial institutions. Both the BOG and the Hellenic Capital Markets Commission (HCMC) have extensive supervisory programs. Each entity has internal departments focused on AML/CTF staffed with auditors and examiners. Supervision includes the issuance of guidelines and circulars, and on-site audits with a component assessing compliance with AML legislation. The Central Bank conducts on-site examinations for banks located in Greece as well as of Greek banks located in the Balkans. The HCMC conducts on-site examinations on a routine basis for its supervised entities and off-cycle

Money Laundering and Financial Crimes

examinations of supervised entities when HCMC internal surveillance activities uncover possible noncompliance with regulations. In addition to their supervisory programs, both the BOG and HCMC conduct continuing education seminars for stakeholders inside and outside of the financial industry, to further heighten awareness of AML/CTF. While the BOG and HCMC have been granted sufficient powers and authorities to monitor financial institutions for AML/CTF requirements, according to the MER, these organizations may not be able to effectively carry out their supervisory functions due to a lack of resources.

Supervised institutions must send to their competent authority a description of the internal control and communications procedures they have implemented to prevent money laundering. In addition, banks must undergo internal audits. Bureaux de Change must send the BOG a monthly report on their daily purchases and sales of foreign currency. Infrequent audits of such companies also occur. However, there is reportedly weak implementation of regulatory requirements documenting the flow of large sums of cash through financial and other institutions.

Law 3148 incorporates EU directives regarding the operation of credit institutions and the operation and supervision of electronic transfers. Under this legislation, the BOG has direct scrutiny and control over transactions by credit institutions and entities involved in providing services for funds transfers. The BOG issues operating licenses after assessing the institutions, their management, and their capacity to ensure the transparency of transactions. The Ministry of Development, through its Directorate of Insurance Companies, supervises the insurance sector, but supervisory authority will soon shift to the Hellenic Private Insurance Supervisory Committee. The Directorate of Insurance Companies has not established a regulatory authority.

Under Decree 2181/93, banks in Greece must demand customer identification information when a customer opens an account or conducts transactions exceeding 15,000 euros (approximately U.S. \$22,000). If there is suspicion of illegal activities, banks may take measures to gather more information on the identification of the person involved in the transaction, but, reportedly, do not normally do so. The BOG has taken steps to change this. Newly enacted legislation now requires banks to obtain specific documents from both natural and legal persons. Furthermore, credit institutions are now required to obtain identification documents in money changing transactions exceeding 500 euros (U.S. \$735). The law requires that banks and financial institutions maintain adequate records and supporting documents for at least five years after ending a relationship with a customer, or, in the case of occasional transactions, for five years after the date of the transaction. According to the MER, customer due diligence (CDD) and other preventative measures lack both sufficient requirements on collecting beneficial ownership information and adequate measures relating to ongoing CDD requirements on existing clients and account holders.

Current AML laws do not adequately prevent anonymous accounts or accounts in fictitious names. Greek law does not prohibit financial institutions from engaging in business with foreign financial institutions that allow their accounts to be used by shell companies.

Both banks and nonbank financial institutions must report suspicious transactions, though in practice, the latter rarely do so. The law requires every financial institution to appoint a compliance officer to whom all other branches or other officers must report suspicious transactions. Reporting obligations also apply to government employees involved in auditing, including employees of the BOG, the Ministry of Economy and Finance, and the Capital Markets Commission. Those who report individuals must furnish all relevant information to the prosecuting authorities. In 2007, the FIU formalized the standard information required on the suspicious transaction reports (STRs), so that the information provided on the form is consistent. Safe harbor provisions in Greek law protect individuals reporting violations of AML laws and statutes.

Greece has adopted banker negligence laws under which individual bankers face liability if their institutions launder money. Authorities levy “fines” on banks and credit institutions if they breach

their obligations to report instances of money laundering, and bank officers can receive fines and a prison term of up to two years. In 2007, the BOG “fined” approximately 14 institutions for failure to supervise general compliance regulations. The fines totaled approximately 20 million euros (approximately U.S. \$30 million). The credit institution deposits the “fines” with the Central Bank in a separate, interest free account. After a designated period of time, the Central Bank returns the money to the credit institution. In 2007, the HCMC “fined” two supervised entities for failure to supervise in relation to AML/CTF regulations. The “fines” ranged from 5,000 to 10,000 euros (U.S. \$7,350-\$14,700). Some believe this sanction is not sufficiently prohibitive.

Law 2331/1995 established the Competent Committee (CC), which functions as Greece’s FIU. Law 3424 makes the CC a statutorily independent authority with access to public and private files and removes tax confidentiality restrictions. The law also broadens the CC’s authority with respect to evaluating information it receives from various organizations. The CC has, on paper, broad authority; however the FATF MER raised concerns about the CC, including its current structure, insufficient staff and technical resources to properly perform its tasks and functions and inadequate security measures to effectively protect information. A senior retired judge chairs the CC, which includes eleven senior representatives from the BOG, various government ministries and law enforcement agencies, the Hellenic Bankers Association, and the securities commission. The CC employs few or no financial analysts or experienced specialized AML/CTF personnel, and is significantly understaffed.

The CC has responsibility for receiving and processing all STRs, of which it receives approximately 1,000 per year. Although the CC recently established a database to track STR submissions, it still lacks other elements of a technology-savvy modern organization. STRs are hand delivered to the CC, where, upon receipt, the committee (comprised of only senior officials) reviews the STRs to determine whether further investigation is necessary. If the committee seeks more information from the reporting institution, the CC mails its questions to the institution. When it receives the reply, the committee reviews the file again to determine whether the report warrants further investigation. When the CC considers an STR to warrant further investigation, it forwards the case to the Special Control Service (YPPEE), which functions as the CC’s investigative arm.

The YPEE is under the direct supervision of the Ministry of Economy and Finance and has formal investigative authority over cases that, broadly defined, involve smuggling and high-worth tax evasion. The CC is responsible for preparing money laundering cases on behalf of the Public Prosecutor’s Office and the YPEE has its own in-house prosecutor to facilitate confidentiality and speed of action. The director of the FIU can temporarily freeze funds.

Although the CC has the authority to impose heavy penalties on those who fail to report suspicious transactions, it has not done so. Reportedly, staff limitations have hampered effective communication with Greece’s broader financial community, as well as with its international counterparts. The lack of adequate personal and fiscal resources and political support for its mission limits its effectiveness.

Authorities do not frequently prosecute money laundering cases independent of a predicate crime, and according to the MER, limited data indicates a low rate of convictions on ML prosecutions. . There are no prosecutors specifically assigned to prosecute financial crimes and all prosecutors carry a very large caseload. Furthermore, the Greek judicial system has only one court handling all judicial activity related to money laundering and terrorist financing. Greek authorities do not have an effective information technology (IT) system in place to track money laundering prosecution statistics. Despite requests by the CC and Greek Bar Association to do so, the Ministry of Justice has yet to compile statistics related to arrests or prosecutions for money laundering or terrorist financing offenses.

The Government of Greece does not provide guidance to institutions on freezing assets without delay and does not monitor compliance with requests. Furthermore, there are no sanctions for failure to follow freezing requests. The current process for notifying ministries and the financial sector to freeze or confiscate funds is lengthy. Therefore, these entities are unable to comply with requests to freeze

assets without delay. Greek law allows for the seizure of assets upon conviction for a money laundering offense with a jail term of three years or greater. The director of the CC can temporarily freeze assets, but must prepare a report and forward it to an investigating magistrate and prosecutor, who conduct further investigation and who, upon conclusion of the investigation, can issue a freezing order, pending the outcome of the criminal case. The YPEE has established a mechanism for identifying, tracing, freezing, seizing, and forfeiting assets of narcotics-related and other serious crimes, the proceeds of which are turned over to the government. YPEE investigators have authorization to immediately seize property pending court review and seize property purchased with proceeds of narcotics trafficking or used to facilitate narcotics trafficking. However, official forfeiture requires a court order. If the basis for the forfeiture is facilitation proceeds, the Government of Greece need not prove that the property was purchased with narcotics-related proceeds. It must only demonstrate that it was used in furtherance of narcotics trafficking. Even legitimate businesses can be seized if they have laundered narcotics money.

Greek authorities maintain that Greece is not an offshore financial center. However, Greek law 89/1967 provides for the establishment of offshore entities of any legal form which may be registered in Greece but engage exclusively in commercial activities outside of Greece—a typical identifying restriction of offshore centers. “Law 89” companies reportedly operate in the shipping industry and are known for their complex corporate and ownership structures which are frequently designed to hide the identity of the true beneficial owners of the companies.

Offshore entities must provide a bank letter of guarantee for U.S. \$50,000 to the Ministry of Economy and Finance. If it is a shipping company, it must cover its annual operating expenses in Greece. It must keep a receipts and expenses book, though it has no obligation to publish any financial statements. These firms fall under the authority of nonGreek jurisdictions and often operate through a large number of intermediaries. As such, these entities can serve as a catalyst for money laundering. Although Greek law allows banking authorities to check these companies’ transactions, other Greek jurisdictions must work with the banking authorities for audits to be effective. There is no separate regulatory authority for the offshore sector and there is no longer a tax exemption for offshore companies.

Greek law does not provide for nominee directors or trustees in Greek companies. Although the government has abolished bearer shares for banks and a limited number of other companies, most companies may still issue bearer shares. The information available in the Companies Registries maintained by several authorities relates solely to the Board of Directors at the time of the incorporation of the company and does not log changes of directors, or the true beneficial owners of the company. Rather, regional registries keep this information in a paper format.

Authorities have recently targeted the gaming industry to restrain money launderers from using Greece’s nine casinos to launder illicit funds, however there is little regulatory oversight of the gaming industry. Greece has three free trade zones, located at the ports of Piraeus, Thessalonica, and Heraklion, where foreign goods may be brought in without payment of customs duties or other taxes if they are subsequently transshipped or re-exported. There is no specific information regarding whether these zones are being used in trade-based money laundering (TBML) or in the financing of terrorism

The BOG maintains that alternative remittance systems do not exist in Greece and has no plans to introduce initiatives for their regulation. Foundations in Greece are self-governing, nonmembership organizations with an endowment that serves public or private purposes and which receive legal capacity by state approval. Types of foundations include private law foundations, public benefit foundations, public foundations, and nonautonomous foundations. Nonprofit organizations fall within the purview of YPEE. The Greek government does not view charitable organizations as vulnerable to terrorist financing or money laundering and does not actively monitor such entities for these crimes.

Laws criminalizing terrorism, organized crime, money laundering and corruption have been in effect since July 2002. In 2004, Law 3251 was enacted criminalizing the financing of, the joining, or the forming of a terrorist group with a penalty of up to ten years imprisonment. If a private legal entity is implicated in terrorist financing, it faces fines of between 20,000 and 3 million euros (approximately U.S. \$44,000 and U.S. \$4.5 million), closure for a period of two months to two years, and ineligibility for state subsidies. However, some have described the law as poorly drafted. The law is not comprehensive as it is not illegal in Greece to fund an already established terrorist group and it is only considered a terrorist financing crime if a person funds a specific attack executed by three or more people. As a consequence, the financing of an individual terrorist act conducted by an individual terrorist or the financing of an individual terrorist is not an offense.

The BOG has circulated to all financial institutions under its supervisory jurisdiction the list of individuals and entities on the United Nations Security Council Resolution (UNSCR) 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Laden, the Al-Qaida organization, or the Taliban, as well as the EU's list of designees. The BOG now includes Office of Foreign Asset Control lists for circulation to its supervised entities. The Greek government does not routinely circulate lists disseminated by the U.S. government, but it does circulate EU lists. In most instances, there must be an active investigation by Greek authorities before the Government of Greece can seize assets, thus hindering its ability to freeze assets without delay. The government has not found any accounts belonging to anyone on the circulated lists.

Greece is a member of the FATF. Its FIU is a member of the Egmont Group. The government is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Greece is a signatory to the UN Convention against Transnational Organized Crime and to the UN Convention against Corruption, but has not yet ratified them. Greece exchanges information on money laundering through its mutual legal assistance treaty (MLAT) with the United States, which entered into force November 20, 2001. The Bilateral Police Cooperation Protocol provides a mechanism for exchanging records with U.S. authorities in connection with investigations and proceedings related to narcotics trafficking, terrorism, and terrorist financing. Cooperation between the U.S. Drug Enforcement Administration and YPEE has been extensive. Greece has signed bilateral police cooperation agreements with twenty countries, including the United States. It also has a trilateral police cooperation agreement with Bulgaria and Romania, and a bilateral agreement with Ukraine to combat terrorism, drug trafficking, organized crime, and other criminal activities. Despite the existing mechanisms for information exchange, the FATF report highlighted a lack of cooperation between Greek national and international authorities.

To meet its stated goal of effectively addressing money laundering, the Greek government should implement all recommendations of the June 2007 FATF mutual evaluation report on Greece. Greece should accelerate its efforts to realize new laws and regulations aimed at upgrading its FIU. This includes fully staffing with experienced analysts and improving its IT standards and capabilities so that analysts can effectively use its database. These IT upgrades should allow Greek authorities to implement a system to track statistics on money laundering prosecutions and convictions, as well as asset freezes and forfeitures. The Greek government should improve its asset freezing capabilities and develop a clear and effective system for identifying and freezing terrorist assets within its jurisdiction. The government should also publicize its system for appealing assets frozen in accordance with its UN obligations.

Greece should ensure uniform enforcement of its cross-border currency reporting requirements and take steps to deter the smuggling of currency across its borders. The government should abolish company-issued bearer shares, so that all bearer shares are legally prohibited. It should also ensure that its "Law 89" offshore companies and companies operating within its free trade zones are subject to the same AML requirements and gatekeeper and due diligence provisions, including know your customer rules and the identification of the beneficial owner, as in other sectors. The GOG should dedicate

additional resources to the investigation and prosecution of ML cases, as well as increase specialization and training on AML/CTF for law enforcement and judicial authorities. The GOG should also amend the existing legislative and regulatory framework to ensure that appropriate CDD requirements are implemented. Finally, it should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Grenada

Grenada is not a regional financial center. As a transit location, money laundering in Grenada is primarily related to smuggling and drug trafficking. Illicit proceeds are typically laundered through a wide variety of businesses, as well as through the purchase of real estate, boats, jewelry, and cars.

As of December 2007, Grenada's domestic financial sector is comprised of six commercial banks, 26 registered domestic insurance companies, two credit unions, and five money remitters. Grenada has one trust company and 1,580 international business companies (IBCs), a significant, if unexplained, decrease from the reported 6,000 IBCs in 2006. There are no casinos or Internet gaming sites operating in Grenada. There are no free trade zones in Grenada, although the Government of Grenada (GOG) has indicated that it may create one in the future. The GOG has repealed its economic citizenship legislation.

Bearer shares are not permitted for offshore banks. Registered agents are required by law to verify the identity of the beneficial owners of all shares. In addition, the International Companies Act requires registered agents to maintain records of the names and addresses of directors and beneficial owners of all shares. There is an U.S. \$11,500 penalty and possible revocation of the registered agent's license for failure to maintain records. Grenada has not enacted laws preventing disclosure of client and ownership information by domestic and offshore services companies to bank supervisors and law enforcement authorities.

The Grenada Authority for the Regulation of Financial Institutions (GARFIN) became operational in early 2007. The GARFIN was created to consolidate supervision of all nonbank financial institutions, and effectively replace the Grenada International Financial Services Authority (GIFSA). Institutions supervised by GARFIN include insurance companies, credit unions, offshore financial services, the building and loan society, money service businesses, and other such services. The Eastern Caribbean Central Bank (ECCB) retains supervision responsibility for Grenada's commercial banks.

The Money Laundering Prevention Act (MLPA), enacted in 1999, and the Proceeds of Crime Act (POCA) No. 3 of 2003 criminalize money laundering in Grenada. Under the MLPA, the laundering of the proceeds of narcotics trafficking and all serious crimes is an offense. Under the POCA, the predicate offenses for money laundering extend to all criminal conduct, which includes illicit drug trafficking, trafficking of firearms, kidnapping, extortion, corruption, terrorism and its financing, and fraud. According to the POCA, a conviction on a predicate offense is not required to prove that certain goods are the proceeds of crime, and subsequently convict a person for laundering those proceeds. The POCA establishes a penalty three to ten years in prison and fines of \$18,500 or more. This legislation applies to banks and nonbank financial institutions, as well as the offshore sector.

Established under the MLPA, the Supervisory Authority supervises the compliance of banks and nonbank financial institutions (including money remitters, stock exchange, insurance, casinos, precious gem dealers, real estate, lawyers, notaries, and accountants) with money laundering and terrorist financing laws and regulations. These institutions are required to know, record, and report the identity of customers engaging in significant transactions. This applies to large currency transactions over the threshold of \$3,700. Records must be maintained for seven years. In addition, a reporting entity must monitor all complex, unusual or large business transactions, or unusual patterns of transactions, whether completed or not. Once a transaction is determined to be suspicious or

potentially indicative of money laundering, the reporting entity must forward a suspicious transaction report (STR) to the Supervisory Authority within 14 days. Reporting individuals are protected by law with respect to their cooperation with law enforcement entities.

The Supervisory Authority issued its Anti-Money Laundering Guidelines in 2001. The guidelines direct financial institutions to maintain records, train staff, identify suspicious transactions, and designate reporting officers. The guidelines also provide examples to help institutions recognize and report suspicious transactions. The Supervisory Authority is authorized to conduct anti-money laundering inspections and investigations. The Supervisory Authority can also conduct investigations and inquiries on behalf of foreign counterparts and provide corresponding information. Financial institutions may be fined for not granting access to Supervisory Authority personnel.

In June 2001, the GOG established a police-style financial intelligence unit (FIU). The FIU is charged with receiving and analyzing suspicious transaction reports (STRs) from the Supervisory Authority, and with investigating alleged money laundering offenses. The FIU has access to the records and databases of all government entities and financial institutions and is empowered to request any documents it considers necessary to its investigations. From January to November 2007, the FIU received 25 STRs and investigations commenced for all STRs received. The FIU has the authority to exchange information with its foreign counterparts without a memorandum of understanding (MOU).

Two foreign nationals were arrested by GOG authorities for money laundering in October 2007. These individuals came to Grenada with a large number of fraudulent credit cards and over a short period of time, withdrew in excess of \$40,000 from automatic teller machines (ATMs) from several local banks. Half of the amount stolen was sent out to a number of different destinations via a legitimate money remittance company, which agreed to freeze the transaction. Local authorities are working with the company to repatriate those funds. The two perpetrators were arrested and charged with money laundering and fraud by false pretense. The case is currently ongoing.

The FIU and the Director of Public Prosecution's Office are responsible for tracing, seizing and freezing assets. Under current law, all assets can be seized, including legitimate businesses if they are used in the commission of a crime. The banking community cooperates with law enforcement efforts to trace funds and seize or freeze bank accounts. The time period for restraint of property is determined by the High Court. Presently, only criminal forfeiture is allowed by law. Proceeds from asset seizures and forfeitures can either be placed in the consolidated fund or the confiscated asset fund, which is supervised by the Supervisory Authority or the Cabinet for use in the development of law enforcement. The approximate dollar amount seized in the past year was U.S. \$62,000, with approximately U.S. \$22,000 forfeited. The Civil Forfeiture Bill, Cash Forfeiture Act, and Confiscation of the Proceeds of Crime Bill were introduced in 2006 and remain under discussion.

Grenada is not engaged in bilateral or multilateral negotiations with other governments to enhance asset tracing, freezing, and seizure. However, the GOG works actively with other governments to ensure tracing, freezing, and seizures take place, if and when necessary, regardless of the status of existing agreements.

The GOG regulates the cross-border movement of currency. However, there is no threshold requirement for currency reporting. Law enforcement and Customs officers have the powers to seize and detain cash that is imported or exported from Grenada. Cash seizure reports are shared between government agencies, particularly between Customs and the FIU.

The GOG criminalized terrorist financing through the Terrorism Act No. 5 2003. Grenada has the authority to identify, freeze, seize, and/or forfeit terrorist finance-related assets under the POCA and the Terrorism Act. The GOG circulates to the appropriate institutions the lists of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. There has

been no known identified evidence of terrorist financing in Grenada. It is suspected that alternative remittance systems are used in Grenada, though none have been positively identified.

In 2003, the GOG passed the Exchange of Information Act No. 2, which strengthens Grenada's ability to share information with foreign regulators. Grenada has a Mutual Legal Assistance Treaty (MLAT), Tax Information Exchange Agreement (TIEA) and an Extradition Treaty with the United States. The GOG cooperates fully with MLAT requests and responds rapidly to U.S. Government requests for information involving money laundering cases.

Grenada is a member of the Caribbean Financial Action Task Force (CFATF), and is expected to undergo a mutual evaluation in 2008. The GOG is also a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Grenada's FIU is a member of the Egmont Group. Grenada is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the Inter-American Convention against Terrorism. The GOG has not yet signed the UN Convention against Corruption.

Although the Government of Grenada has strengthened the regulation and oversight of its financial sector, it must remain alert to potential abuses and must steadfastly implement the laws and regulations it has adopted. The GOG should also move forward in adopting civil forfeiture legislation, and establish mechanisms to identify and regulate alternative remittance systems. Law enforcement and customs authorities should initiate money laundering investigations based on regional smuggling. Grenada should also become a party to the UN Convention against Corruption.

Guatemala

Guatemala is a major transit country for illegal narcotics from Colombia and precursor chemicals from Europe. Those factors, combined with historically weak law enforcement and judicial regimes, corruption, and increasing organized crime activity, contribute to a favorable climate for significant money laundering in Guatemala. According to law enforcement agencies, narcotics trafficking and corruption are the primary sources of money laundered in Guatemala; however, the laundering of proceeds from other illicit activities, such as human trafficking, contraband, kidnapping, tax evasion, and vehicle theft, is substantial. Officials of the Government of Guatemala (GOG) believe that the sources of the criminal proceeds laundered in Guatemala are derived from both domestic sources (primarily corruption cases) and foreign criminal activities. GOG officials also believe that cash couriers, offshore accounts, and wire transfers are used to launder funds, which are subsequently invested in real estate, capital goods, large commercial projects, and shell companies, or are otherwise transferred through the financial system.

Guatemala is not considered a regional financial center, but it is an offshore center. Exchange controls have been lifted and dollar accounts are common, but some larger banks conduct significant business through their offshore subsidiaries. The Guatemalan financial services industry is comprised of 22 commercial banks; ten offshore banks, all of which are affiliated, as required by law, with a domestic financial group (including affiliated credit card, insurance, finance, commercial banking, leasing, and related companies); two licensed money exchangers; 27 money remitters, including wire remitters and remittance-targeting courier services; 17 insurance companies; 17 financial societies; 15 bonded warehouses; 325 savings and loan cooperatives; eight credit card issuers; nine leasing entities; 11 financial guarantors; and one check-clearing entity run by the Central Bank. There are also hundreds of unlicensed money exchangers that exist informally.

The Superintendence of Banks (SIB), which is directed by the Monetary Board, has oversight and inspection authority over the Central Bank (Bank of Guatemala), as well as over banks, credit institutions, financial enterprises, securities entities, insurance companies, currency exchange houses

and other institutions as may be designated by the Bank of Guatemala Act. Guatemala's relatively small free trade zones target regional maquila (assembly line industry) and logistic center operations, and are not considered by GOG officials to be a major money laundering concern, although some proceeds from tax-related contraband may be laundered through them.

The offshore financial sector initially offered a way to circumvent currency controls and other costly financial regulations. However, financial sector liberalization has largely removed incentives for legitimate businesses to conduct offshore operations. All offshore institutions are subject to the same requirements as onshore institutions and are regulated by the Superintendence of Banks. In June 2002, Guatemala enacted the Banks and Financial Groups Law (No. 19-2002), which places offshore banks under the oversight of the SIB. The law requires offshore banks to be authorized by the Monetary Board and to maintain an affiliation with a domestic institution. It also prohibits an offshore bank that is authorized in Guatemala from doing business in another jurisdiction; however, banks authorized by other jurisdictions may do business in Guatemala under certain limited conditions.

To authorize an offshore bank, the financial group to which it belongs must first be authorized, under a 2003 resolution of the Monetary Board. By law, no offshore financial services businesses, other than banks, are allowed. In 2004, the SIB and Guatemala's financial intelligence unit (FIU), the *Intendencia de Verificación Especial (IVE)*, concluded a process of reviewing and licensing all offshore entities, a process which resulted in the closure of two operations. No offshore trusts have been authorized. Offshore casinos and Internet gaming sites are not regulated.

There is continuing concern over the volume of money passing informally through Guatemala. Much of the more than U.S. \$4.1 billion in 2007 remittance flows passed through informal channels, although sector reforms led to an increased use of banks and other formal means of transmission. Terrorist finance legislation enacted in August 2005 requires remitters to maintain name and address information on senders (principally U. S. based) on transfers equal to or over an amount to be determined by implementing regulations. Increasing financial sector competition should continue to expand services and bring more people into the formal banking sector, isolating those who abuse informal channels.

Decree 67-2001, or the "Law Against Money and Asset Laundering," criminalizes money laundering in Guatemala. This law specifies that individuals convicted of money or asset laundering are subject to a noncommutable prison term ranging from six to 20 years, and fines equal to the value of the assets, instruments or products resulting from the crime. Convicted foreigners are deported from Guatemala. Conspiracy and attempt to commit money laundering are also penalized. The law applies to money laundering from any crime and does not require a minimum threshold to be invoked. It also holds institutions and individuals responsible for failure to prevent money laundering or allowing money laundering to occur, regardless of personal culpability. Bank and financial institution directors or other employees can lose their banking licenses and face criminal charges if they are found guilty of failure to prevent money laundering. This law also applies to the offshore entities that operate in Guatemala but are registered under the laws of another jurisdiction.

Decree 67-2001 also obligates individuals to declare the cross-border movement of currency in excess of approximately U.S. \$10,000 at the port of entry. The declaration forms are provided and collected by the tax authority at land borders, airports, and ports. The tax authority sends a copy of the sworn declaration to IVE for its database. The IVE can share this information with other countries under the terms and conditions specified by mutual agreement. In addition, the Law Against the Financing of Terrorism penalizes the omission of declaration with a sentence from one to three years in prison. At Guatemala City's international airport, a special unit was formed in 2003 to enforce the use of customs declarations upon entry to and exit from Guatemala. Money seized at the airports—approximately U.S. \$1.8 million in 2007—suggests that proceeds from illicit activity are regularly hand-carried over

Money Laundering and Financial Crimes

Guatemalan borders. However, apart from a cursory check of a self-reporting customs form, there is little monitoring of compliance at the airport. Compliance is not regularly monitored at land borders.

In addition to the requirements of Decree 67-2001, the Guatemalan Monetary Board's Resolution JM-191, which approves the "Regulation to Prevent and Detect the Laundering of Assets" (RPDLA), establishes anti-money laundering requirements for financial institutions. The RPDLA required all financial institutions under the oversight and inspection of the SIB to establish anti-money laundering measures, and introduced requirements for transaction reporting and record keeping. The Guatemalan financial sector has largely complied with these requirements and has a generally cooperative relationship with the SIB.

Financial institutions are prohibited from maintaining anonymous accounts or accounts that appear under fictitious or inexact names. Nonbank financial institutions, however, may issue bearer shares, and there is limited banking secrecy. However, Guatemalan law prohibits banking secrecy or privacy laws from being used to prevent the disclosure of financial information to bank supervisors and law enforcement authorities. Financial institutions are required to keep a registry of their customers as well as some types of transactions, such as the opening of new accounts or the leasing of safety deposit boxes. Financial institutions must also keep records of the execution of cash transactions exceeding \$10,000 or more per day, and report these transactions to the IVE. Under Decree 67-2001, financial institutions must maintain records of these registries and transactions for five years. Financial institutions are also mandated by law to report all suspicious transactions to the IVE. The law also exonerates financial institutions and their employees of any criminal, civil or administrative penalty for their cooperation with law enforcement and supervisory authorities with regards to the information they provide.

Decree 67-2001 established the IVE within the Superintendence of Banks to supervise financial institutions and ensure their compliance with the law. The IVE began operations in 2002 and in 2007 had a staff of 32. The IVE has the authority to obtain all information related to financial, commercial, or business transactions that may be connected to money laundering. The IVE conducts inspections of financial institution management, compliance officers, anti-money laundering training programs, "know-your-client" policies, and auditing programs. From January 2001 to December 2007, the IVE imposed over U.S. \$115,000 in administrative penalties for institutional failure to comply with anti-money laundering regulations.

Since its inception, the IVE has received approximately 2,302 suspicious transaction reports (STRs) from the 400 obligated entities in Guatemala. All STRs are received electronically, and the IVE has developed a system of prioritizing them for analysis. After determining that an STR is highly suspicious, the IVE gathers further information from public records and databases, other covered entities and foreign FIUs, and assembles a case. Once the IVE has determined a case warrants further investigation, the case must receive the approval of the SIB before being sent to the Anti-Money or Other Assets Laundering Unit (AML Unit) within the Public Ministry. Under current regulations, the IVE cannot directly share the information it provides to the AML Unit with any other special prosecutors (principally the anticorruption or counternarcotics units) in the Public Ministry. The IVE also assists the Public Ministry by providing information upon request for other cases the prosecutors are investigating.

The AML Unit is in charge of directing the investigation and prosecution of money laundering cases. This unit has a staff of 14 officials, and an investigative support group of 16 law enforcement officers and investigators. Both the prosecutors and investigators receive yearly ad hoc training in various investigative and legal issues. In 2006, Guatemala created a money laundering task force. The money laundering task force is a joint unit comprised of individuals from the Guatemalan Tax Authority (SAT), the IVE, Public Ministry, Prosecutor's Office, Government Ministry, National Police and Drug Police. Together they work on investigating financial crimes, building evidence and bringing the cases

to prosecution. In late 2007, the task force was working on four major money laundering investigations and a number of smaller money laundering and drug-related cases. Under the Anti-Organized Crime Law of 2006, the use of undercover operations, controlled deliveries, and wire taps is permitted to investigate many forms of organized crime activity, including money laundering crimes.

Twenty-seven cases have been referred by the IVE to the AML Unit. In several cases, assets have been frozen. Sixteen money laundering prosecutions have been concluded, fifteen of which resulted in convictions. The Public Ministry's AML Unit had initiated 63 cases as of January 2007, five of which have been transferred to other offices (such as the anticorruption unit) for investigation and prosecution, due to the nature of the particular crime. The seizures were made possible by information supplied by cooperating financial institutions.

Current law permits the seizure of any assets linked to money laundering. The IVE, the National Civil Police, and the Public Ministry have the authority to trace assets; the Public Ministry can seize assets temporarily in urgent circumstances, and the Courts of Justice have the authority to permanently seize assets. In 2003, the Guatemalan Congress approved reforms to allow seized money to be shared among several GOG agencies, including police and the IVE. Nevertheless, the Constitutional Court ruled that forfeited currency remains under the jurisdiction of the Supreme Court of Justice. The Anti-Organized Crime Law provides the possibility for a summary procedure to forfeit the seized assets and allows both civil and criminal forfeiture.

The courts do not allow seized currency to be used by enforcement agencies while cases remain open. For money laundering and narcotics cases, any seized money is deposited in a bank safe and all material evidence is sent to the warehouse of the Public Ministry. There is no central tracking system for seized assets, and it is currently impossible for the GOG to provide an accurate listing of the seized assets in custody. In 2006, Guatemalan authorities seized approximately U.S. \$222,000 in bulk currency. No statistics are currently on the amount of assets seized in 2007. The lack of access to the resources of seized assets outside of the judiciary has made sustaining seizure levels difficult for the resource-strapped enforcement agencies.

In June 2005, the Guatemalan Congress passed legislation criminalizing terrorist financing, the Law Against the Financing of Terrorism. Implementing regulations were enacted by the Monetary Board in December 2005. The counter-terrorist financing legislation also clarifies the legality of freezing assets in the absence of a conviction where the assets were destined to support terrorists or terrorist acts. The legislation brings Guatemala into compliance with the FATF Special Recommendations on terrorist financing and the United Nations Security Council Resolution 1373. The GOG has cooperated fully with U.S. efforts to track terrorist financing funds.

Guatemala is a party to the UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Guatemala is also a party to the Inter-American Convention against Terrorism and the Central American Convention for the Prevention of Money Laundering and Related Crimes. The GOG is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). In 2003, the IVE became a member of the Egmont Group. The IVE has signed a number of Memoranda of Understanding regarding the exchange of information on money laundering issues, seventeen of which also include the exchange of information regarding the financing of terrorism.

Corruption and organized crime remain endemic in Guatemala and are the biggest long-term challenges to the rule of law in Guatemala. The Government of Guatemala has made efforts to comply with international standards and improve its anti-money laundering and counter-terrorist financing regime; however, Guatemala should eliminate the use of bearer shares as well as identify and regulate

offshore financial services and gaming establishments. The GOG should also continue efforts to improve enforcement of existing regulations and implement needed reforms. Cooperation between the IVE and the Public Ministry has improved in recent years, and several investigations have led to prosecutions. However, Guatemala should increase its capacity to successfully investigate and prosecute money laundering cases. Additionally, the GOG should identify or create a centralized agency to manage and dispose of seized and forfeited assets, create an assets forfeiture fund which would distribute forfeited assets to law enforcement agencies to assist in the fight against money laundering, terrorist financing, and other financial crime.

Guernsey

The Bailiwick of Guernsey (the Bailiwick) encompasses a number of the Channel Islands (Guernsey, Alderney, Sark, and Herm). A Crown Dependency of the United Kingdom, it relies on the United Kingdom for its defense and international relations. However, the Bailiwick is not part of the UK. Alderney and Sark have their own separate parliaments and civil law systems. Guernsey's parliament legislates in matters of criminal justice for all of the islands in the Bailiwick. Guernsey is a sophisticated financial center and, as such, it continues to be vulnerable to money laundering at the layering and integration stages.

The approximately 18,800 companies registered in the Bailiwick do not fall within the standard definition of an international business company (IBC). Guernsey and Alderney incorporate companies, but Sark, which has no company legislation, does not. Companies in Guernsey must disclose beneficial ownership to the Guernsey Financial Services Commission (FSC) before legal formation or acquisition.

Guernsey has 47 banks, all of which have offices, records, and a substantial presence in the Bailiwick. The banks are licensed to conduct business with residents and nonresidents alike. There are 632 international insurance companies and 851 collective investment funds. There are also 18 bureaux de change, ten of which are part of a licensed bank. Bureaux de change and other money service providers must register their information with the FSC.

Guernsey has a comprehensive legal framework to counter money laundering and the financing of terrorism. Guernsey had further honed its anti-money laundering and counter-terrorist financing (AML/CTF) legislation with the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007. The legislation criminalizes money laundering for all crimes except drug trafficking, which the Drug Trafficking (Bailiwick of Guernsey) Law, 2000, as amended, covers in identical terms. The Disclosure (Bailiwick of Guernsey) Law 2007 makes failure to disclose the knowledge or suspicion of money laundering a criminal offense. The duty to disclose suspicious activity extends to all businesses, not only financial services businesses. The original 1999 money laundering law creates a system of suspicious transaction reporting (including suspicion of tax evasion) to Guernsey's financial intelligence unit (FIU), the Financial Intelligence Service (FIS). In 2007, the FSC issued companion guidance entitled "Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing" which replaced the Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism.

Guernsey's legal framework contains additional legislative provisions aimed at assisting in the detection of money laundering and terrorist financing. These include search and seizure powers, customer information orders and account monitoring orders. The Transfer of Funds (Guernsey) Ordinance 2007 requires any parties that offer funds transfer services to provide verified identification information for any person transferring funds electronically.

Guernsey authorities have approved further measures to strengthen the existing AML/CTF regime that should be in force by the middle of 2008. These include a comprehensive civil forfeiture law, new

regulations for certain entities involved in high value transactions, and legislation governing charities and other nonprofit organizations.

Guernsey enacted the Prevention of Corruption (Bailiwick of Guernsey) Law of 2003 and the Regulation of Fiduciaries, Administration Businesses, and Company Directors, etc. (Bailiwick of Guernsey) Law of 2000 (“the Fiduciary Law”) to license, regulate and supervise company and trust service providers. Pursuant to Section 35 of the Fiduciary Law, the FSC must license all fiduciaries, corporate service providers and persons acting as company directors on behalf of any business. The FSC creates Codes of Practice for corporate service providers, trust service providers and company directors. To receive licenses, these agencies must follow strict standards, including client identification and “know your customer” (KYC) requirements. These entities are subject to regular inspection, and an entity’s failure to comply could result in prosecution and revocation of its license. The Bailiwick is fully compliant with the Offshore Group of Banking Supervisors (OGBS) Statement of Best Practice for Company and Trust Service Providers.

The FSC regulates the Bailiwick’s financial banks, insurance companies, mutual funds and other collective investment schemes, investment firms, fiduciaries, company administrators and company directors. The Bailiwick does not permit bank accounts to be opened unless there has been a KYC inquiry and the customer provides verification details. Regulations contain penalties to be applied when financial services businesses do not follow their obligations. Upon a company’s application for incorporation, the FSC evaluates the request. The Royal Court maintains the registry of incorporated companies. The Court will not permit incorporation unless the FSC and the Attorney General or Solicitor General have given approval. The Commission conducts regular on-site inspections and analyzes the accounts of all regulated institutions.

On July 1, 2005, the European Union Savings Tax Directive (ESD) came into force. The ESD is an agreement between the Member States of the European Union (EU) to automatically exchange information with other Member States about EU tax resident individuals who earn income in one EU Member State but reside in another. Although not part of the EU, the three UK Crown Dependencies (Guernsey, Jersey, and the Isle of Man), have voluntarily agreed to apply the same measures to those in the ESD and have elected to implement the withholding tax option (also known as the “retention tax option”) within the Crown Dependencies.

Under the retention tax option, each financial services provider will automatically deduct tax from interest and other savings income paid to EU resident individuals. The tax will then be submitted to local and Member States tax authorities annually. The tax authorities receive a bulk payment but do not receive personal details of individual customers. If individuals elect the exchange of information option, then no tax is deducted from their interest payments but details of the customer’s identity, residence, paying agent, level and time period of savings income received by the financial services provider will be reported to local tax authorities where the account is held and then forwarded to the country where the customer resides.

The Guernsey authorities have established a forum, the Crown Dependencies Anti-Money Laundering Group, where the Attorneys General, Directors General, and representatives of Police, Customs, the regulatory community and FIUs from the Crown Dependencies meet to coordinate AML/CTF policies and strategy.

The FIS operates as the Bailiwick’s FIU, and is comprised of Police and Customs Officers. The Service Authority, a committee of senior Police and Customs Officers who coordinate the Bailiwick’s financial crime strategy, directs the FIS. With a mandate to focus on money laundering and terrorist financing issues, the FIS serves as the central point within the Bailiwick for the receipt, collation, analysis, and dissemination of all financial crime intelligence. Much of this information comes from suspicious transaction report (STR) filings. In 2007, the FIS received 539 STRs.

The Bailiwick narcotics trafficking, money laundering, and terrorism laws designate the same foreign countries as the UK to enforce foreign restraint and confiscation orders.

In 2008, Guernsey will be the subject of an assessment regarding its compliance with internationally accepted standards and measures of good practice relative to its regulatory and supervisory arrangements for the financial sector. The International Monetary Fund (IMF) will conduct this assessment. The previous IMF assessment, conducted in 2002, determined that Guernsey had developed a legal and institutional AML/CTF framework and had a high level of compliance with what was then the Financial Action Task Force (FATF) Forty Recommendations.

There has been counterterrorism legislation covering the Bailiwick since 1974. The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, replicates equivalent UK legislation. The Terrorism Law criminalizes the failure to report suspicion or knowledge of terrorist financing.

Guernsey cooperates with international law enforcement on money laundering cases. The FSC also cooperates with regulatory/supervisory and law enforcement bodies. The Criminal Justice (International Cooperation) (Bailiwick of Guernsey) Law, 2000, furthers cooperation between Guernsey and other jurisdictions by allowing certain investigative information concerning financial transactions to be exchanged. In cases of serious or complex fraud, Guernsey's Attorney General can provide assistance under the Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law 1991.

On September 19, 2002, the United States and Guernsey signed a Tax Information Exchange Agreement, which came fully into force in 2006. The agreement provides for the exchange of information on a variety of tax investigations, paving the way for audits that could uncover tax evasion or money laundering activities. Guernsey is negotiating similar agreements with other countries. The 1988 U.S.-UK Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking, as amended in 1994, was extended to the Bailiwick in 1996.

Guernsey enacted the necessary legislation to implement the Council of Europe Convention on Mutual Assistance in Criminal Matters, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and the 1988 UN Drug Convention, upon their extension to the Bailiwick in 2002. The Bailiwick has requested that the UK Government seek the extension to the Bailiwick of the UN International Convention for the Suppression of the Financing of Terrorism.

Guernsey is a member of the Offshore Group of Insurance Supervisors and the Offshore Group of Banking Supervisors. The FIS has been a member of the Egmont Group since 1997 and represents the jurisdiction within The Camden Assets Recovery Inter-Agency Network (CARIN), an informal network of European Union (EU) member state contacts convened to work on asset recovery.

Guernsey continues to amend current legislation to stay current with international standards. Guernsey should ensure passage of its new 2008 legislation, and enact it, as soon as possible. It should integrate civil forfeiture into its legal framework. Guernsey should also work to ensure that the obliged entities uphold their legal obligations, and that the regulatory authorities have the tools they need to provide supervisory functions, especially with regard to nonfinancial businesses and professions. Guernsey should likewise ensure that all obliged entities receive the UN 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations.

Guinea-Bissau

Guinea-Bissau is not a regional financial center. Guinea-Bissau's instability and tiny economy make it an unlikely site for major money laundering. Increased drug trafficking and the prospect of oil

production, however, increase its vulnerability to money laundering and financial crime. Drug traffickers transiting between Latin America and Europe have increased their use of the country. Often, Guinea-Bissau is the placement point for proceeds from drug payoffs, theft of foreign aid, and corrupt diversion of oil and other state resources headed for investment abroad. A recent boom in construction of luxury homes, hotels and businesses, and the proliferation of expensive vehicles stands in sharp contrast with the conditions in the poor local economy. It is likely that at least some of the new wealth derives from money laundered from drug trafficking. Banking officials also think the country is vulnerable to trade-based money laundering (TBML).

The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the eight countries in the West African Economic and Monetary Union (WAEMU or UEMOA), including Guinea-Bissau, and uses the CFA franc currency. The Commission Bancaire, the BCEAO division responsible for bank inspections, is based in Abidjan. However, it does not execute a full AML examination during its standard banking compliance examinations.

The legal basis for Guinea-Bissau's AML/CTF framework is the Loi Uniforme Relative a Lutte Contre le Blanchiment de Capiteaux No. 2004-09 of February 6, 2004, or the Anti-Money Laundering Uniform Law (Uniform Law). As the common law passed by the members of UEMOA/WAEMU, all member states are required to enact and implement the legislation. On November 2, 2004, Guinea-Bissau became the third WAEMU/UEMOA country to enact the Uniform Law. The new legislation largely meets international standards with respect to money laundering. Guinea-Bissau has an "all crimes" approach to money laundering. The law requires banks and other financial institutions to know their customers and record and report the identity of any person who engages in significant transactions, including the recording of large currency transactions. Covered institutions include financial institutions and nonbank financial institutions such as exchange houses, brokerages, cash couriers, casinos, insurance companies, charities, nongovernmental organizations (NGOs), and intermediaries such as lawyers, accountants, notaries and broker/dealers. All obliged entities must report all suspicious transactions to the financial intelligence unit (FIU). There is no threshold amount triggering a report. Safe harbor provisions give reporting individuals and their supervisors civil and criminal immunity and immunity from professional sanctions for providing information to the FIU in good faith. There is no exemption for "self laundering". It is not necessary to have a conviction for the predicate offense before prosecuting or obtaining a conviction for money laundering. Criminal liability applies to all legal persons as well as natural persons. The new legislation meets many international standards with respect to money laundering, and goes beyond, by covering the microfinance sector, but does not comply with all Financial Action Task Force (FATF) recommendations concerning politically-exposed persons (PEPs), and lacks certain compliance provisions for nonfinancial institutions. All three banks operating in the country report that they have anti-money laundering (AML) compliance programs in place. However, Article 26 of National Assembly Resolution No. 4 of 2004 stipulates that if a bank suspects money laundering, it must obtain a declaration of all properties and assets from the subject and notify the Attorney General, who must then appoint a judge to investigate. The bank solicitation of an asset list from its client could amount to "tipping off" the subject. The WAEMU/UEMOA Uniform Law does not deal with terrorist financing.

Western Union and MoneyGram function under the auspices of the banks. Unlicensed money remitters and currency exchangers, although prevalent, are illegal. Authorities report problems with porous borders and cash smuggling; reportedly, corruption in the Customs agency exacerbates this situation.

The Uniform Law provides for the establishment of an FIU, and a 2006 Directive to establish it is in place. However, no operational FIU exists in the country. Guinea-Bissau is working with external donors to establish a functioning FIU, which will be housed within the Ministry of Economy and Finance. A senior Ministry of Finance official will administer the FIU. The FIU's mandate will be to receive and analyze suspicious transaction reports (STRs) and, when it deems appropriate, to refer

files to the Prosecutor General. The FIU will rely on counterparts in law enforcement and other governmental institutions to provide information upon request for the FIU's investigations. Lack of capacity, corruption, instability, and distrust (particularly of the judicial sector), could significantly hamper progress in the FIU's development. Reportedly, banks are reluctant to file STRs because of the fear of "tipping off" by an allegedly indiscrete judiciary. The FIU, when operational, can legally share information with any other FIU in the WAEMU/UEMOA countries.

The Judicial Police and Prosecutors investigate money laundering as well as terrorist financing. The Attorney General's office houses a small unit to investigate corruption and economic crimes. In November 2007, Guinea-Bissau's government Audit Office created a commission to investigate illegal acquisition of wealth by present and former government officials. However, a lack of training and capacity, as well as endemic corruption and reported lack of cooperation from banks, impede investigations. Official statistics regarding the prosecution of financial crimes are unavailable. There are no known prosecutions of money laundering.

Although the current AML legislation obliges NGOs and nonprofits, including charities, to file STRs, the current regulatory regime is unknown.

Article 203, Title VI of Guinea-Bissau's penal code criminalizes terrorist financing. However, there are no reporting requirements or attendant regulations. In addition, because the penal code only criminalizes the financing of terrorist groups or organizations, it does not address financing of a single or individual terrorist. The penal code also does not criminalize the financing of terrorist organizations when the money is not used to commit terrorist acts. The BCEAO has released Directive No. 04/2007/CM/UEMOA, obliging member states to pass domestic counter-terrorist financing legislation. Member states must enact a law against terrorist financing, which will likely be a Uniform Law to be adopted by all WAEMU/UEMOA members in the same manner as the AML law. Each national assembly must then enact the law. In July 2007, UEMOA/WAEMU released attendant guidance on terrorist financing for member states. In addition, the FATF-style regional body for the Economic Community of Western African States (ECOWAS), the African Anti-Money Laundering Intergovernmental Group (GIABA) has drafted a uniform law, which it has recommended that all of its member states adopt and enact.

The Ministry of Finance and the BCEAO circulate the UN 1267 Sanctions Committee consolidated list to commercial financial institutions. To date, no entity has identified assets relating to terrorist entities. The WAEMU/UEMOA Council of Ministers has issued a directive requiring banks to freeze assets of entities designated by the Sanctions Committee.

Multilateral ECOWAS treaties deal with extradition and legal assistance. Under the Uniform Law, once established, the FIU may share information freely with other FIUs in the union. Guinea-Bissau is a party to the 1988 UN Drug Convention, and has signed but not ratified the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, or the African Union (AU) Anticorruption Convention. Guinea-Bissau is a member of ECOWAS and GIABA. It has not signed or ratified the UN Convention against Corruption. Transparency International's 2007 Corruption Perception Index ranks Guinea Bissau 147 out of 180 countries.

The Government of Guinea-Bissau (GOGB) should continue to work with its partners in GIABA, WAEMU/UEMOA and ECOWAS to establish and implement a comprehensive AML/CTF regime that comports with all international standards. GOGB should ensure that the sectors covered by its AML law have implementing regulations and supervisory authorities to ensure compliance with the law's requirements. The GOGB should clarify, amend or eliminate Article 26 of the 2004 National Assembly Resolution that appears to mandate actions resulting in the tipping off of suspects. It should also adopt and enact the uniform terrorist financing law when it is presented to the WAEMU/UEMOA states. Guinea-Bissau should amend the definitions in its penal code to comport with the international

standards regarding financing of individual terrorists and terrorist groups engaging in acts other than terrorism. It should establish, staff and train, its FIU, and ensure that resources are available to sustain its capacity. It should work to improve the training and capacity of its police and judiciary to combat financial crimes, and address any issues resulting from a lack of understanding of money laundering and terrorist financing. Guinea-Bissau should undertake efforts to eradicate systemic corruption and become a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Conventions against Corruption and Transnational Organized Crime, and the African Union (AU) Anti-corruption Convention.

Guyana

Guyana is neither an important regional nor an offshore financial center, nor does it have any free trade zones. Money laundering is perceived as a serious problem, and has been linked to trafficking in drugs, firearms, and persons, as well as to corruption and fraud. The Government of Guyana (GOG) made no arrests or prosecutions for money laundering in 2007. Guyana currently has inadequate legal and enforcement mechanisms to combat money laundering, although legislation tabled in Parliament would enhance the GOG's anti-money laundering regime.

The Money Laundering Prevention Act (MLPA) of 2000 criminalizes money laundering related to narcotics trafficking, illicit trafficking of firearms, extortion, corruption, bribery, fraud, counterfeiting, and forgery. The MLPA does not specifically cover the financing of terrorism or all serious crimes in its list of offenses. Banks, finance companies, factoring companies, leasing companies, trust companies, and securities and loan brokers are required to report suspicious transactions to the GOG's financial intelligence unit (FIU), and records of suspicious transaction reports (STRs) must be kept for six years. However, the GOG does not release statistics on the number of STRs received by the FIU, despite the requirement to make these statistics available to relevant authorities as mandated by the Financial Action Task Force (FATF). The MLPA also requires that the cross-border transportation of currency exceeding U.S. \$10,000 be reported to the Customs Administration, but does not allow for the provision of this information to the FIU or other law enforcement bodies. The MLPA establishes the Guyana Revenue Authority, the Customs Anti-Narcotics Unit, the Attorney General, the Director for Public Prosecutions, and the FIU as the authorities responsible for investigating financial crimes.

The GOG's anti-money laundering regime is rendered ineffective by other major structural weaknesses of the MLPA. While the MLPA provides for the seizure of assets derived as proceeds of crime, guidelines for implementing seizures and forfeitures have never been established. Conviction for a predicate offense is considered necessary before a money laundering conviction can be obtained, and the list of such predicate offenses is cursory. While the FIU may request additional information from obligated entities, it does not have access to law enforcement information or the authority to exchange information with its foreign counterparts. These limitations collectively stifle the analytical and investigative capabilities of the FIU and law enforcement agencies. As a result of these legislative weaknesses, there have been no money laundering prosecutions or convictions to date.

To augment the tools available to the GOG's anti-money laundering authorities, the FIU drafted legislation entitled the Anti-Money Laundering and Countering the Financing of Terrorism Bill 2007. The bill provides for the identification, freezing, and seizure of proceeds of crime and terrorism; establishes comprehensive powers for the prosecution of money laundering, terrorist financing, and other financial crimes; requires reporting entities to take preventive measures to help combat money laundering and terrorist financing; provides for the civil forfeiture of assets; expands the scope of the money laundering offense; and mandates the accessibility of all relevant data among law enforcement agencies. The legislation provides for oversight of export industries, the insurance industry, real estate, and alternative remittance systems, and sets forth the penalties for noncompliance. The bill also establishes the FIU as an independent body that answers only to the President, and defines in detail its

role and powers. The draft legislation was tabled in Parliament in late 2007, but its passage in the near future is uncertain.

In January 2007, the National Assembly passed the Gambling Prevention (Amendment) Bill, which legalizes casino gambling. The bill establishes a Gaming Authority authorized to issue casino licenses to new luxury hotel or resort complexes with a minimum of 150 rooms. Vocal opposition to the bill from religious groups, opposition parties, and the public included concerns that casino gambling would provide a front for money launderers. No casinos have opened in Guyana to date.

The Ministry of Foreign Affairs and the Bank of Guyana continue to assist U.S. efforts to combat terrorist financing by working towards compliance with relevant United Nations Security Council Resolutions (UNSCRs). In 2001, the Bank of Guyana, the sole financial regulator as designated by the Financial Institutions Act of March 1995, issued orders to all licensed financial institutions expressly instructing the freezing of all financial assets of terrorists, terrorist organizations, and individuals and entities associated with terrorists and their organizations. Guyana has no domestic laws authorizing the freezing of terrorist assets, but the government created a special committee on the implementation of UNSCRs, co-chaired by the Head of the Presidential Secretariat and the Director General of the Ministry of Foreign Affairs. To date the procedures have not been tested, as no terrorist assets have been identified in Guyana. The FIU director also disseminates the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list to relevant financial institutions.

Guyana is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). Guyana is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. On September 12, 2007, the GOG became a party to the International Convention for the Suppression of the Financing of Terrorism, and on June 5, 2007, Guyana ratified the Inter-American Convention against Terrorism. The GOG has not signed the UN Convention against Corruption. Guyana's FIU is one of the few in the region that is not a member of the Egmont Group, and no change in that status is anticipated until Guyana's anti-money laundering laws have been modernized and the financing of terrorism is criminalized. Guyana does not have a Mutual Legal Assistance Treaty (MLAT) with the United States.

The Government of Guyana should pass the draft legislation on money laundering and terrorist financing that is currently before the Parliament. The passage of this legislation would extend preventive measures to a far wider range of reporting entities, including casinos and designated nonfinancial businesses and professions. The draft legislation would also provide greater resources and critical autonomy for the FIU, enable the FIU to access law enforcement data, and ensure that the FIU has the operational capacity to meet the membership requirements of the Egmont Group. In short, the passage of this legislation is essential in enhancing the GOG's compliance with international standards and ensuring that its anti-money laundering and counter-terrorist financing regime is operational and effective. In the interim, Guyana should provide appropriate resources and awareness training to its regulatory, law enforcement, and prosecutorial personnel, and establish procedures for asset seizure and forfeiture. The GOG should also become a party to the UN Convention against Corruption.

Haiti

Haiti is not a major financial center. Haiti's dire economic condition and unstable political situation inhibit the country from advancing its formal financial sector. Nevertheless, Haiti is a major drug-transit country with money laundering activity linked to the drug trade. Money laundering and other financial crimes are facilitated through the banks and casinos, and through foreign currency transactions and real estate transactions. While the informal economy in Haiti is significant and partly

funded by illicit narcotics proceeds, smuggling is historically prevalent and predates narcotics trafficking.

Flights to Panama City, Panama, remain the main identifiable mode of transportation for money couriers. Suspected drug flights from Venezuela continue, where a permissive environment allows smuggling aircraft to operate with impunity. Travelers, predominantly Haitian citizens, usually hide large sums ranging from U.S. \$30,000 to \$100,000 on their persons. There is low confidence in the efforts of Haitian customs and narcotics personnel to interdict these outbound funds. Suspicions that clandestine fees are collected to facilitate the couriers continuing without arrest appear to be well-founded. In addition, those persons that are actually interdicted are frequently released by the courts and the funds are ordered to be returned.

During interviews, couriers usually declare that they intend to use the large amounts of U.S. currency to purchase clothing and other items to be sold upon their return to Haiti, a common practice in the informal economic sector. Cash that is routinely transported to Haiti from Haitians and their relatives in the United States in the form of remittances represented over 21.2 percent of Haiti's gross domestic product in 2006, according to the World Bank. The Inter-American Development Bank estimated the flow of remittances through official channels to Haiti at \$1.65 billion in fiscal year 2006.

The Government of Haiti (GOH) has made progress in recent years to improve its legal framework, create and strengthen core public institutions, and enhance financial management processes and procedures. The constitutional government of President René Préval and Prime Minister Jacques Edouard Alexis continued the monetary, fiscal and foreign exchange policies initiated under the past Interim Government of Haiti with the assistance of the International Monetary Fund and the World Bank. Continued insecurity and a lack of personnel expertise, however, have reduced the impact of the Government's initiatives and hampered its ability to modernize its regulatory and legal framework.

Despite political instability, Haiti has taken steps to address its money laundering and financial crimes problems. President Préval has openly affirmed his commitment to fight corruption, drug trafficking, and money laundering. He is actively seeking technical assistance and cooperation with countries in the region to reinforce Haiti's institutional capacity to fight financial crime. In March 2007, the GOH participated in a Summit on Drug and Money Laundering in the Dominican Republic to identify synergies between countries in the region (Haiti, Dominican Republic, Jamaica and Colombia) to fight organized crime. Preparations are underway for a subsequent meeting to be held by the end of December 2007 in Cartagena, Colombia.

Since 2001, Haiti has used the Law on Money Laundering from Illicit Drug Trafficking and other Crimes and Punishable Offenses (AML Law) as its primary anti-money laundering legislation. Although the government has publicly committed to combat corruption, the court system is slow to move forward with pending cases. None of the investigations initiated under the interim government have led to any prosecutions, and the Financial Crimes Task Force (FCTF), which is charged with conducting financial investigations, is currently inoperative.

The AML Law criminalizes money laundering and establishes a wide range of financial institutions as obligated entities, including banks, money remitters, exchange houses, casinos, and real estate agents. Insurance companies, which are only nominally represented in Haiti, are not covered. The AML Law requires financial institutions to establish money laundering prevention programs and to verify the identity of customers who open accounts or conduct transactions that exceed 200,000 gourdes (approximately U.S. \$5,550). It also requires exchange brokers and money remitters to compile information on the source of funds exceeding 200,000 gourdes or its equivalent in foreign currency. Microfinance institutions and credit unions, however, remain largely unregulated. A draft banking law, if passed by Parliament, will address this regulatory gap.

Money Laundering and Financial Crimes

The AML Law contains provisions for the forfeiture and seizure of assets; however, the government cannot seize and declare the assets forfeited until there is a conviction. Although the AML Law provides grounds for seizure, it does not contain procedures to handle the management and proceeds of seized assets. This deficiency in the law reduces the government's authority and resources to prosecute cases. Out of U.S. \$565,723 seized in 2007 at the airport in Port-au-Prince, courts ordered that U.S. \$367,417 be returned to the owners.

Implementation of the AML Law is compromised by weak enforcement mechanisms, poor understanding of the law on the part of legal and judicial personnel and an overall weak judicial system. From 2001 to 2007, 475 persons were arrested in connection with drug trafficking and money laundering. Fifteen individuals were sent to the United States to face prosecution. The remaining 460 individuals have yet to be prosecuted in Haitian courts. An amendment to the AML Law to redress weaknesses in the current law is being drafted for consideration by Parliament.

In 2002, Haiti formed a National Committee to Fight Money Laundering (CNLBA) under the supervision of the Ministry of Justice and Public Safety. The CNLBA is in charge of promoting, coordinating, and recommending policies to prevent, detect, and suppress the laundering of assets obtained from the illicit trafficking of drugs and other serious offenses. Haiti's financial intelligence unit (FIU), established in 2003, is the Unité Centrale de Renseignements Financiers (UCREF), which falls under the supervision of the CNLBA. The UCREF's mandate is to receive and analyze reports submitted by financial institutions in accordance with the law. The UCREF has 42 employees, including 23 analysts. Institutions, including banks, credit unions exchange brokers, insurance companies, lawyers, accountants, and casinos, are required to report to the UCREF transactions involving funds that may be derived from a crime, as well as transactions that exceed 200,000 gourdes (U.S. \$5,550). Failure to report such transactions is punishable by more than three years' imprisonment and a fine of 20 million gourdes (approximately U.S. \$550,000). Banks are required to maintain records for at least five years and to present this information to judicial authorities and UCREF officials upon request. Bank secrecy or professional secrecy cannot be invoked as grounds for refusing information requests from these authorities.

In 2006, the UCREF assisted the U.S. in at least three major investigations. UCREF also assisted the interim government in filing the first-ever civil lawsuit in a U.S. court for reparation of Haitian government funds diverted through U.S. banks and businesses. However, the lawsuit was dropped shortly after the new government took office. Despite recent achievements, the UCREF is still not fully functional, and the UCREF's analysts lack the experience and skills needed to independently analyze suspect financial activities, write adequate reports and expeditiously move cases to prosecutors. Due to the absence of an investigative institution tasked with conducting financial investigations in the justice system, the UCREF responded to fill the void. This has led to a perception of conflict of interest and has, in some high-profile cases, sparked controversy.

In November, in response to a request for assistance from President Preval, the U.S. Treasury and the GOH entered into an agreement to restructure UCREF into an administrative FIU, and to reconstitute the investigative functions of the FCTF into a new and separate Office of Financial and Economic Affairs (BAFE). The U.S. Treasury Department agreed to provide training and technical assistance to BAFE investigators as well as the UCREF analysts, prosecutors, and judges. The World Bank has also entered into an agreement with the GOH to assist with training. These steps were supported by President Préval, who has sent out a presidential mandate to his ministers to support these new efforts in combating money laundering and corruption. In addition, draft counter-terrorist financing legislation has been submitted to the USG for review and comment.

Corruption is an ongoing challenge to economic growth. Haiti is ranked one of the most corrupt countries in the world according to Transparency International's Corruption Perception Index for 2007. The GOH has made incremental progress in enforcing public accountability and transparency,

but substantive institutional reforms are still needed. In 2004, the government established the Specialized Unit to Combat Corruption (ULCC) in the Ministry of Economy and Finance. The ULCC is in the process of drafting a national strategy to combat corruption and has prepared a draft law for asset declaration by public sector employees and a code of ethics for the civil service. ULCC will submit the law to Parliament for consideration in the coming months.

Haiti has yet to pass legislation criminalizing the financing of terrorists and terrorism, and is not a party to the International Convention for the Suppression of the Financing of Terrorism. Haiti reportedly circulates the list of terrorists and terrorist organizations identified in UN Security Council Resolution 1267. The AML Law may provide sufficient grounds for freezing and seizing the assets of terrorists; however, given that there is currently no indication of the financing of terrorism in Haiti, this has not been tested.

Haiti is a party to the 1988 UN Drug Convention, and has signed, but not ratified, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. Haiti is a member of the OAS/CICAD Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). In September 2007, the World Bank conducted an assessment of the GOH that will also serve as a CFATF mutual evaluation; the report will be released in the spring of 2008. The UCREF is not a member of the Egmont Group of financial intelligence units. The UCREF has memoranda of understanding with the FIUs of the Dominican Republic, Panama, Guatemala and Honduras.

The GOH appears cognizant of deficiencies in its anti-money laundering and counter-terrorist financing regime through its efforts to improve its legal framework to combat, drug trafficking, money laundering, and corruption, and its action to reform the judicial process. President Preval has made these improvements a key element of his national agenda. Areas in need of improvement include an ineffective court system, weak enforcement mechanisms and poor knowledge of current laws governing this area. The GOH should move quickly to prosecute cases of corruption, drug trafficking and money laundering. This could send a positive message that financial crimes will be punished to the fullest extent of the law and also help garner broader public support for the rule of law. The GOH should also reinforce the capacity of the Haitian justice system to prosecute financial crimes. Initiatives to enhance the UCREF's capacity to meet the Egmont Group membership standards and provide timely and accurate reports on suspicious financial activities are also needed. The GOH should finalize its draft legislation on terrorist financing to criminalize the financing of terrorism and become a party to the International Convention for the Suppression of the Financing of Terrorism.

Honduras

Money laundering in Honduras stems primarily from significant narcotics trafficking, particularly cocaine, throughout the region. Trafficking in persons also constitutes a growing source of laundered funds. Laundered proceeds typically pass directly through the formal banking system, but currency exchange houses and front companies may be used with increasing frequency. High remittance inflows, which reached more than \$2.6 billion in 2007, as well as a rapidly growing construction sector and smuggling of contraband goods, may also generate funds that are laundered through the banking system. Money laundering in Honduras derives both from domestic and foreign criminal activity, and the majority of proceeds are suspected to be controlled by local drug trafficking organizations and organized crime syndicates. Honduras does not appear to be experiencing an increase in financial crimes such as bank fraud. Lack of resources for investigations and analysis, as well as corruption, remain serious problems, particularly within the judiciary and law enforcement sectors.

Honduras is not an important regional or offshore financial center. It does not have a significant black market for smuggled goods, although recent high-profile smuggling cases have involved gasoline and

illegal lobster. Honduras has established a number of free trade zones with special tax and customs benefits. The majority of companies with free trade zone status operate in the textile and apparel industry, mostly assembling piece goods that originated in the United States for re-export to the United States. Under Honduran legislation, companies may register for “free trade zone” status, and enjoy the associated tax benefits, regardless of their location in the country. In 2007, banks reported two abnormal transactions into the accounts of free-trade zone factory owners. Although prosecutors suspect money laundering, they were not able to build enough evidence to prosecute either case. There is no other evidence Honduran free trade zone companies are being used in trade-based money-laundering schemes or by financiers of terrorism.

Money laundering has been a criminal offense in Honduras since 1998. Law No. 27-98 criminalizes the laundering of narcotics-related proceeds and contains various record-keeping and reporting requirements for financial institutions. Decree No. 45-2002 strengthens the legal framework and available investigative and prosecutorial tools to fight money laundering. Decree 45-2002 expands the definition of money laundering to include transfer of assets that proceed directly or indirectly from trafficking of drugs, arms, human organs or persons; auto theft; kidnapping; bank and other forms of financial fraud; and terrorism, as well as any sale or movement of assets that lacks economic justification. The penalty for money laundering is 15 to 20 years. The law also requires all persons entering or leaving Honduras to declare (and, if asked, present) cash and convertible securities that they are carrying if the amount exceeds U.S. \$10,000 or its equivalent.

Decree 45-2002 also creates the financial intelligence unit (FIU), the Unidad de Información Financiera (UIF), within the National Banking and Insurance Commission (CNBS). Banks and financial institutions are required to report any suspicious transactions and all transactions over \$10,000, or its equivalent to the UIF. The UIF and reporting institutions must keep a registry of reported transactions for five years. Banks are required to know the identity of all their clients and depositors, regardless of the amount of deposits, and to keep adequate records of the information. Banker negligence provisions subject individual bankers to two- to five-year prison terms if, by carelessness, negligence, inexperience, or nonobservance of the law, they permit money to be laundered through their institutions. Anti-money laundering requirements apply to all financial institutions that are regulated by the CNBS, including state and private banks, savings and loan associations, bonded warehouses, stock markets, currency exchange houses, securities dealers, insurance companies, credit associations, and casinos.

Decree No. 129-2004 eliminates any ambiguity concerning the responsibility of banks to report information to the supervisory authorities, and the duty of these institutions to keep customer information confidential, by clarifying that the provision of information requested by regulatory, judicial, or other legal authorities shall not be regarded as an improper divulgence of confidential information. Under the Criminal Procedure Code, officials responsible for filing reports on behalf of obligated entities are protected by law with respect to their cooperation with law enforcement authorities. However, some have alleged that their personal security is put at risk if the information they report leads to the prosecution of money launderers.

Congress is currently considering legislation that, if adopted, would bring the Government of Honduras (GOH) up to international legal standards for illicit financing, including money laundering and terrorist financing. In October 2007, the CNBS proposed to Congress major amendments to the money laundering law and proposed a new chapter to the penal code that would criminalize terrorist financing. The proposed amendments to the money laundering law would give the UIF oversight for collecting all suspicious transactions reports, and expand the scope of entities required to report suspicious transactions to the UIF beyond the financial scope of the CNBS. Such entities would include real estate agents, used car dealership, antique and jewelry dealers, remittance companies, armed car contractors, and nongovernmental organizations. The reforms would also give the UIF sole

oversight and responsibility not only for collecting suspicious transaction reports but for analyzing and presenting to prosecutors cases deemed appropriate for prosecution.

The Public Ministry (Attorney General's Office), UIF, and police all suffer from low funding, limited capacity, and a lack of personnel and training. For example, the police officers charged with investigations of money laundering crimes in Honduras must ride public buses to conduct investigations. The lack of capacity and coordination limits the scope of analysis and prosecutions, and prosecutors expend the bulk of their limited resources focusing on high-profile crimes related to money laundering, such as narcotics, trafficking in persons, and cash smuggling. Prior to 2004, there had been no successful prosecutions of crimes specifically labeled as money laundering in Honduras. Between 2004 and 2006, prosecutors obtained 11 convictions. Prosecutors initiated legal proceedings in eight cases in 2007, all of which are still ongoing, and obtained two additional convictions from prosecutions initiated in 2005. Only two of 54 ongoing investigations in 2007 originated from financial reports.

Attempts to improve coordination among the Public Ministry (Attorney General's Office), the UIF, and police have met with some degree of success; however there is still a need for additional improvement. An attempt in late 2004 to create a coordinating body, the Interagency Commission for the Prevention of Money Laundering and Financing of Terrorism (CIPLAFT), failed in early 2006, for political reasons. Although Decree 45-2002 requires that a public prosecutor be assigned to the UIF, the Special Prosecutor for Money Laundering himself acts as coordinator and contact is sporadic. Nevertheless, response times for information sharing between the UIF and the seized assets unit have improved due to a 2006 agreement between the Public Ministry, CNBS, and UIF to prioritize money laundering cases. These actions helped to streamline the number of cases for potential prosecution, and allowed many cases to be officially closed. Fewer active cases have allowed the overloaded prosecutors and under-funded police units to focus on the strongest and most important cases. Adoption of the new anti-money laundering amendments should improve coordination and clarify division of responsibilities for investigations and reporting.

Remittance inflows, mostly from the United States, are estimated at more than U.S. \$2.6 billion in 2007, which constitutes more than 25 percent of GDP. There has been no evidence to date linking these remittances to the financing of terrorism. However, it is estimated that up to half of cash flows labeled as remittances to Honduras may involve laundered money. Without the new money laundering amendment, the UIF lacks oversight capacity to properly investigate remittance companies, which are required to report suspicious transactions but currently not required to register under Honduran law. Remittances are increasingly sent through wire transfer or bank services, but the remittance companies themselves facilitate transactions that are carried out by separate financial institutions.

The GOH's asset seizure law has been in effect since 1993. The law allows for both civil and criminal forfeiture, and there are no significant legal loopholes that allow criminals to shield their assets. Decree No. 45-2002 strengthens the asset seizure provisions of the law, and establishes an Office of Seized Assets (OABI) under the Public Ministry. Decree 45-2002 also authorizes the OABI to guard and administer all goods, products, or instruments of a crime and requires money seized or money realized from the auctioning of seized goods to be transferred to the public entities that participated in the investigation and prosecution of the crime.

The OABI has moved to distribute funds to various law enforcement units and nongovernmental organizations (NGOs). The funds, which constituted the first systematic distribution under the new guidelines, went to the Supreme Court, federal prosecutors, OABI, and two civil society groups. Equitable sharing of seized monies has been a continuing problem, controlled by political influence. Police entities involved in the original investigations rarely see an equitable share of the assets seized. Groups like OABI and the Public Ministry generally receive an inflated portion of the forfeiture

proceeds, leaving next to nothing for the police. In some cases, entities that have nothing to do with the investigation receive an unjustified portion of the funds

The OABI is currently a poorly administered organization, evident by the vast amounts of assets that are unaccounted for, especially after the initial seizure, as well as the number of assets rotting away in parking lots, boat yards, and airports. The processing of final forfeiture of assets is mostly motivated by the entities that “arm wrestle” over who will actually receive disbursement of monies from auctioned assets or bulk cash seizure. This is typically influenced by political will. Momentum is now gaining for OABI to more quickly liquidate all assets once confiscated, in an effort to avoid parking lots full of deteriorating assets or high protection and maintenance fees. With new management and guidelines in place, OABI is set to expand its role significantly when a witness protection law passes that will allow the unit to hold all seized assets, not just assets seized under the money laundering law.

Decree No. 45-2002 leaves ambiguous the question of whether legitimate businesses found to be laundering money derived from criminal activities can be seized. Although the chief prosecutor for organized crime believes that businesses laundering criminal assets cease to be “legitimate,” subjecting them to seizure and prosecution, this authority is not explicitly granted in the law. There has been no test case to date that would set an interpretation. There are currently no new laws being considered regarding seizure or forfeiture of assets of criminal activity.

Under the Criminal Procedure Code, when goods or money are seized in any criminal investigation, a criminal charge must be submitted against the suspect within 60 days of the seizure; if one is not submitted, the suspect has the right to demand the release of the seized assets.

As of December 2006, the total value of assets seized since Decree 45-2002 came into effect was approximately U.S. \$5.7 million, including U.S. \$4.6 million in tangible assets such as cars, houses, and boats. The total for 2007 decreased compared to 2006, because the prosecutor was forced to return almost U.S. \$1 million this year, more than the sum collected. However, several high profile cases succeeded: U.S. \$750,000 collected from the sale of an abandoned plane in 2007, probably related to narcotics, was used to purchase several cars for police investigators, and U.S. \$500,000 collected from a high-profile lobster-smuggling case was awarded to the Ministry of Agriculture. Most of these seized assets have derived from crimes related to drug trafficking; none is suspected of being connected to terrorist activity.

Decree 45-2002 designates an asset transfer related to terrorism as a crime, but terrorist financing is not identified as a crime itself. However, in October 2007 the CNBS proposed adding a new chapter and five appendices to the Penal Code that would make financing of terrorism a crime. The crime would carry a 20 to 30 year prison sentence, along with a fine of up to \$265,000. Changes to the penal code may not be discussed by Congress until the Supreme Court issues an opinion on the penalties. The proposal was being considered by the Supreme Court as of November 2007. It is unlikely that the terrorist financing and money laundering amendments will be considered by Congress before April 2008.

Under separate authority, the Ministry of Foreign Affairs is responsible for instructing the CNBS to issue freeze orders for organizations and individuals named by the United Nations Security Council Resolution (UNSCR) 1267 and those organizations and individuals on the list of Specially Designated Global Terrorists by the United States pursuant to Executive Order 13224. The Commission directs Honduran financial institutions to search for, hold, and report on terrorist-linked accounts and transactions, which, if found, would be frozen. Both the Ministry of Foreign Affairs and CNBS have responded promptly to these requests. CNBS has reported that, to date, no accounts linked to the entities or individuals on the lists have been found in the Honduran financial system.

Honduras cooperates with U.S. investigations and requests for information pursuant to the 1988 United Nations Drug Convention. No specific written agreement exists between the United States and

Honduras to establish a mechanism for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing, and other crime investigations. However, Honduras has cooperated, when requested, with appropriate law enforcement agencies of the U.S. Government and other governments investigating financial crimes. The UIF has signed memoranda of understanding to exchange information on money laundering investigations with Panama, El Salvador, Guatemala, Mexico, Peru, Colombia and the Dominican Republic.

Honduras is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. At the regional level, Honduras is a member of the Central American Council of Bank Superintendents, which meets periodically to exchange information. Honduras is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering, and the Caribbean Financial Action Task Force (CFATF). In 2005, the UIF became a member of the Egmont Group.

The Government of Honduras made progress in 2007 by continuing to implement existing anti-money laundering regulations, and proposing improvements to existing anti-money laundering legislation and amendments to the criminal code to criminalize terrorist financing. The GOH should ensure the passage and implementation of the proposed legislation in 2008 to bring its anti-money laundering and counter-terrorist financing regime into greater compliance with international standards. In the interim, the GOH should continue to support the developing law enforcement and regulatory entities responsible for combating money laundering and other financial crimes. It should hire and train more financial crimes investigators and analysts; improve cooperation between police, prosecutors, and the UIF; and ensure that resources are available to strengthen its anti-money laundering regime. The GOH should also resolve any ambiguity regarding the seizure of businesses used for criminal purposes.

Hong Kong

Hong Kong is a major international financial center. Its low taxes and simplified tax system, sophisticated banking system, shell company formation agents, and the absence of currency and exchange controls facilitate financial activity but also make Hong Kong vulnerable to money laundering. The Hong Kong Special Administrative Region Government (HKSARG) considers the primary sources of laundered funds to be corruption (both foreign and domestic), tax evasion, fraud, illegal gambling and bookmaking, prostitution, loan sharking, commercial crimes, and intellectual property rights infringement. Laundering channels include Hong Kong's banking system, legitimate and underground remittance and money transfer networks, trade-based money laundering, and large-ticket consumer purchases—such as property, gold and jewelry. The proceeds from narcotics trafficking are believed to be only a small percentage of illicit proceeds laundered.

Money laundering is a criminal offense in Hong Kong under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO). The money laundering offense extends to the proceeds of drug-related and other indictable crimes. Money laundering is punishable by up to 14 years' imprisonment and a fine of HK \$5,000,000 (approximately U.S. \$641,000).

Money laundering ordinances apply to covered institutions—including banks and nonbank financial institutions—as well as to intermediaries such as lawyers and accountants. All persons must report suspicious transactions of any amount to the Joint Financial Intelligence Unit (JFIU). The JFIU does not investigate suspicious transactions itself but receives, stores, and disseminates suspicious transactions reports (STRs) to the appropriate investigative unit. Typically, STRs are passed to the Narcotics Bureau, the Organized Crime and Triad Bureau of the Hong Kong Police Force, or to the Customs Drug Investigation Bureau of the Hong Kong Customs and Excise Department.

Financial regulatory authorities have issued anti-money laundering guidelines reflecting the revised FATF Forty Recommendations on Money Laundering to institutions under their purview and monitor compliance through on-site inspections and other means. The Hong Kong Monetary Authority (HKMA) is responsible for supervising and examining compliance of financial institutions that are authorized under Hong Kong's Banking Ordinance. The Hong Kong Securities and Futures Commission (SFC) is responsible for supervising and examining compliance of persons that are licensed by the SFC to conduct business in regulated activities, as defined in Schedule 5 of the Securities and Futures Ordinance. The Office of the Commissioner of Insurance (OCI) is responsible for supervising and examining compliance of insurance institutions. Hong Kong law enforcement agencies provide training and feedback on suspicious transaction reporting.

Financial institutions are required to know and record the identities of their customers and maintain records for five to seven years. The filing of a suspicious transaction report cannot be considered a breach of any restrictions on the disclosure of information imposed by contract or law. Remittance agents and moneychangers must register their businesses with the police and keep customer identification and transaction records for cash transactions above a legal threshold for at least six years. A directive from Hong Kong's Monetary Authority (HKMA) reduced this threshold amount from HK \$20,000 (approximately U.S. \$2,565) to HK \$8,000 (approximately U.S. \$1,000), effective January 1, 2007.

Hong Kong does not require reporting of the movement of any amount of currency across its borders, or of large currency transactions above any threshold level. Hong Kong is examining the effectiveness of its existing regime in interdicting illicit cross border cash couriering activities. Reportedly, Hong Kong is deliberating ways of complying with FATF Special Recommendation Nine but does not intend to put in place a "declaration system" and is instead considering a disclosure-based system. Law enforcement agents in Hong Kong are already empowered to seize criminal proceeds anywhere in the jurisdiction, including at the border.

Hong Kong does not make a distinction between onshore and offshore entities, including banks. Its financial regulatory regimes are applicable to residents and nonresidents alike. No differential treatment is provided for nonresidents, including with respect to taxation and exchange controls. The HKMA regulates banks. The Office of Commissioner of Insurance (OCI) and the Securities and Futures Commission (SFC) regulate insurance and securities firms, respectively. All three impose licensing requirements and screen business applicants. There are no legal casinos or Internet gambling sites in Hong Kong.

In Hong Kong, it is not uncommon to use solicitors and accountants, acting as company formation agents, to set up shell or nominee entities to conceal ownership of accounts and assets. Many of the more than 500,000 international business companies (IBCs) created in Hong Kong are established with nominee directors; and many are owned by other IBCs registered in the British Virgin Islands. The concealment of the ownership of accounts and assets is ideal for laundering funds. Additionally, some banks permit shell companies to open bank accounts, based only on vouching by the company formation agent. In such cases, the HKMA's anti-money laundering guidelines require banks to verify the identity of the owners of the company, including beneficial owners. The bank should also assess whether the intermediary is "fit and proper." However, solicitors and accountants have filed a low number of suspicious transaction reports in recent years; and Hong Kong officials seek to improve their reporting through regulatory requirements and oversight.

Hong Kong's open financial system has long made it the primary conduit for funds transferred out of China. Hong Kong's role has been evolving as China's financial system gradually opens. On February 25, 2004, Hong Kong banks began to offer Chinese currency-based (renminbi or RMB) deposit, exchange, and remittance services. Later that year, Hong Kong banks began to issue RMB-based credit cards, which could be used both in Mainland China and in Hong Kong shops that had enrolled

in the Chinese payments system, China Union Pay. In November 2005, Hong Kong banks were permitted modest increases in the scope of RMB business they can offer clients. The new provisions raised daily limits and expanded services. This change brought many financial transactions related to China out of the money-transfer industry and into the more highly regulated banking industry, which is better equipped to guard against money laundering. Banks in Hong Kong are still not permitted to make loans in RMB.

Despite Hong Kong's efforts to encourage capital shifts to the banking industry, Chinese capital controls impel entities in both Hong Kong and Mainland China to use underground financial systems to avoid restrictions on currency exchange. A well-publicized June 2007 raid by Chinese police on an underground bank in Shenzhen resulted in the detention of six suspects, including a Hong Kong-based businesswoman, accused of facilitating the transfer of RMB 4.3 billion (over U.S. \$570 million) out of China since the beginning of 2006—including transfers by Chinese state-owned enterprises. Authorities believe the majority of these funds were used to purchase properties and stocks in Hong Kong. Media reports indicate that such underground exchange houses are rampant in Guangdong province and have transferred more than RMB 200 billion (U.S. \$26.7 billion) out of China since 2006.

Under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO), a court may issue a restraining order against a defendant's property at or near the time criminal proceedings are instituted. Property includes money, goods, real property, and instruments of crime. A court may issue confiscation orders at the value of a defendant's proceeds from illicit activities. Cash imported into or exported from Hong Kong that is connected to narcotics trafficking may be seized, and a court may order its forfeiture. Legitimate businesses can be seized if the business is the "realizable property" of a defendant. Realizable property is defined under the DTRoP and OSCO as any property held by the defendant, any property held by a person to whom the defendant has directly or indirectly made a gift, or any property that is subject to the effective control of the defendant. The Secretary of Justice is responsible for the legal procedures involved in restraining and confiscating assets. There is no time frame ascribed to freezing drug proceeds or the proceeds of other crimes. Regarding terrorist property, a formal application for forfeiture must be made within two years of freezing. Confiscated or forfeited assets and proceeds are paid into general government revenue. In July 2002, the legislature passed several amendments to the DTRoP and OSCO to strengthen restraint and confiscation provisions. These changes, effective January 1, 2003, lowered the evidentiary threshold for initiating confiscation and restraint orders against persons or properties suspected of drug trafficking, eliminated the requirement of actual notice to an absconded offender, eliminated the requirement that the court fix a period of time in which a defendant is required to pay a confiscation judgment, authorized courts to issue restraining orders against assets upon arrest rather than charging, required the holder of property to produce documents and otherwise assist the government in assessing the value of the property, and created an assumption under the DTRoP (to make it consistent with OSCO) that property held within six years of the violation by a person convicted of drug money laundering constitutes proceeds from that money laundering.

According to JFIU figures, as of September 30, 2007, the value of assets under restraint was \$199 million, and the value of assets under a court confiscation order but not yet paid to the government was \$9.85 million. JFIU also reported that, as of September 30, 2007, \$56.5 million had been confiscated and paid to the government since the enactment of DTRoP and OSCO. Hong Kong has shared confiscated assets with the United States.

Hong Kong Customs and Hong Kong Police are responsible for conducting financial investigations. The Hong Kong Police has a number of dedicated units responsible for investigating financial crime, but the primary units responsible for investigating money laundering and terrorist financing are the Commercial Crimes and Narcotics Bureaus in Police Headquarters. There were 157 prosecutions for money laundering during the first 6 months of 2007. Hong Kong Customs had a significant money

laundering case in 2006 in which the mastermind of a local pirated optical disc syndicate was convicted of money laundering involving HK \$27.4 million (U.S. \$3.5 million) accrued over a four-year period from piracy activities. This conviction was upheld on appeal in May 2007. The judge increased the sentence by 50 percent, in accordance with OSCO provisions. Hong Kong Customs arrested two individuals charged with copyright infringement and money laundering in 2007.

The JFIU receives and analyzes STRs to develop information that could aid in prosecuting money laundering cases and, in suitable cases, distributes reports to law enforcement investigating units. The JFIU can refer cases to all Hong Kong law enforcement agencies and, in certain circumstances, to regulatory bodies in Hong Kong as well as to overseas law enforcement bodies. The JFIU also conducts research on money laundering trends and methods and provides case examples (typologies) to financial and nonfinancial institutions to assist them in identifying suspicious transactions. The JFIU has no regulatory responsibilities. Since 1994, when OSCO first mandated the filing of suspicious transaction reports (STRs), the number of STRs received by JFIU has generally increased. In the first nine months of 2007, 12,308 STRs were filed, of which 1798 were referred to law enforcement agencies. This compares with 10,782 STRs filed for the same period in 2006, 13,505 STRs filed during all of 2005, 14,029 filed during 2004, and 11,671 during 2003. The JFIU launched an electronic system for reporting STRs by registered users in late 2006.

On July 3, 2004, the Legislative Council passed the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance. This law is intended to implement UNSCR 1373 and the FATF Special Eight Recommendations on Terrorist Financing in place in July 2004. It extends the HKSARG's freezing power beyond funds to the property of terrorists and terrorist organizations. It also criminalizes the provision or collection of funds by a person intending or knowing that the funds will be used in whole or in part to commit terrorist acts. Hong Kong's financial regulatory authorities have directed the institutions they supervise to conduct record searches for assets of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224.

The People's Republic of China (PRC) represents Hong Kong on defense and foreign policy matters, including UN affairs. Through the PRC, the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism are all applicable to Hong Kong.

To help deal with anti-money laundering (AML) issues from a practical perspective and reflect business needs, the Hong Kong Monetary Authority (HKMA) has recently coordinated the establishment of an Industry Working Group on AML. The Group, which includes representatives of some 20 authorized institutions, has met twice. Three subgroups have been established to share experiences and consider the way forward on issues such as PEPs (politically exposed persons), terrorist financing, transaction monitoring systems and private banking issues. The subgroup on Customer Due Diligence (CDD) issued guidelines on issues related to PEPs in November 2007. The HKMA has also implemented a number of initiatives on AML issues, including issuing circulars and guidance to authorized institutions on combating the financing of weapons of mass destruction conducting in-depth examinations of institutions' AML controls and setting out best practices for AML in high-risk areas—such as correspondent banking, private banking, and remittance.

The HKMA circulated guidelines that require banks to maintain a database of terrorist names and management information systems to detect unusual patterns of activity in customer accounts. The Securities and Futures Commission (SFC) and the Office of the Commissioner of Insurance (OCI) circulated guidance notes in 2005 that provided additional guidance on CDD and other issues, reflecting the new requirements in the Revised FATF Forty Recommendations on Money Laundering and Special Recommendations on Terrorist Financing. In 2006, the OCI and the SFC revised their guidance notes to take into account the latest recommendations by the FATF.

Other bodies governing segments of the financial sector are also engaged in advancing anti-money laundering efforts. The Hong Kong Estates Agents Authority, for instance, has drawn up specific guidelines for real estate agents on filing suspicious transaction reports; and the Law Society of Hong Kong and the Hong Kong Institute of Certified Public Accountants are in the process of drafting such guidance for their members.

Hong Kong is an active member of the Financial Action Task Force's FATF and Offshore Group of Banking Supervisors and was a founding member of the Asia Pacific Group on Money Laundering (APG).

In November 2007, the APG and FATF conducted a site visit as part of their joint mutual evaluation of Hong Kong. The mutual evaluation report will be discussed at FATF's June 2008 Plenary

Hong Kong's banking supervisory framework is in line with the requirements of the Basel Committee on Banking Supervision's "Core Principles for Effective Banking Supervision." Hong Kong's JFIU is a member of the Egmont Group and is able to share information with its international counterparts. Hong Kong is known to cooperate with foreign jurisdictions in combating money laundering.

Hong Kong's mutual legal assistance agreements generally provide for asset tracing, seizure, and sharing. Hong Kong signed and ratified a mutual legal assistance agreement (MLAA) with the United States that came into force in January 2000. Hong Kong has MLAA's with 22 other jurisdictions. Hong Kong has also signed surrender-of-fugitive-offenders (extradition) agreements with 17 countries, including the United States, and has signed agreements for the transfer of sentenced persons with ten countries, also including the United States. Hong Kong authorities exchange information on an informal basis with overseas counterparts and with Interpol.

The Government of Hong Kong should further strengthen its anti-money laundering regime by establishing threshold reporting requirements for currency transactions and putting into place "structuring" provisions to counter evasion efforts. Per FATF Special Recommendation IX, Hong Kong should also establish mandatory cross-border currency reporting requirements. Hong Kong should continue to encourage more suspicious transaction reporting by lawyers and accountants, as well as by business establishments, such as auto dealerships, real estate companies, and jewelry stores. Hong Kong should also take steps to stop the use of "shell" companies, IBCs, and other mechanisms that conceal the beneficial ownership of accounts by more closely regulating corporate formation agents. Particularly, since Hong Kong is a major trading center, Hong Kong law enforcement and customs authorities should seek to address trade-based money laundering.

Hungary

With an advantageous and pivotal location in central Europe, a cash-based economy and a well-developed financial services industry, criminal organizations from countries such as Russia and Ukraine have reportedly entrenched themselves in Hungary. Money laundering is related to a variety of criminal activities, including illicit narcotics trafficking, prostitution, trafficking in persons, and organized crime. Other prevalent economic and financial crimes include real estate fraud and the copying/theft of bankcards. Financial crime reportedly has not increased in recent years though there have been some isolated, albeit well-publicized, cases.

Hungary has worked continuously to improve its money laundering enforcement regime following its 2003 removal from the Financial Action Task Force (FATF) list of Non-Cooperative Countries and Territories. Since then, it has worked to implement the FATF Forty Recommendations and the Nine Special Recommendations on Terrorist Financing. In early 2005, the International Monetary Fund (IMF), in conjunction with the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), conducted the third-round mutual evaluation of Hungary's anti-money laundering and counter-terrorist financing (AML/CTF) regime. Of the FATF

49 Recommendations, Hungary received 38 ratings of “largely compliant” or better. Since the evaluation, Hungarian authorities have been committed to full implementation of the IMF/MONEYVAL recommendations to address deficiencies in its AML/CTF framework and implementation.

Hungary banned offshore financial centers, including casinos, by Act CXII of 1996 on Credit Institutions. Hungary discontinued its preferential tax treatment for offshore centers at the end of 2005; and in 2006 these companies automatically became Hungarian companies. The only special status they retain is the ability to keep financial records in foreign currencies. Hungary no longer permits the operation of free trade zones.

Act CXII of 1996 on Credit Institutions bans the use of any indigenous alternative remittance systems that bypass, in whole or in part, financial institutions. Act CXX of 2001 eliminated bearer shares and required that all such shares be transferred to identifiable shares by the end of 2003. All shares now are subject to transparency requirements, and both owners and beneficiaries must be registered.

The Government of Hungary (GOH) has prohibited the use of anonymous savings booklets since 2001. Act CXX of 2001 eliminated bearer shares and required that all such shares be transferred to identifiable shares by the end of 2003. All shares are now subject to transparency requirements, and all owners and beneficiaries must be registered. By mid-2003, Hungary had successfully transferred 90 percent of anonymous savings accounts into identifiable accounts. Individuals with remaining anonymous passbook accounts now need written permission from the police to access their accounts. The total balance remaining in anonymous accounts is approximately 20 million euros (approximately U.S. \$29.5 million) for 2.5 million owners. This total is mainly comprised of accounts for which savings booklets were lost, accounts whose holders have not proceeded with the conversion nor tried to make a withdrawal, and accounts whose original owners have died and their heirs do not know how to access the funds.

The European Union’s Third Money Laundering Directive (Directive 2005/60/EC of the European Parliament and of the Council of October 26, 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing) entered into force in December 2005 with member states required to enact the laws, regulations and administrative provisions necessary to comply with this Directive by December 15, 2007. The EU’s Third Directive, which is consistent with the FATF 40 Recommendations and Nine Special Recommendations, necessitated that Hungary re-codify its original money laundering legislation, Act XV of 2003 on the Prevention and Impeding of Money Laundering. Hungary amended the legislation, and the implementing regulations entered into force in August 2006. These measures ensure the uniform implementation of the EU Directive with regard to the definition of “politically exposed persons” (PEPs), the technical criteria for simplified customer due diligence procedures, and exemptions for financial activity conducted on an occasional or very limited basis.

On November 19, 2007, the Parliament adopted Act CXXXVI on the Prevention and Combating of Money Laundering and Terrorist Financing (AML/CTF Act) and published the AML/CTF Act on November 28, 2007. The AML/CTF Act entered into force on December 15, 2007.

The AML/CTF Act establishes the legislative framework for the prevention and combat of terrorist financing and complies with international AML standards and requirements. The AML/CTF Act expands its scope to cover the following professions: financial services, investment services, insurance industry, commodity exchange services, postal money order and transfers, real estate agents, auditors, accountants, tax advisors, casinos, jewelry, lawyers, and notaries. The AML/CTF Act introduces more specific and detailed provisions relating to customer and beneficial owner identification and verification. The Act introduces a risk-sensitive approach regarding customer due diligence (CDD) and establishes detailed rules for CDD, including simplified as well as enhanced CDD for low or high-risk customers or business relationships, appropriate procedures to determine whether a person is a

PEP, and other requirements. Regulation (EC) No 1781/2006 of the European Parliament and of the Council of November 15, 2006 regarding originator information accompanying transfers of funds entered into force on the January 1, 2007. Hungary has implemented the regulation's requirements in the AML/CTF Act.

Obligated entities must send a suspicious transaction report (STR) to the financial intelligence unit (FIU) and suspend the transaction if there is suspicion of money laundering or terrorist financing. The AML/CTF Act sets out the requirements for disclosure of information, and mandates the keeping of statistics so that the effectiveness of the AML/CTF measures can be evaluated. The Act contains provisions on the internal procedures, training and internal communication, detailing special protocols for lawyers and notaries. Safe harbor provisions protect individuals when executing their AML/CTF reporting obligations.

Only banks or their authorized agents can operate currency exchange booths, of which there are approximately 300 in Hungary. These exchange houses are subject to "double supervision," because they are subject to both the banks' internal control mechanisms, as well as to supervision by the HFSA. In addition, the AML/CTF Act contains threshold-reporting requirements for currency exchange enterprises. Exchange booths must verify customer identity for currency exchange transactions totaling or exceeding 500,000 forints (approximately U.S. \$3,000), whether in single transaction or derived from consecutive separate transactions. Exchange booths must file STRs for suspicious transactions in any amount.

Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of October 26, 2005 on controls of cash entering or leaving the Community addresses FATF Special Recommendation Nine regarding cash couriers. The regulation requires travelers to make a declaration to the competent authorities of all movement of cash reaching or exceeding 10,000 euros (approximately U.S. \$15,000). Act No. XLVIII of 2007 on the promotion of the Regulation states that based on the EC regulation, the Hungarian customs authorities should record the information obtained under Article 3 (Obligation to declare) as well as the data collected in connection with any inspection of the declaration. If the data suggests money laundering or terrorist financing, the Hungarian Customs and Finance Guard (HCFG) must immediately send an STR to the financial intelligence unit (FIU).

A new provision on the money laundering offence [Section 303 of the Hungarian Criminal Code (HCC) after the amendment by Act XXVII of 2007] brings Hungary into compliance with the Vienna and Palermo Conventions by enlarging the scope of the money laundering offence to cover the transfer of proceeds to a third party even if it is carried out through a nonbanking or nonfinancial transaction. Act XXVII of 2007 also addresses problems that have occurred with the AML reporting regime. Strict criminal penalties for nonreporting have resulted in over-filing by Hungarian financial institutions. This, in turn, has resulted in a high volume of STRs that are reportedly of low quality. Act XXVII of 2007 reduces the maximum punishment for intentional noncompliance with reporting obligations from three years imprisonment to two years imprisonment. Hungary has also abolished the negligent form of nonreporting as a criminal offence. Section 9 of Act XXVII of 2007 includes provisions punishing individual financing of terrorist acts. In January 2008, Act XIX of 1998 on the Hungarian Criminal Procedure was amended. This amendment transferred the authority to investigate money laundering crimes and noncompliance with the AML/CTF Act from the Hungarian National Police (HNP) to the HCFG.

Hungary's financial regulatory body, the Hungarian Financial Supervisory Authority (HFSA), supervises financial service providers with the exception of cash processors, which are supervised by the National Bank of Hungary. The Hungarian Tax and Financial Control Administration supervises casinos. The FIU supervises most designated nonfinancial businesses and professions (DNFBPs), such as real estate agents, accountants and tax advisors. Supervisory functions are performed by self-regulatory bodies in certain cases: the Hungarian Bar Association with respect to lawyers, the

Money Laundering and Financial Crimes

Hungarian Association of Notaries Public with respect to notaries public, and by the Chamber of Hungarian Auditors and Auditing Activities with respect to auditors. The Hungarian Trade Licensing Office is the supervisory authority with respect to the natural and legal persons trading in goods and allowing cash payments above the amount of 3.6 million forints (approximately U.S. \$20,000).

In 2006, the HFSA established a new division to deal with money laundering and financial crimes. The division coordinates supervisory tasks related to money laundering and terrorist financing and also assists other departments of the HFSA with on-site inspections. In 2007, the HFSA enlarged the staff of its Financial Forensic division. One of the HFSA's major undertakings in 2007 was its participation in the implementation of the Third EU Directive on AML/CTF. The HFSA established a standing AML/CTF working group with the participation of the representatives of financial institutions and their associations.

Hungary's FIU, the National Bureau of Investigation's Anti-Money Laundering Department (ORFK), was originally a unit under the HNP. The FIU serves as the national center for receiving and analyzing STRs and other information regarding potential money laundering or terrorist financing, and disseminating them to the competent authorities. As a law-enforcement style FIU, the ORFK has the authority to itself investigate money laundering cases. From January 1, 2007 until December 15, 2007 the FIU received 9,475 STRs, opened 40 cases, and confiscated 971,681,352 forints (approximately U.S. \$5.5 million). In 2006, the FIU received 9,999 STRs, and opened 193 cases based upon STRs received.

As of December 15, 2007, the ORFK has undergone substantial organizational changes. It has moved from its current position within the HNP to the Hungarian Customs Authority. Although the ORFK still exists and receives STR data, its future operational capacity under the Hungarian Customs Authority remains unclear. The FIU's move to the Customs Authority has caused a significant reduction in information exchange with international counterparts. The Egmont Group of FIUs has decided to temporarily suspend information exchange with the ORFK, pending further clarification of the structural changes within the FIU.

The Hungarian Criminal Code (HCC), Act IV of 1978 contains a provision on asset forfeiture. Under this provision, assets used to commit crimes, pose a danger to public safety, or derive from criminal activity, are subject to forfeiture. All property related to criminal activity during the interval when its owner was involved with a criminal organization can be confiscated, unless the owner proves it was acquired legally. For most crimes, the police or FIU first freeze the assets and inform the bank within 24 hours whether they will pursue an investigation. A court ruling determines forfeiture and seizure for all crimes, including terrorist financing. The banking community has cooperated fully with enforcement efforts to trace funds and seize and freeze bank accounts. If the owner of the assets requests it, and the FIU approves the request, the frozen assets may be released on the basis of financial need, such as health-related expenses or basic sustenance,

Act IV of 1978, Article 261, criminalizes terrorist acts. Hungary has criminalized terrorism and all forms of terrorist financing with Act II of 2003, which modifies Criminal Code Article 261. Section 261 of the HCC, amended by Act XXVII of 2007, states that any person sponsoring activities of a terrorist or a terrorist group by providing material assets or any other support faces two to ten years imprisonment. The HFSA provides access for supervised institutions as well as for the general public on its homepage to access updates to the UN 1373 Sanctions Committee Consolidated List and its equivalent EU list, as well as the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. Terrorist finance-related assets can be frozen. The Act XIX of 1998 on Criminal Procedures, Articles 151, 159, and 160, provide for the immediate seizure, sequestration, and precautionary measures against terrorist assets.

Hungary and the United States have a Mutual Legal Assistance Treaty and a nonbinding information sharing arrangement designed to enable U.S. and Hungarian law enforcement to work more closely to

fight organized crime and illicit transnational activities. In May 2000, Hungary and the U.S. Federal Bureau of Investigation established a joint task force to combat Russian organized crime groups. Hungary has signed bilateral agreements with 41 other countries to cooperate in combating terrorism, drug trafficking, and organized crime.

Hungary is a member of the MONEYVAL Committee, a FATF-style regional body (FSRB). Hungary's FIU is a member of the Egmont Group; however, information exchanges within this body have been suspended pending the finalization of the FIU's reorganization and new functions. Hungary is a party to the UN International Convention for the Suppression of the Financing of Terrorism; the UN Convention against Transnational Organized Crime; the 1988 UN Drug Convention; and the UN Convention against Corruption.

Hungary has strengthened its legal and institutional background, and has made a significant progress regarding international communication and cooperation as well as training for the service providers who face money laundering and terrorist financing risks. Despite this progress, the GOH needs to continue its efforts with regard to implementation. An increased level of cooperation and coordination among the different law enforcement entities involved in fighting financial crime should be pursued. Prosecutors, judges, and police require enhanced knowledge to promote the successful prosecution of money laundering cases. The police and FIU should also have the option to extend their 24-hour time limit for the freezing of assets. The HFSA and other supervisory bodies should improve supervision and provide increased outreach and guidance to financial institutions with regard to reporting obligations. Hungary should re-criminalize negligent nonreporting of suspicious activities and transactions. The GOH should take steps to ensure that nonbank financial institutions file STRs. Increased AML/CTF training for the employees of financial institutions and other obliged entities is also necessary to improve the quality of STRs filed, in particular those which may be related to the financing of terrorism. The GOH should distribute the updates of the UN designated terrorist lists to the obliged entities, and not rely on posting updates online.

India

India's emerging status as a regional financial center, its large system of informal cross-border money flows, and its widely perceived tax avoidance problems all contribute to the country's vulnerability to money laundering activities. Some common sources of illegal proceeds in India are narcotics trafficking, illegal trade in endangered wildlife, trade in illegal gems (particularly diamonds), smuggling, trafficking in persons, corruption, and income tax evasion. Historically, because of its location between the heroin-producing countries of the Golden Triangle and Golden Crescent, India continues to be a drug-transit country.

India's strict foreign-exchange laws and transaction reporting requirements, combined with the banking industry's due diligence policy, make it increasingly difficult for criminals to use formal channels like banks and money transfer companies to launder money. However, large portions of illegal proceeds are often laundered through "hawala" or "hundi" networks or other informal money transfer systems. Hawala is an alternative remittance system that is popular among not only immigrant workers, but all strata of Indian society. Hawala transaction costs are less than the formal sector; hawala is perceived to be efficient and reliable; the system is based on trust and it is part of the Indian culture. According to Indian observers, funds transferred through the hawala market are equal to between 30 to 40 percent of the formal market. The Reserve Bank of India (RBI), India's central bank, estimates that remittances to India sent through legal, formal channels in 2006-2007 amounted to U.S. \$28.2 billion. Due to the large number of expatriate Indians in North America and the Middle East, India continues to retain its position as the leading recipient of remittances in the world, followed by China and Mexico.

Many Indians, especially among the poor and illiterate, do not trust banks and prefer to avoid the lengthy paperwork required to complete a money transfer through a financial institution. The hawala system can provide the same remittance service as a bank with little or no documentation and at lower rates and provide anonymity and security for their customers. Hawala is also used to avoid currency restrictions, assists in capital flight, facilitates tax evasion, and avoids government scrutiny in financial transactions. The Government of India (GOI) neither regulates hawala dealers nor requires them to register with the government. The RBI argues that hawala dealers cannot be regulated since they operate illegally and therefore cannot be registered. Indian analysts also note that hawala operators are often protected by some politicians.

However, the Indian government is attempting to regulate a broader swath of the financial sector. In December 2005, the RBI issued guidelines requiring financial institutions, including money changers, to follow “know your customer” (KYC) guidelines and maintain transaction records for the sale and purchase of foreign currency. Foreigners and Nonresident Indians are permitted to receive cash payments up to U.S. \$3,000 or its equivalent in other currencies from moneychangers. Recently, the RBI has been taking additional steps to crack down on unlicensed money transmitters and increase monitoring of nonbanking money transfer operations like currency exchange kiosks and wire transfer services. In September 2007, the RBI asked Western Union’s Indian-based subsidiary, Western Union Services India, to desist from appointing any more sub-agents until further instruction. Western Union officials have explained to U.S. government officials that this is due to a new policy the Ministry of Home Affairs (MHA) is formulating to require wire transfer businesses to perform due diligence on sub-agents and seek RBI and MHA approval before appointing new sub-agents.

Historically, in Indian hawala transactions, gold has been one of the most important commodities. There is a widespread cultural demand for gold in India and South Asia. Since the mid-1990s, India has liberalized its gold trade restrictions. In recent years, the growing Indian diamond trade has been considered an important factor in providing counter-valuation; a method of “balancing the books” in external hawala transactions. Invoice manipulation is also used extensively to avoid both customs duties, taxes, and to launder illicit proceeds through trade-based money laundering.

India has illegal black market channels for selling goods. Smuggled goods such as food items, computer parts, cellular phones, gold, and a wide range of imported consumer goods are routinely sold through the black market. By dealing in cash transactions and avoiding customs duties and taxes, black market merchants offer better prices than those offered by regulated merchants. However, due to trade liberalization, the rise in foreign companies working and investing in India, and increased government monitoring, the business volume in smuggled goods has fallen significantly. In the last 10-15 years, most products previously sold in the black market are now traded through lawful channels.

With tax evasion a widespread problem in India, the GOI is gradually making changes to the tax system. The government now requires individuals to use a personal identification number to pay taxes, purchase foreign exchange, and apply for passports. The GOI also introduced a central value added tax (VAT) in April 2005 which replaced numerous complicated state sales taxes and excise taxes with one national uniform VAT rate. As a result, the incentives and opportunities for entrepreneurs and businesses to conceal their sales or income levels have been reduced. Except for Uttar Pradesh, all Indian states have implemented the national VAT mandate. Uttar Pradesh announced in late October 2007 that it would also implement the VAT.

In the aftermath of September 11, India joined the global community in addressing concerns about money laundering and terrorist finance by implementing the Prevention of Money Laundering Act (PMLA) in January 2003. The PMLA criminalized money laundering, established fines and sentences for money laundering offenses, imposed reporting and record keeping requirements on financial institutions, provided for the seizure and confiscation of criminal proceeds, and established a financial

intelligence unit (FIU). In July 2005, the PMLA's implementing rules and regulations were promulgated. The legislation outlines predicate offenses for money laundering. Predicate offenses are listed in a schedule to the Act, but these do not include many of the predicate offenses listed as essential by the FATF Recommendations, including organized crime, fraud, smuggling and insider trading. Penalties for offenses under the PMLA are severe and may include imprisonment for three to seven years and fines as high as U.S. \$12,500. If the money laundering offense is related to a drug offense under the Narcotic Drugs and Psychotropic Substances Act (NDPSA), imprisonment can be extended to a maximum of ten years. The PMLA mandates that banks, financial institutions, and intermediaries of the securities market (such as stock market brokers) maintain records of all cash transactions (deposits/withdrawals, etc.) exceeding U.S. \$25,000 and keep a record of all transactions dating back 10 years.

The Criminal Law Amendment Ordinance allows for the attachment and forfeiture of money or property obtained through bribery, criminal breach of trust, corruption, or theft, and of assets that are disproportionately large in comparison to an individual's known sources of income. The 1973 Code of Criminal Procedure, Chapter XXXIV (Sections 451-459), establishes India's basic framework for confiscating illegal proceeds. The NDPSA of 1985, as amended in 2000, calls for the tracing and forfeiture of assets that have been acquired through narcotics trafficking and prohibits attempts to transfer and conceal those assets. The Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act of 1976 (SAFEMA) also allows for the seizure and forfeiture of assets linked to Customs Act violations. The Competent Authority (CA), within the Ministry of Finance (MOF), administers both the NDPSA and the SAFEMA.

The 2001 amendments to the NDPSA allow the CA to seize any asset owned or used by an accused narcotics trafficker immediately upon arrest. Previously, assets could only be seized after a conviction. Even so, Indian law enforcement officers lack knowledge of the procedures for identifying individuals who might be subject to asset seizure/forfeiture and in tracing assets to be seized. They also appear to lack sufficient knowledge in drafting and expeditiously implementing asset freezing orders. In 2005, pursuant to the NDPSA and with U.S. government funding through its Letter of Agreement (LOA) with India, the CA began training law enforcement officials on asset forfeiture laws and procedures. CA has since held ten asset seizure and forfeiture workshops in New Delhi, Himachal Pradesh, Uttar Pradesh, Rajasthan, Andhra Pradesh, Karnataka and Assam. CA reports that the workshops have led to increased seizures and forfeitures. In 2007, the joint U.S./GOI Project Implementation Committee provided additional funds so that the Competent Authority could expand its training.

One of the GOI's principal provisions in combating money laundering is the Foreign Exchange Management Act (FEMA) of 2000. The FEMA's objectives include establishing controls over foreign exchange, preventing capital flight, and maintaining external solvency. FEMA also imposes fines on unlicensed foreign exchange dealers. Related to the FEMA is the Conservation of Foreign Exchange and Prevention of Smuggling Act (COFEPOSA), which provides for preventive detention in smuggling and other matters relating to foreign exchange violations. The MOF's Directorate of Enforcement (DOE) enforces the FEMA and COFEPOSA. The RBI also plays an active role in the regulation and supervision of foreign exchange transactions.

In April 2002, the Indian Parliament also passed the Prevention of Terrorism Act (POTA), which criminalizes terrorist financing, among other provisions. In March 2003, the GOI announced that it had charged 32 terrorist groups under the POTA. In July 2003, the GOI arrested 702 persons under the POTA. In November 2004, due to concerns that the overall law permitted overreaching police powers not related to the terrorist financing provisions, the Parliament repealed the POTA and amended the Unlawful Activities (Prevention) Act 1967 (UAPA) to include the POTA's salient elements such as criminalization of terrorist financing.

Money Laundering and Financial Crimes

As part of the PMLA mandate, India's FIU was established in January 2006 to combat money laundering and terrorist financing. The FIU is responsible for receiving, processing, analyzing, and disseminating cash and suspicious transaction reports from financial institutions, banking companies, and intermediaries of the securities market. Over the last two years, the FIU has become fully operational and disseminates report analysis to law enforcement, investigative, and intelligence officers to investigate and prevent money laundering and curb financial crimes. The FIU has a staff of forty-three officers, headed by an Indian Administrative Service Director of equal rank to a Joint Secretary in the GOI ministries.

As of September 2007, FIU received more than 1800 suspicious transaction reports (STRs), of which about 800 were shared with relevant enforcement agencies. According to FIU officials, income tax evasion has been readily detected in the STRs and has also led to the arrest of suspected terror operatives. Reporting entities have immunity from civil proceedings for disclosures to FIU. The FIU also receives threat information and leads from foreign intelligence agencies concerning terrorists, terrorist groups, and international financial crimes information. Cash smuggling reports, which are prepared by Customs and the Enforcement Directorate, are not disclosed to the FIU but are shared with them indirectly on a need to know basis.

The FIU is an independent body reporting directly to the Economic Intelligence Council (EIC), which is headed by the Finance Minister. For administrative purposes, the FIU's operations are supervised by the MOF's Department of Revenue. While the FIU receives processes, analyzes, and disseminates information relating to suspect financial transactions to enforcement agencies and foreign FIUs, the unit does not have criminal enforcement, investigative, or regulatory powers. In 2007, the FIU initiated a project to adopt industry best practices and appropriate technology for creating an Information Technology Integrator. The integrator will process financial intelligence and alert on suspicious transactions.

In June 2007, India's FIU was admitted as a member of the Egmont Group. Admission of India's FIU as a member of the Egmont Group is seen by Indian officials as a major step forward in India joining the international community in its fight against money laundering and terrorist financing. FIU officials have expressed an interest in signing bilateral MOUs with foreign FIUs to facilitate sharing of money laundering information.

Under the MOF, the Enforcement Directorate is responsible for investigations and prosecutions of money laundering cases. In 2006-2007, the Enforcement Directorate initiated investigations into 38 cases of money laundering, eight of which were related to terrorist financing. The directorate has made seven seizure cases of properties worth \$436,000. Headquartered in New Delhi, the directorate has seven zonal offices in Mumbai, Kolkata, Delhi, Jalandhar, Chennai, Ahmedabad, and Bangalore. In addition to the MOF, the Central Bureau of Investigation (CBI), the Directorate of Revenue Intelligence (DRI), Customs and Excise, RBI, and the CA are involved in GOI's anti-money laundering efforts.

The CBI is a member of INTERPOL. All state police forces and other law enforcement agencies have a link through INTERPOL/New Delhi to their counterparts in other countries for purposes of criminal investigations. India's Customs Service is a member of the World Customs Organization and shares enforcement information with countries in the Asia/Pacific region.

To assist in enhancing coordination among various enforcement agencies and directorates at the MOF, the GOI has established an Economic Intelligence Council (EIC). This provides a forum to strengthen intelligence and operational coordination, to formulate common strategies to combat economic offenses, and to discuss cases requiring interagency cooperation. In addition to the central EIC, there are eighteen regional economic committees in India. The Central Economic Intelligence Bureau (CEIB) functions as the secretariat for the EIC in the MOF. The CEIB interacts with the National

Security Council, the Intelligence Bureau, and the Ministry of Home Affairs on matters concerning national security and terrorism.

In October 2006, the MOF started the process to reconcile its list of predicate crimes under the PMLA with that of international FATF recommendations. Having made some progress towards that commitment, India gained FATF observer status in February 2007 and has a two-year probationary period to adopt FATF core recommendations towards gaining full membership. As defined by FATF, this includes criminalization of money laundering, customer due diligence, record-keeping, suspicious transaction reporting, criminalization of terrorist financing, and suspicious transaction reporting relating to terrorist financing, as well as expressing a political commitment to international standards for anti-money laundering. India is a member of the Asia/Pacific Group (APG) on Money Laundering, a FATF-style regional body.

The MOF is leading an inter-ministerial effort to amend the PMLA to meet FATF requirements. At present, the PMLA does not include comprehensive provisions on terrorist financing, and the required legislative amendments to the PMLA are still awaiting Cabinet approval before moving to Parliament for enactment. MOF officials have stated that changes to the PMLA will include incorporating provisions of the UAPA that criminalize terrorist financing, adopt most FATF recommended categories for predicate offenses, and implement reporting requirements for money changers, money transfer service providers, and casinos.

The Securities and Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority and the National Housing Board have also adopted anti-money laundering policies. SEBI has also issued a circular to all registered intermediaries on their obligations as financial institutions to prevent money laundering. This includes guidelines on maintaining records, preserving sensitive information with respect to certain transactions, and reporting suspicious cash flows and financial transactions to the FIU.

Prompted by the RBI's 2002 notice to commercial banks to adopt due diligence rules, many of these institutions have taken steps to combat money laundering. For example, most private banks and several public banks have hired anti-money laundering compliance officers to design systems and training to ensure compliance with these regulations. The Indian Bankers Association has also established a working group to develop self-regulatory anti-money laundering procedures and assist banks in adopting the mandated rules.

The RBI and SEBI have worked together to tighten regulations, strengthen supervision, and ensure compliance with KYC norms, which were implemented in December 2005. This includes, for example, provisions that banks must identify politically involved account holders who reside outside of India and identify the source of these funds before accepting deposits of more than U.S. \$10,000. The RBI continues to update its due diligence guidelines based on FATF recommendations. For banks that are found noncompliant, the RBI has the power to order banks to freeze assets.

Banks are required to file STRs with FIU. Banks have installed software to enable their internal controllers to better monitor accounts for any unusual relationship between the size of the deposit and the turnover in the account and for matching names of terrorists and terrorist-associated countries. All banks have been advised by RBI that they should guard against establishing relationships with foreign financial institutions that permit their accounts to be used by shell companies. The UNSCR 1267 Sanctions Committee's consolidated list is routinely circulated to all financial institutions.

India does not have an offshore financial center but does license offshore banking units (OBUs). These OBUs are required to be predominantly owned by individuals of Indian nationality or origin resident outside India. The OBUs include overseas companies, partnership firms, societies, and other corporate bodies. OBUs must be audited to confirm that ownership by a nonresident Indian is not less than 60 percent. These entities are susceptible to money laundering activities, in part because of a lack of

stringent monitoring of transactions in which they are involved. Finally, OBU's must be audited financially; however, the auditing firm is not required to obtain government approval.

GOI regulations governing charities remain antiquated and the process by which charities are governed at the provincial and regional levels is weak. The GOI does require charities to register with the state-based Registrar of Societies, and, if seeking tax exempt status, they must apply separately with the Exemptions Department of the Central Board of Direct Taxes. There are no guidelines or provisions governing the oversight of charities for anti-money laundering or counter-terrorist financing (AML/CTF) purposes, and there is insufficient integration and coordination between charities' regulators and law enforcement authorities regarding the threat of terrorist finance. The Foreign Contribution Regulation Act (FCRA) of 1976, supervised by the MHA, regulates the use of foreign funds received by charitable/nonprofit organizations.

The GOI is a party to the 1988 UN Drug Convention. It is a signatory to, but has not yet ratified, the UN Convention against Transnational Organized Crime or the UN Convention against Corruption. India is a party to the UN International Convention for the Suppression of the Financing of Terrorism. India has signed and ratified a number of mutual legal assistance treaties with many countries, including the United States.

The Government of India should move forward expeditiously with amendments to the PMLA that explicitly criminalize terrorist financing, and expand the list of predicate offenses so as to meet FATF's core recommendations. Further steps in tax reform will also assist in negating the popularity of hawala and in reducing money laundering, fraud, and financial crimes. The GOI should ratify the UN Conventions against Transnational Organized Crime and Corruption. The GOI needs to promulgate and implement new regulations for nongovernment organizations including charities. Given the number of terrorist attacks in India and the fact that in India hawala is directly linked to terrorist financing, the GOI should prioritize cooperation with international initiatives that provide increased transparency in alternative remittance systems. India should devote more law enforcement and customs resources to curb abuses in the diamond trade. It should also consider the establishment of a Trade Transparency Unit (TTU) that promotes trade transparency; in India, trade is the "back door" to underground financial systems. The GOI also needs to strengthen regulations and enforcement targeting illegal transactions in informal money transfer channels.

Indonesia

Although neither a regional financial center nor an offshore financial haven, Indonesia is vulnerable to money laundering and terrorist financing due to a poorly regulated financial system, cash-based economy, the lack of effective law enforcement, and widespread corruption. Most money laundering in the country is connected to nondrug criminal activity such as gambling, prostitution, bank fraud, theft, credit card fraud, maritime piracy, sale of counterfeit of goods, illegal logging, and corruption. Indonesia also has a long history of smuggling, a practice facilitated by thousands of miles of unpatrolled coastline and law enforcement and customs infrastructure riddled with corruption. The proceeds of illicit activities are easily parked offshore and only repatriated as required for commercial and personal needs.

In June 2001, the Financial Action Task Force (FATF) added Indonesia to its list of Non-Cooperative Countries and Territories (NCCT). This designation was due to a number of serious deficiencies in Indonesia's Anti-Money Laundering (AML) framework including the lack of a basic set of AML provisions and the failure to criminalize money laundering. As a result of Indonesia's enactment of relevant AML legislation and its ongoing efforts to implement reforms to its AML regime, the FATF removed Indonesia from its NCCT list on February 11, 2005.

In April 2002, Indonesia passed Law No. 15/2002 Concerning the Crime of Money Laundering, making money laundering a criminal offense. The law identifies 15 predicate offenses related to money laundering, including narcotics trafficking and most major crimes. Law No. 15/2002 established the Financial Transactions Reports and Analysis Centre (PPATK), Indonesia's financial intelligence unit (FIU) to develop policy and regulations to combat money laundering and terrorist financing.

Law No. 15/2002 stipulated important provisions to enhance Indonesia's anti-money laundering regime, such as: obligating financial service providers to submit suspicious transactions reports and cash transaction reports; exempting reporting, investigation and prosecution of criminal offenses of money laundering from the provisions of bank secrecy that are stipulated in Indonesia's banking law; placing the burden of proof on the defendant; establishing the PPATK as an independent agency with the duty and the authority to prevent and eradicate money laundering; and establishing a clear legal basis for freezing and confiscating the proceeds of crime.

In September 2003, Parliament passed Law No. 25/2003, amending Law No. 15/2002, to further address FATF's concerns. Law No. 25/2003 provides a new definition for the crime of money laundering, making it an offense for anyone to deal intentionally with assets known, or reasonably suspected, to constitute proceeds of crime with the purpose of disguising or concealing the origin of the assets. The amendment removes the threshold requirement for proceeds of crime. The amendment further expands the scope of regulations by expanding the definition of reportable suspicious transactions to include attempted or unfinished transactions. The amendment also shortens the time to file an STR to three days or less after the discovery of an indication of a suspicious transaction. However, there is no clear legal obligation to report STRs related to terrorist financing. The amendment makes it an offense to disclose information about the reported transactions to third parties, which carries a penalty of imprisonment for a maximum of five years and a maximum fine of one billion rupiah (approximately U.S. \$105,000).

Additionally, Articles 44 and 44A of Law 25/2003 provide for mutual legal assistance with respect to money laundering cases, with the ability to provide assistance using the compulsory powers of the court. Article 44B imposes a mandatory obligation on the PPATK to implement provisions of international conventions or international recommendations on the prevention and eradication of money laundering. In March 2006, the GOI expanded Indonesia's ability to provide mutual legal assistance by enacting the first Mutual Legal Assistance (MLA) Law (No. 1/2006), which establishes formal, binding procedures to facilitate MLA with other states.

A proposed second amendment to the AML law was submitted to the parliament in October 2006. If passed, it would require nonfinancial service businesses and professionals who potentially could be involved in money laundering, such as car dealers, real estate companies, jewelry traders, notaries and public accountants, to report suspicious transactions. The amendments also would include civil asset forfeiture and give more investigative powers to the PPATK, as well as the authority to block financial transactions suspected of being related to money laundering. Despite these provisions, the draft amendments appear to have remaining gaps when measured against current AML/CTF international standards.

Indonesia's FIU, PPATK, established in April 2002, became operational in October 2003 and continues to make progress in developing its human and institutional capacity. The PPATK is an independent agency that receives, analyzes, and evaluates currency and suspicious financial transaction reports, provides advice and assistance to relevant authorities, and issues publications. As of November 2007 the PPATK had received approximately 12,000 suspicious transactions reports (STRs) from 112 banks, seven rural banks, and 82 nonbank financial institutions. Approximately 5,000 of these STRs were received during 2007. The agency also reported that it had received a total of over four million cash transaction reports (CTRs) from 132 banks, 48 moneychangers, 35 rural

banks, five insurance companies, and two securities companies. PPATK have submitted a total of 521 cases to various law enforcement agencies based on their analysis of 882 STRs.

The PPATK actively pursues broader cooperation with relevant GOI agencies. The PPATK has signed a total of 16 domestic memoranda of understanding (MOUs) to assist in financial intelligence information exchange with the following entities: Attorney General's Office (AGO), Bank Indonesia (BI), the Capital Market Supervisory Agency (BAPEPAM), the Ministry of Finance Directorate General of Financial Institutions, the Directorate General of Taxation, Director General for Customs and Excise, the Ministry of Forestry Center for International Forestry Research, the Indonesian National Police, the Supreme Audit Board (BPK), the Corruption Eradication Committee, the Judicial Commission, the Directorate General of Immigration, the State Auditor, the Directorate General of the Administrative Legal Affairs Department of Law and Human Rights, the Anti-Narcotics National Board, and the Province of Aceh.

Bank Indonesia (BI), the Indonesian Central Bank, issued Regulation No. 3/10/PBI/2001, "The Application of Know Your Customer Principles," on June 18, 2001. This regulation requires banks to obtain information on prospective customers, including third party beneficial owners, and to verify the identity of all owners, with personal interviews if necessary. The regulation also requires banks to establish special monitoring units and appoint compliance officers responsible for implementation of the new rules and to maintain adequate information systems to comply with the law. BI has issued an Internal Circular Letter No. 6/50/INTERN, dated September 10, 2004 concerning Guidelines for the Supervision and Examination of the Implementation of KYC and AML by Commercial Banks. In addition, BI also issued a Circular Letter to Commercial Banks No. 6/37/DPNP dated September 10, 2004 concerning the Assessment and Imposition of Sanctions on the Implementation of KYC and other Obligations Related to Law on Money Laundering Crimes. BI is also preparing Guidelines for Money Changers on Record Keeping and Reporting Procedures, and Money Changer Examinations to be given by BI examiners. Currently, banks must report all foreign exchange transactions and foreign obligations to BI.

With respect to the physical movement of currency, Article 16 of Law No. 15/2002 contains a reporting requirement for any person taking cash into or out of Indonesia in the amount of 100 million Rupiah or more, or the equivalent in another currency, which must be reported to the Director General of Customs and Excise. These reports must be given to the PPATK in no later than five business days and contain details of the identity of the person. Indonesia Central Bank regulation 3/18/PBI/2001 and the Directorate General of Customs and Excise Decree No.01/BC/2005 contain the requirements and procedures of inspection, prohibition, and deposit of Indonesia Rupiah into or out of Indonesia.

The Decree provides implementing guidance for Ministry of Finance Regulation No.624/PMK. 2004 of December 31, 2004, and requires individuals who import or export more 100 million Rupiah in cash (approximately U.S. \$10,500) to declare such transactions to Customs. This information is to be declared on the Indonesian Customs Declaration (BC3.2). The cash declaration requirements do not cover bearer negotiable instruments as required by FATF's Special Recommendation IX. In addition, cash can only be restrained if the passenger fails to disclose or a false declaration is made. In most cases, the cash is returned to the traveler after a small administrative penalty is applied. There is no clear authority to stop, restrain or seize money that is suspected of promoting terrorism or crime or constitutes the proceeds of crime. As of December 2007, the PPATK has received more than 2,137 reports from Customs on cross border cash carrying issues. The reports were derived from two airports, Jakarta Cengkayang and Denpasar, the seaports of Batam and Tanjung Balai Karimun, Bandung, Batam and Denpasar. As of July 2007, the Indonesian National Police have conducted 20 investigations based on cross-border currency reports. Despite these investigations, detection capacity is very weak and criminal penalties are limited and are not being applied.

Indonesia's bank secrecy law covers information on bank depositors and their accounts. Such information is generally kept confidential and can only be accessed by the authorities in limited circumstances. However, Article 27(4) of the Law No. 15/2002 expressly exempts the PPATK from "the provisions of other laws related to bank secrecy and the secrecy of other financial transactions" in relation to its functions in receiving and requesting reports and conducting audits of providers of financial services. In addition, Article 14 of the Law No. 15/2002 exempts providers of financial services from bank secrecy provisions when carrying out their reporting obligations. Providers of financial services, their officials, and employees are given protection from civil or criminal action for making required disclosures under Article 15 of the anti-money laundering legislation.

There is a mechanism to obtain access to confidential information from financial institutions through BI regulation number 2/19/PBI/2000. PPATK has the authority to conduct supervision and monitoring compliance of providers of financial services. PPATK may also advise and assist relevant authorities regarding information obtained by the PPATK in accordance with the provisions of this Law No. 15/2002.

The GOI has limited formal instruments to trace and forfeit illicit assets. Under the Indonesian legal system, confiscation against all types of assets must be effected through criminal justice proceedings and be based on a court order. The GOI has no clear legal mechanism to trace and freeze assets of individuals or entities on the UNSCR 1267 Sanctions Committee's consolidated list, and there is no clear administrative or judicial process to implement this resolution and UNSCR 1373. While the BI circulates the consolidated list to all banks operating in Indonesia, this interagency process is too complex and inefficient to send out asset-freezing instructions in a timely manner. In addition, no clear instructions are provided to financial institutions as to what will happen when assets are discovered. Banks also note that without very specific information, the preponderance of similar names and inexact addresses, along with lack of a unique identifier in Indonesia, make identifying the accounts very difficult. Attempts to use a criminal process are confusing and ad hoc at best, and rely on lengthy investigation processes before consideration can be given to freezing or forfeiting assets.

Article 32 of Law No. 15/2002, as amended by Law No. 25/2003, provides that investigators, public prosecutors and judges are authorized to freeze any assets that are reasonably suspected to be the proceeds of crime. Article 34 stipulates that if sufficient evidence is obtained during the examination of the defendant in court, the judge may order the sequestration of assets known or reasonably suspected to be the proceeds of crime. In addition, Article 37 provides for a confiscation mechanism if the defendant dies prior to the rendition of judgment.

In August, 2006, the GOI enacted Indonesia's first Witness and Victim Protection Law (No. 13/2006). Indonesia's AML Law and Government Implementing Regulation No. 57/2003 also provide protection to whistleblowers and witnesses.

The October 18, 2002 emergency counter-terrorism regulation, the Government Regulation in Lieu of Law of the Republic of Indonesia (Perpu), No. 1 of 2002 on Eradication of Terrorism, criminalizes terrorism and provides the legal basis for the GOI to act against terrorists, including the tracking and freezing of assets. The Perpu provides a minimum of three years and a maximum of 15 years imprisonment for anyone who is convicted of intentionally providing or collecting funds that are knowingly used in part or in whole for acts of terrorism. However, the terrorist financing regulation appears to suffer from a number of deficiencies. For example, the terrorist financing offense must be linked to a specific act of terrorism and the prosecution must prove that the offender specifically intended that the funds be used for acts of terrorism. This regulation is necessary because Indonesia's anti-money laundering law criminalizes the laundering of "proceeds" of crimes, but it is often unclear to what extent terrorism generates proceeds. Terrorist financing is therefore not fully included as a predicate for the money laundering offence. In October 2004, an Indonesian court convicted and

sentenced one Indonesian to four years in prison on terrorism charges connected to his role in the financing of the August 2003 bombing of the Jakarta Marriott Hotel.

The GOI has begun to take into account alternative remittance systems and charitable and nonprofit entities in its strategy to combat terrorist financing and money laundering. The PPATK has issued guidelines for nonbank financial service providers and money remittance agents on the prevention and eradication of money laundering and the identification and reporting of suspicious and other cash transactions. The GOI has initiated a dialogue with charities and nonprofit entities to enhance regulation and oversight of those sectors.

Indonesia is an active member of the Asia/Pacific Group on Money Laundering (APG), and currently serves as the co-chair. The APG conducted its second mutual evaluation of Indonesia in November 2007 and the report will be discussed and adopted at the APG Annual Meeting in July 2008. In June 2004, PPATK became a member of the Egmont Group. The PPATK has pursued broader cooperation through the MOU process and has concluded 23 MOUs with other Egmont FIUs. The PPATK has also entered into an Exchange of Letters enabling international exchange with Hong Kong. Indonesia has signed Mutual Legal Assistance Treaties with Australia, China and South Korea. Indonesia joined other ASEAN nations in signing the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters on November 29, 2004, though the GOI has not yet ratified the treaty. The Indonesian Regional Law Enforcement Cooperation Centre was formally opened in 2005 and was created to develop the operational law enforcement capacity needed to fight transnational crimes.

The GOI has enacted Law No. 7/2007 to implement the 1988 UN Drug Convention, to which it is a party. The GOI also has enacted Law No. 22/1997 Concerning Drugs and Psychotropic Substances, which makes the possession, purchase or cultivation of narcotic drugs or psychotropic substances for personal consumption a criminal offense. The GOI is a party to the UN International Convention for the Suppression of the Financing of Terrorism and a party to the UN Convention against Corruption. The GOI has signed but has yet to ratify the UN Convention against Transnational Organized Crime. Indonesia is ranked 143 of 180 countries ranked in Transparency International's 2007 Corruption Perception Index.

While The Government of Indonesia has made progress in constructing an AML regime, efforts to combat terrorist financing have been weak. Sustained public awareness campaigns, new bank and financial institution disclosure requirements, and the PPATK's support for Indonesia's first credible anti-corruption drive has led to increased public awareness about money laundering and, to a lesser degree, terrorist financing. However, weak human and technical capacity, poor interagency cooperation, and rampant corruption in business and government remain significant impediments to the continuing development of an effective anti-money laundering regime. The highest levels of GOI leadership should continue to demonstrate strong support for strengthening Indonesia's anti-money laundering regime. In particular, the GOI must continue to improve capacity and interagency cooperation in analyzing suspicious and cash transactions, investigating and prosecuting cases, and achieving deterrent levels of convictions. As part of this effort, Indonesia should review and streamline its process for reviewing UN designations and identifying, freezing and seizing terrorist assets, and become a party to the UN Convention against Transnational Organized Crime.

Iran

Iran is not a regional financial center. Iran's economy is marked by a bloated and inefficient state sector and over-reliance on the petroleum industry. Iran's huge oil and gas reserves produce 60 percent of government revenue-and state-centered policies that cause major distortions in the economy. Iran earns about U.S. \$50 billion a year in oil exports. Private sector activity is typically small-scale; workshops, farming, and services. Reportedly, a prominent Iranian banking official estimates that money laundering encompasses an estimated 20 percent of Iran's economy. There are other reports

that approximately U.S. \$12 billion a year is laundered via smuggling commodities in Iran and over U.S. \$6 billion is laundered by international criminal networks. The World Bank reports that about 19 percent of Iran's GDP pertains to unofficial economic activities. Money laundering in Iran encompasses narcotics trafficking, smuggling, trade fraud, counterfeit merchandise and intellectual property rights violations, cigarette smuggling, trafficking in persons, hawala, capital flight, and tax evasion.

After the Iranian Revolution of 1979, the Government of Iran (GOI) nationalized the country's banks, leaving the following: Bank Refah, Bank Melli Iran, Bank Saderat, Bank Tejarat, Bank Mellat and Bank Sepah, and three specialized institutions, Bank Keshavrzi, Bank Maskan and Bank Sanat va Madden. No foreign banks were allowed to operate in the country. Since 1983, consistent with Islamic law, banks have been prohibited from paying interest on deposits or charging interest on loans. However, alternative financial instruments were developed including profit-sharing and financing based on trade. In 1994, Iran authorized the creation of private credit institutions. Licenses for these banks were first granted in 2001. Currently, these banks include Karafarin, Parsian, Saman Eghtesad, Pasargad, Sarmayeh, and Eghtesade Novin. Standard Chartered Bank became the first foreign bank to be awarded a license to establish a branch in Iran, although this was limited to Kish, a free-zone island. Currently, some 40 international banks have representative offices in Iran, which may undertake lending but not accept deposits.

There are currently no meaningful anti-money laundering (AML) controls on the Iranian banking system. The Central Bank of Iran (CBI) has issued AML circulars that address suspicious activity reporting and other procedures that demonstrate an awareness of international standards, but there is a lack of implementation. In 2003, the Majlis (Parliament) reportedly passed an anti-money laundering act. The act includes customer identification requirements, mandatory record keeping for five years after the opening of accounts, and the reporting of suspicious activities. However, the act has not been implemented due to reported pressure by vested interests within the government. Iran has reported to the United Nations that it has established a financial intelligence unit (FIU). However, Iran has not provided any documentation or details on the FIU.

The U.S. Department of State has designated Iran as a State Sponsor of Terrorism. On September 8, 2006 the U.S. Treasury Department issued a regulation prohibiting U.S. financial institutions from handling any assets, directly or indirectly, relating to Iran's Bank Saderat, based on evidence of its involvement in transferring funds to terrorist groups. Bank Saderat is one of Iran's largest with approximately 3,400 branches. On January 9, 2007, the U.S. Treasury Department imposed sanctions against Bank Sepah, a state-owned Iranian financial institution for providing support and services to designated Iranian proliferation firms, particularly Iran's missile procurement network. There are reports that Bank Sepah requested other financial institutions to remove its name from processing suspect transactions in the international financial system. Bank Sepah is the fifth largest Iranian state-owned bank and has international branches in Europe.

On October 11, 2007, FATF released a statement of concern stating that "Iran's lack of a comprehensive AML/CTF regime represents a significant vulnerability within the international financial system. FATF calls upon Iran to address on an urgent basis its AML/CTF deficiencies, including those identified in the 2006 International Monetary Fund Article IV Consultation Report for Iran. FATF members are advising their financial institutions to consider the risk arising from the deficiencies in Iran's AML/CTF regime and practice enhanced "due diligence." Iran is currently the only country for which FATF has publicly identified such significant AML/CTF vulnerabilities. On October 16, 2007, the Department of Treasury issued an advisory to financial institutions that they "should be aware that there may be an increased effort by Iranian entities to circumvent international sanctions and related financial community scrutiny through the use of deceptive practices involving shell companies and other intermediaries or requests that identifying information be removed from transactions. Such efforts may originate in Iran or Iranian free trade zones subject to separate

regulatory and supervisory controls, including Kish Island. Such efforts may also originate wholly outside of Iran at the request of Iranian controlled entities.”

On October 25, 2007, the Department of Treasury designated for proliferation activities under Executive Order 13382 Iran’s state-owned Banks Melli and Mellat. Bank Melli is Iran’s largest bank. Bank Melli provides banking services to entities involved in Iran’s nuclear and ballistic missile programs, including entities listed by the UN for their involvement in those programs. Bank Melli provides banking services to the Iranian Revolutionary Guards Corps (IRGC) and the Qods Force. When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement in the international banking system. Bank Mellat provides banking services in support of Iran’s nuclear entities, including those designated by the United States and by the UN Security Council under UNSCRs 1737 and 1747. On October 25, Bank Saderat was also designated for its support for terrorism, specifically channeling funds to terrorist organizations including Hizballah and EU-designated terrorist groups Hamas, PFLP-GC, and Palestinian Islamic Jihad.

Iran has a very large underground economy, which is spurred by restrictive taxation, widespread smuggling, currency exchange controls, capital flight, and a large Iranian expatriate community. The IMF reports that Iran has the highest “brain drain” rate of 90 countries measured. Over 400,000 Iranians live in Dubai. Anyone engaging in transfers or transactions of foreign currency into or out of Iran must abide by CBI regulations, including registration and licensing. Those who do not are subject to temporary or permanent closure. The regulations and circulars address money transfer businesses, including hawaladars. However, underground hawala and moneylenders in the bazaar are active in Iran. Since there is an absence of an adequate banking system and working capital, the popular informal system meets the need for currency exchange and money lending. Many hawaladars and traditional bazaari are linked directly to the regional hawala hub in Dubai. Counter valuation in hawala transactions is often accomplished via trade. The trade and smuggling of goods into Iranian commerce leads to a significant amount of trade-based money laundering and value transfer. Approximately 7,500 Iranian-owned companies operate out of Dubai.

Iran’s real estate market is often used to launder money. Frequently, real estate settlements and payment are made overseas. In addition, there are reports that a massive amount of Iranian capital has been invested in the United Arab Emirates, particularly in Dubai real estate. Iranian investments in Dubai may be in excess of U.S. \$350 billion.

Via a transit trade agreement, goods purchased primarily in Dubai are sent to ports in southern Iran and then via land routes to markets in Afghanistan. The transit trade facilitates the laundering of Afghan narcotics proceeds via barter transactions, trade-based money laundering, and trade goods that provide counter valuation in the regional hawala markets. According to the United Nations Office on Drugs and Crime, approximately 60 percent of Afghanistan’s opium is trafficked across Iran’s border. Reportedly, Iran has an estimated three million drug users and the highest per capita heroin addiction rate in the world. Opiates not intended for the Iranian domestic market transit Iran to Turkey, where the morphine base is converted to heroin. Heroin and hashish are delivered to buyers located in Turkey. The drugs are then shipped to the international market, primarily Europe. In Iran and elsewhere in the region, proceeds from narcotics sales are sometimes exchanged for trade goods via value transfer. The United Nations Global Program against Money Laundering (GPML) also reports that illicit proceeds from narcotics trafficking are used to purchase goods in the domestic Iranian market and then the goods are often exported and sold in Dubai.

Iran’s “bonyads,” or charitable religious foundations, were originally established at the time of the Iranian revolution to help the poor. They have rapidly expanded beyond their original mandate. Although still funded, in part, by Islamic charitable contributions, today’s bonyads monopolize Iranian import-export concerns and major industries including petroleum, automobiles, hotels, and banks.

Bonyad conglomerates account for a substantial percentage of Iran's gross national product. Individual bonyads such as Imman Reza Foundation and the Martyrs' Foundation have billions of dollars in assets. Mullahs direct the bonyad foundations. Given the low rate of capital accumulation in the Iranian economy, the foundations constitute one of the few governmental institutions for internal economic investment. Reportedly, the bonyads stifle entrepreneurs not affiliated with them due to the bonyads' favored status, which includes exemption from taxes, the granting of favorable exchange rates, and lack of accounting oversight by the Iranian government. Bonyads have been involved in funding terrorist organizations and serving as fronts for the procurement of nuclear capacity and prohibited weapons and technology.

On October 25, 2007, the United States designated Iran's IRGC, the armed guardians of Iran's theocracy, as a proliferator of weapons of mass destruction. The elite Quds Force was included in the designation as a supporter of terrorism. The Revolutionary Guard's suspect financing is entwined with Iran's economy. The Revolutionary Guard is involved with more than 100 companies and manages billions of dollars in business. Similar to bonyads, the military/business conglomerate uses high-level political connections, no-bid contracts, and squeezes out competitors. Corruption is widespread throughout Iranian society; at the highest levels of government, favored individuals and families benefit from "baksheesh" deals. Iran is ranked 131 out of 179 countries listed in Transparency International's 2007 Corruption Perception Index. Despite some limited attempts at reforming bonyads and other entities, there has been little transparency or substantive progress.

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

The Government of Iran should engage with the FATF and construct and implement a viable anti-money laundering and terrorist finance regime that adheres to international standards. Iran should be more active in countering regional smuggling. Iran should implement meaningful reforms in bonyads that promote transparency and accountability. Iran should create an anti-corruption law with strict penalties and enforcement, applying it equally to figures with close ties to the government and the clerical communities. It should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Iran should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Iran should refrain from supporting terrorism or the funding of terrorism.

Iraq

Iraq's economy is primarily cash-based, and there is little data available on the extent of money laundering. However, cross-border smuggling is widespread, including the smuggling of bulk cash. Iraq is a major market for smuggled cigarettes and counterfeit goods, and money is laundered through intellectual property right violations. There is a large market for stolen cars from Europe and the United States. Ransoms generated from kidnapping generate tens of millions of dollars every year. Kidnappings are linked to human exploitation and terrorist finance. Iraq is a source country for human trafficking. Trade-based money laundering, customs fraud, and value transfer are found in the underground economy and are commonly used in informal value transfer systems such as hawala. Hawala networks are prevalent and are widely used in Iraq and the region. Cash, trade-based money laundering, and hawala are all components of terrorist and insurgent finance found in Iraq. In early 2006, the Iraqi oil ministry estimated that ten percent of the \$4 billion to \$5 billion in fuel imported for public consumption at subsidized rates in 2005 was smuggled internally and out of the country for resale at market rates. Large amounts of Iraqi oil are smuggled to Iran and other Gulf countries through routes established by Saddam Hussein when Iraq was under sanctions in the 1990s. The

organized smuggling rings siphon oil from pipelines, and load it onto tanker trucks that carry the oil to small boats in the Persian Gulf. Corrupt officials facilitate the smuggling by issuing certificates and permits that allow the smugglers to pass through security checkpoints. Moreover, it is reported that approximately ten percent of all oil smuggling profits are going to insurgents. Subsidy scams and black market sales also exist for gasoline, kerosene, and cooking fuel. Corruption is a severe problem that permeates society and commerce and is also found at the highest levels of government, and large public and private institutions. Transparency International's 2007 International Corruption Perception Index ranked Iraq 178 of 180 countries surveyed. The formal financial sector is growing and at least ten new banks, both domestic and international, have been licensed to operate in Iraq. The two largest state-owned banks control at least 90 percent of the banking sector.

The Coalition Provisional Authority (CPA), the international body that governed Iraq beginning in April 2003, issued regulations and orders that carried the weight of law in Iraq. The CPA ceased to exist in June 2004, at which time the Iraqi Interim Government assumed authority for governing Iraq. Drafted and agreed to by Iraqi leaders, the Transitional Administrative Law (TAL) described the powers of the Iraqi government during the transition period. Under TAL Article 26, regulations and orders issued by the CPA pursuant to its authority under international law remain in force until rescinded or amended by legislation duly enacted and having the force of law. The constitution, which was ratified in October 2005, also provides for the continuation of existing laws, including CPA regulations and orders that govern money laundering.

The CPA Order No. 93, "Anti-Money Laundering Act of 2004" (AMLA) governs financial institutions in connection with: money laundering, financing of crime, financing terrorism, and the vigilance required of financial institutions in regard to financial transactions. The law also criminalizes money laundering, financing crime (including the financing of terrorism), and structuring transactions to avoid legal requirements. The AMLA covers: banks; investment funds; securities dealers; insurance entities; money transmitters and foreign currency exchange dealers, as well as persons who deal in financial instruments, precious metals or gems; and persons who undertake hawala transactions. Covered entities are required to verify the identity of any customer opening an account for any amount. Covered entities are also required to verify the identity of nonaccount holders performing a transaction or series of potentially related transactions whose value is equal to or greater than five million Iraqi dinars (approximately U.S. \$4,125). Beneficial owners must be identified upon account opening or for transactions exceeding ten million Iraqi dinar (approximately U.S. \$8,250). Records must be maintained for at least five years. Covered entities must report suspicious transactions and wait for guidance before proceeding with the transaction; the relevant funds are frozen until guidance is received. Suspicious transaction reports (STRs) are to be completed for any transaction over four million Iraqi dinars (approximately U.S. \$3,300) that is believed to involve funds that are derived from illegal activities or money laundering, intended for the financing of crime (including terrorism), or over which a criminal organization has disposal power, or a transaction conducted to evade any law and which has no apparent business or other lawful purpose. The "tipping off" of customers by bank employees where a transaction has generated a suspicious transaction report is prohibited. Bank employees are protected from liability for cooperating with the government. Willful violations of the reporting requirement may result in imprisonment or fines.

CPA Order No. 94, "Banking Law of 2004," gives the Central Bank of Iraq (CBI) the authority to license banks and to conduct due diligence on proposed bank management. Order No. 94 establishes requirements for bank capital, confidentiality of records, audit and reporting requirements for banks, and prudential standards. The CBI is responsible for the supervision of financial institutions. The CBI was mandated by the AMLA to issue regulations and require financial institutions to provide employee training, appoint compliance officers, develop internal procedures and controls to deter money laundering, and establish an independent audit function. The CBI has branches in Irbil, Sulimaniyah, Dahuk (which are located in the Northern Kurdistan Region of Iraq) and Basra. The CBI

also houses Iraq's financial intelligence unit, the Money Laundering Reporting Office (MLRO). The CBI branches are responsible for licensing and examining private and public banks, and money exchangers and transmitters. The CBI branches are required to conduct periodic examinations of the banks. For public banks this occurs every six months and every three months for private banks. Order No. 94 gives administrative enforcement authority to the CBI, up to and including the removal of institution management and revocation of bank licenses. While the banks are ostensibly providing traditional banking services such as lending to the community in practice, they collect funds and send excess reserves to the CBI in Baghdad where they receive an 18 to 20 per cent return. There is no time limit for reserves to be held in the CBI for accrual of interest. Outside of this relationship, there is poor communication with the CBI, particularly with respect to money laundering, terrorist financing and other potential risks.

One of the most significant challenges facing the CBI is the lack of communication both among its branches and between the branches and the CBI in Baghdad. There is a general lack of modern banking technology, in particular a lack of an electronic payment system and wire transfer capability. As the financial sector is relatively new, there is little institutional knowledge with respect to anti-money laundering/counterterrorist finance (AML/CTF) issues. Another challenge confronting the CBI, is the lack of trust, confidence, and modernization in the formal financial sector due to the history of misuse and abuses of the sector during the Saddam Hussein regime

Bulk cash smuggling is a major problem in Iraq. The CBI is considering issuance of regulations to require large currency transaction reports for the cross-border transport of currency of more than 15 million Iraqi dinars (approximately U.S. \$12,380). Neither Iraqis nor foreigners are permitted to transport more than U.S. \$10,000 in currency when exiting Iraq.

An additional vulnerability to Iraq's AML/CTF regime is that money exchanges and money transmitters are largely unregulated. Although they are required to be licensed, the level of supervision is nominal. Money exchanges are not subject to the same examination process as banks nor are they required to report suspicious transactions. The current training given to managers and operators of money exchanges and money transmitters on AML/CTF and banking examination practices is inadequate. The MLRO, which in other circumstances could assist in the training and monitoring for AML/CTF, is not developed enough yet to execute its core mission and also suffers from a lack of communication with CBI branches outside of Baghdad. Most transactions, foreign exchange operations, and money remittances take place through such money transmitter businesses and not through the banking sector. Most international remittances are done via related offices in Amman or Dubai. While simple funds transfers can take weeks to accomplish through the banking sector, the same transactions can be done very rapidly and far more effectively through money exchange and transfer services.

Although financial institutions are required to report suspicious transactions including potential money laundering and terrorist financing under the Anti-money Laundering Ordinance, in practice they do not do so, due to the isolation of the MLRO and a lack of training and technology. The MLRO was formed in June/July 2006 and has a small but dedicated staff. The CBI and representatives from the United States are working together to build the MLRO's capacity and implement the day-to-day functions of a financial intelligence unit (FIU). The MLRO operates independently to collect, analyze and disseminate information on financial transactions subject to financial monitoring and reporting, including suspicious activity reports. The MLRO is also empowered to exchange information with other Iraqi or foreign government agencies. The CBI and its MLRO finalized implementing regulations to the AMLA, which became effective September 15, 2006.

The predicate offenses for the crimes of money laundering and the financing of crime are quite broad and extend beyond "all serious offenses" to include "some form of unlawful activity." The penalties for violating the AMLA depend on the specific nature of the underlying criminal activity. For

example, “money laundering” is punishable by a fine of up to 40 million dinar (approximately U.S. \$33,000) or twice the value of the property involved in the transaction (whichever is greater) or imprisonment of up to four years or both. Other offenses for which there are specific penalties include the financing of crime with a fine of up to 20 million dinar (approximately U.S. \$16,510) or two years imprisonment or both and structuring transactions of up to 10 million dinar (approximately U.S. \$8,250) or one year imprisonment or both. No arrests or prosecutions under the AMLA have been reported to date.

The AMLA includes provisions for the forfeiture of any property. Such property includes, but is not limited to, funds involved in a covered offense, or any property traceable to the property, or any property gained as a result of such an offense, without prejudicing the rights of bona fide third parties. The courts can order confiscation of property, but it appears they can only do so if the property is directly related to the crime, including drug proceeds. According to the Iraqi Penal Code, a person must pay the government back for any property stolen from the government. In other cases of theft, restitution is made to the victim(s). Any property forfeited to the state becomes state property and goes into the general treasury. Should the government confiscate perishables, it can sell them while the case is on-going and if the defendant is acquitted, the government returns the money it realized from the sale of the goods to the defendant. While the case is on going, the government appoints a judicial guardian to supervise and maintain the property pending the outcome of the case. The AMLA also blocks any funds or assets, other than real property (which is covered by a separate regulation), belonging to members of the former Iraqi regime and authorizes the Minister of Finance to confiscate such assets following a judicial or administrative order. The lack of automation or infrastructure in the banking sector, however, hinders the government’s ability to identify and freeze assets linked to illicit activity.

Iraq has free trade zones in Basra/Khor al-Zubair, Ninewa/Falafel, Sulaymaniyah, and Al-Quaymen. Under the Free Zone (FZ) Authority Law, goods imported and exported from the FZ are generally exempt from all taxes and duties, unless the goods are imported into Iraq. Additionally, capital, profits, and investment income from projects in the FZ are exempt from taxes and fees throughout the life of the project, including in the foundation and construction phases.

The CBI is also mandated by the AMLA to distribute the UN 1267 Sanction Committee’s consolidated list of suspected terrorists or terrorist organizations. No asset freezes pertaining to any names on the consolidated list have been reported to date.

Iraq became a member of the Middle East and North Africa Financial Action Task Force (MENAFATF) in September 2005. Iraq is a party to the 1988 UN Drug Convention, but not the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, or the UN Convention against Corruption.

The Government of Iraq continues to lay the foundation for anti-money laundering and counterterrorist finance regimes. In these efforts, there is strong cooperation with the U.S. Government. However, there is much work ahead. While Iraq’s economy is primarily cash-based, this is likely to change as the expected development of the energy sector will increase the need for the development of a formal financial sector that is integrated into the international payment system. Concurrently, the financial sector must adopt AML/CTF standards and practices. Iraq should take a more active part in MENAFATF and in implementing its recommendations. As independent foreign banks become more interested in opening branches in Iraq, the CBI should be cautious in granting licenses to banks from jurisdictions of concern. Iraq should continue its efforts to build capacity and actively implement the provisions of the AMLA and related authorities. As a priority, as Iraq’s MLRO becomes fully functional, it should develop increased capacity to investigate financial crimes and enforce the provisions of the AMLA. Iraqi law enforcement, border authorities, and customs service should strengthen border enforcement and identify and pursue smuggling and trade-based money

laundering networks. Increased border enforcement is also a prerequisite in combating terrorist finance. The Government of Iraq should also take concerted steps to combat the corruption that hinders development and impedes an effective anti-money laundering and counter-terrorist finance regime. Iraq should become a party to the UN Convention against Corruption, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Ireland

Ireland is an increasingly significant European financial hub. Narcotics-trafficking, fraud, and tax offenses are the primary sources of funds laundered in Ireland. Money laundering occurs in credit institutions, although launderers have also made use of money remittance companies, solicitors, accountants, and second-hand car dealerships. The most common laundering methods are: the purchase of high-value goods for cash; the use of credit institutions to receive and transfer funds in and out of Ireland; the use of complex company structures to filter funds; and the purchase of properties in Ireland and abroad.

The Shannon Free Zone was established in 1960 as a free trade zone, offering investment incentives for multinational companies. The Shannon Free Zone is supervised by “Shannon Development,” a government-founded body. Reportedly, there are no indications that the Shannon Free Zone is being used in trade-based money laundering (TBML) schemes or by financiers of terrorism. The international banking and financial services sector is concentrated in Dublin’s International Financial Services Centre (IFSC). In 2007, there were approximately 440 international financial institutions and companies operating in the IFSC. Services offered include banking, fiscal management, re-insurance, fund administration, and foreign exchange dealing. Although there are no tax benefits for companies in the IFSC, Ireland offers the lowest corporate tax rate (12.5 percent) in the EU. Casinos, including Internet casinos, are illegal in Ireland. Private gaming clubs, however, operate casino-like facilities that fall outside the scope of the law.

Ireland criminalized money laundering relating to narcotics trafficking and all indictable offenses under the 1994 Criminal Justice Act. The law requires financial institutions (banks, building societies, the Post Office, stock brokers, credit unions, bureaux de change, life insurance companies, and insurance brokers) to report suspicious transactions. There is no monetary threshold for reporting suspicious transactions. The obliged entities submit suspicious transaction reports (STRs) to the Garda (Irish Police) Bureau of Fraud Investigation, Ireland’s financial intelligence unit (FIU), and to the Revenue (Tax) Department in addition to the FIU, as required by law. Reporting entities must submit the STR before the suspicious transaction is finalized. There are no other legal requirements governing the time period within which an STR must be filed. Financial institutions must implement customer identification procedures and retain records of financial transactions. Ireland has amended its Anti-Money Laundering (AML) law to extend customer identification and suspicious transaction reporting requirements to lawyers, accountants, auditors, real estate agents, auctioneers, and dealers in high-value goods. Ireland’s Customer Due Diligence procedure requires designated entities to take measures to identify customers when opening new accounts or conducting transactions exceeding 13,000 euros (approximately U.S. \$19,000). These requirements do not extend to existing customers prior to May 1995 except in cases where authorities suspect that money laundering or another financial crime is involved.

The Corporate Law requires that every company applying for registration in Ireland must demonstrate that it intends to carry on an activity in the country. Companies must maintain an Irish resident director at all times, or post a bond as a surety for failure to comply with the appropriate company law. In addition, the law limits the number of directorships that any one person can hold to 25, with certain exemptions. This limitation aims to curb the use of nominee directors as a means of disguising

beneficial ownership or control. The Company Law Enforcement Act 2001 (Company Act) established the Office of the Director of Corporate Enforcement (ODCE). The ODCE investigates and enforces provisions of the Company Act. Under the law, a company must provide the names of its directors. The ODCE has the authority to uncover a company's beneficial ownership and control. The Company Act also creates a mandatory reporting obligation for auditors suspicious of breaches of company law to the ODCE. In 2006, the ODCE secured the conviction of 31 company directors and other individuals on 41 charges for breaching various requirements of the Company Act. An additional 17 company officers were disqualified from eligibility for a lead position in companies for periods ranging from one to 10 years.

EU Regulation 1889/2005, introduced in Ireland on June 15, 2007, requires travelers transporting more than 10,000 euros (approximately U.S. \$14,600) into or out of the EU to declare these funds. The declarations are automatically reported to the FIU. Customs authorities also require reports detailing movements of precious metals and stones into or out of the EU when Ireland is the initial entry or final exit point. The FIU will have access to these reports.

The Third EU Money Laundering Directive entered into force in December 2005 and was transposed into Irish law prior to the December 2007 deadline. The Government of Ireland (GOI) is likely to implement new legislation to address customer due diligence, the identification of beneficial owners, politically exposed persons, and the designation of trusts. A Mutual Evaluation conducted in 2005 by the Financial Action Task Force (FATF), published in 2006, noted that Ireland's money laundering definition met the FATF requirements. The mutual evaluation report (MER) acknowledged that Ireland achieved a high standing in AML legal structures and international cooperation, although the number of money laundering prosecutions and convictions was low.

The Irish Financial Services Regulatory Authority (IFSRA), the financial regulator, is a component of the Central Bank and Financial Services Authority of Ireland (CBFSAI) and is responsible for supervising the financial institutions for compliance with money laundering procedures. IFSRA is obliged to report any suspected breaches of the Criminal Justice Act 1994 by the institutions it supervises to the FIU and the Revenue Commissioners. Reports cover suspicion of money laundering and terrorist financing, failure to establish identity of customers, failure to retain evidence of identification, and failure to adopt measures to prevent and detect the commission of a money laundering offense. IFSRA also regulates the IFSC companies that conduct banking, insurance, and fund transactions.

Ireland's FIU receives and analyzes financial disclosures, and disseminates them for investigation. The MER found that although Ireland's FIU met the requirements of the FATF methodology it had limited technical and human resources to manage and evaluate STRs effectively. In 2006, the FIU received 10,403 STRs. Three people were convicted for money laundering. Information regarding the number of STRs received in 2007 is not yet available. A conviction on charges of money laundering carries a maximum penalty of 14 years' imprisonment and an unlimited fine. The lengthiest penalty applied for a money laundering conviction to date has been six years.

Ireland estimates that up to 80 percent of STRs may involve tax violations. Value Added Tax (VAT) Intra-Community Missing Trader Fraud is extensive within the EU, and attacks the VAT system, in which criminals obtain VAT registration to acquire goods VAT free from other Member States. They then sell on the goods at VAT inclusive prices and disappear without remitting the VAT paid by their customers to the tax authorities. There is evidence in several fraud investigations that conduit traders involved in the supply chain have established themselves in Ireland.

The Criminal Assets Bureau (CAB), authorized to confiscate the proceeds of crime in cases where there is no criminal conviction, reports to the Minister for Justice and includes experts from the Garda, Tax, Customs, and Social Security Agencies. Under the 1996 Proceeds of Crime Act, authorities may freeze specified property valued in excess of 13,000 euros (approximately U.S. \$19,000) for seven

years, unless the court is satisfied that all or part of the property is not criminal proceeds. With the consent of the High Court and the parties concerned, the authorities have the power to dispose of assets without having to wait the seven years. As of November 2007, the authorities have executed 14 such consent orders. This Act also allows the authorities to take foreign criminality into account in assessing whether assets are the proceeds of criminal conduct. Under certain circumstances, the High Court can freeze, and, where appropriate, seize the proceeds of crimes.

In 2006, CAB obtained interim and disposal orders on assets valued at approximately 6.8 million euros (approximately U.S. \$10 million). The CAB has the authority to cooperate with agencies in other jurisdictions, which strengthens Irish cooperation with asset recovery agencies in the United Kingdom.

With the Criminal Justice (Terrorism Offenses) Act, Ireland's legislation comports with United Nations Conventions and European Union Framework decisions on combating terrorism. The IFSRA works with the Department of Finance to draft guidance for regulated institutions on combating and preventing terrorist financing. The authorities revised and issued the guidance to institutions upon the passage of the Criminal Justice Act in 2005.

To date, there have been no prosecutions for terrorism offenses under the Criminal Justice Act. The FATF MER noted that the Act neglects to criminalize funding of either a terrorist acting alone or two terrorists acting in concert. The MER also noted inadequate implementation of UN Security Council Resolution (UNSCR) 1373, in that Ireland relies exclusively on an EU listing system without subsidiary mechanisms to deal with terrorists on the list who are European citizens (EU Regulations do not apply for freezing purposes to such persons) or with persons designated as terrorists by other jurisdictions who are not on the EU list.

The Criminal Justice (Terrorism Offenses) Act imposes evidentiary requirements obstructing Ireland from fulfilling its UNSCR 1373 obligation to freeze all funds and assets of individuals who commit terrorist acts whether or not there is evidence that those particular funds are intended for use in terrorist acts. The Garda can apply to the courts to freeze assets when certain evidentiary requirements are met. From 2001 through 2007, Ireland had reported to the European Commission the names of five individuals who maintained a total of seven accounts that were frozen in accordance with the provisions of the European Union's (EU) Anti-Terrorist Legislation. No designated individuals or entities have surfaced in Ireland's system since 2004. The aggregate value of the funds frozen was approximately U.S. \$6,400.

In July 2005, the United States and Ireland signed instruments on extradition and mutual legal assistance as part of a sequence of bilateral agreements that the United States is concluding with all 25 EU Member States. The instruments supplement and update the 1983 U.S.-Ireland extradition treaty and the 2001 bilateral treaty on mutual legal assistance (MLAT). The 2005 instrument also provides for searches of suspect foreign located bank accounts, joint investigative teams, and testimony by video-link. The 1983 extradition treaty between Ireland and the U.S. is in force, but as of November 2007, the GOI has not completed the ratification process for the 2001 MLAT. In November 2006, for the first time in eighteen extradition requests, Ireland extradited a U.S. citizen.

Ireland is a member of the FATF, and its FIU is a member of the Egmont Group. Ireland is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. It has signed, but not ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

The GOI should enact legislation to prohibit the establishment of "shell" companies. Law enforcement should have a stronger role in identifying the true beneficial owners of shell companies as well as of trusts in the course of investigations. Ireland should increase the technical and human resources provided to the FIU to manage and evaluate STRs effectively. The GOI should enact legislation that

covers both funding of a terrorist acting alone and funding of two terrorists acting in concert, as well as legislation fully implementing UNSCR 1373. To this end, Ireland should remove the evidentiary requirements acting as obstacles to full compliance, as well as circulate the UN and the U.S. lists to its regulators and obligated entities. Ireland should continue implementation of its new anti-terrorism legislation and its AML law amendments, and ensure stringent enforcement of all such initiatives. Ireland should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Isle of Man

The Isle of Man (IOM) is a Crown Dependency of the United Kingdom with its own parliament, government, and laws. Its large and sophisticated financial center is potentially vulnerable to money laundering at the layering and integration stages. Most of the illicit funds in the IOM are from fraud schemes and narcotics trafficking in other jurisdictions, including the United Kingdom. The U.S. dollar is the most common currency used for criminal activity in the IOM. Identity theft and Internet abuse are growing segments of financial crime activity.

No current data regarding the entities that comprise the IOM financial industry has been reported. As of September 30, 2004, the IOM's financial industry consisted of approximately 19 life insurance companies, 25 insurance managers, more than 177 captive insurance companies, 53 licensed banks and two licensed building societies, 82 investment business license holders, 30.1 billion pounds (approximately U.S. \$59 billion) in bank deposits, and 164 collective investment schemes with 6.5 billion pounds (approximately U.S. \$12.7 billion) of funds under management. There were also 171 licensed corporate service providers.

The IOM criminalized money laundering related to narcotics trafficking in 1987. The Criminal Justice (Money Laundering Offenses) Act 1998, extends the definition of money laundering to cover all serious crimes and led to the creation of the Anti-Money Laundering (AML) Code, which came into force in December 1998. The AML Code has subsequently been replaced by the Criminal Justice (Money Laundering) Code 2007 (the Code), enacted in September 2007. Requirements under the 2007 Code apply to banking, investment, and collective investment schemes, fiduciary services business, insurance, building societies, credit unions, local authorities authorized to raise or borrow money, bureaux de change, estate agents, bookmakers and casinos (excluding online gambling), accountants, notaries and legal practitioners, insurance intermediaries, retirement benefits schemes, administrators and trustees, auditors, the Post Office, and any activity involving money transmission services or check encashment facilities.

The Code requires that obligated entities implement AML policies, procedures, and practices, including employing them for countering terrorist financing. The Code mandates that obligated entities institute procedures to establish customer identification requirements; report suspicious transactions; maintain adequate records; adopt adequate internal controls and communication procedures; provide appropriate training for employees; and establish internal reporting protocols. There is no minimum threshold for obliged entities to file a suspicious transaction report (STR), and safe harbor provisions in the law protect reporting individuals when they file an STR. It is an offense to fail to disclose suspicion of money laundering for all predicate crimes. Failure to comply with the requirements of the Code may bring a fine, imprisonment of up to two years, or both.

The Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA) regulate the IOM financial sector. The IPA regulates insurance companies, insurance management companies, general insurance intermediaries, and retirement benefit schemes and their administrators. The FSC is responsible for the licensing, authorization, and supervision of banks, building societies, investment businesses, collective investment schemes, corporate service providers, and companies. The FSC also maintains the Company Registry Database for the IOM, which contains company records dating back

to the first company incorporated in 1865. Statutory documents filed by IOM companies can now be searched and purchased online through the FSC's website.

As IOM's companion to the AML Code, the FSC has AML Guidance Notes (AMLGN), which the FSC rewrote in 2007. The new guidance reflects evolving international standards, new legislation on the Island, and the new licensee status of Corporate Service Providers and Trust Service Providers. In 2008, the FSC will release the new revised guidance as an "Anti-Money Laundering and the Financing of Terrorism Handbook."

The FSC has worked with its counterparts from the Crown Dependencies of Guernsey and Jersey. One of these initiatives was a consultation paper called Overriding Principles for a Revised Know Your Customer (KYC) Framework, to develop a more coordinated AML approach. Work between the Crown Dependencies is continuing, to develop a coordinated strategy on money laundering, and to ensure maximum compliance with the revised Financial Action Task Force (FATF) Forty Recommendations on Money Laundering.

Money service businesses (MSBs) not already regulated by the FSC or IPA must register with Customs and Excise. With this, the IOM implemented the first two EU Directives on Money Laundering, and provides for their supervision by Customs and Excise to ensure compliance with the AML Code. In December 2007, the FSC issued a Consultative Paper on the Proposed Regulation of MSBs, including electronic money (e-money) providers. This document will assist the Island in meeting the standards set by the Financial Action Task Force ("FATF") 40 Recommendations and Nine Special Recommendations on Terrorist Financing. The paper also airs proposals to bring money MSBs and e-money providers under some form of regulation, which would initially be limited.

The IPA, as regulator of the IOM's insurance and pensions business, issues Anti-Money Laundering Standards for Insurance Businesses (the "Standards"). The Standards are binding upon the industry and include "Overriding Principles" requiring all insurance businesses to check their businesses to determine that they have sufficient information available to prove customer identity. The current set of Standards became effective March 31, 2003. The IPA conducts on-site visits to examine procedures and policies of companies under its supervision.

The Online Gambling Regulation Act 2001 and an accompanying AML (Online Gambling) Code 2002 are supplemented by AML guidance notes issued by the Gambling Control Commission, a regulatory body which provides guidance on the prevention of money laundering in the online gaming sector. The Online Gambling legislation, unique to the gaming industry when it passed, brought regulation to an unregulated gaming environment. The revised version of the Online Gambling and Peer to Peer Gambling AML Code came into force in 2006.

The Companies, Etc. (Amendment) Act 2003 provides for additional supervision for all licensable businesses, e.g., banking, investment, insurance, and corporate service providers. The act abolished future bearer shares after April 1, 2004, and mandates that all existing bearer shares be registered before the bearer can exercise any rights relating to the shares.

The Financial Crime Unit (FCU), under the Department of Home Affairs, the intelligence financial unit (FIU) of the Isle of Man, was formed in April 2000 and evolved from the police Fraud Squad. It is the central point for the collection, analysis, investigation, and dissemination of suspicious transaction reports (STRs) from obligated entities. The FCU's work is broadly split between financial intelligence, legal co-operation with other jurisdictions in terms of financial investigation, and local financial crime investigation involving serious or complex cases. It is comprised of Police and Customs Officers, Police Support Staff, and other government departments such as Internal Audit and HM Attorney General's Chambers. The FIU has access to Customs, police, and tax information. The FIU disseminates STRs to the Customs, Tax Administrators, FSC, and the IPA. The FCU is responsible for investigating financial crimes and terrorist financing cases. The FIU received approximately 1,574

suspicious transaction reports in 2007, and 1,653 STRs in 2006. Approximately 45 percent of the STRs are disseminated to the United Kingdom, five percent to other European countries, and seven percent to nonEuropean countries (mainly the U.S.). IOM authorities charged eight people with money laundering offenses in 2007, and investigations are proceeding. Six of the eight have been charged in relation to narcotics, and two to fraud, including wire fraud. In 2006, IOM authorities obtained one conviction for money laundering.

IOM legislation provides powers to constables, including customs officers, to investigate whether a person has benefited from any criminal conduct. These powers allow information to be obtained about that person's financial affairs. These powers can be used to assist in criminal investigations abroad as well as in the IOM. The Customs and Excise (Amendment) Act 2001 gives various law enforcement and statutory bodies within the IOM the ability to exchange information, where such information would assist them in discharging their functions. The Act also permits Customs and Excise to release information it holds to any agency within or outside the IOM for the purposes of any criminal investigation and proceeding. Such exchanges can be either spontaneous or by request.

The Criminal Justice Acts of 1990 and 1991, as amended, extend the power to freeze and confiscate assets to a wider range of crimes, increase the penalties for a breach of money laundering codes, and repeal the requirement for the Attorney General's consent prior to disclosure of certain information. The law also lowers the standard for seizing cash from "reasonable grounds" to believe that it was related to drug or terrorism crimes to a "suspicion" of any criminal conduct. Assistance by way of restraint and confiscation of a defendant's assets is available under the 1990 Act to all countries and territories designated by Order under the Act. Assistance is also available under the 1991 Act to all countries and territories in the form of the provision of evidence for the purposes of criminal investigations and proceedings. The availability of such assistance is not convention-based nor does it require reciprocity.

All charities operating within the IOM are registered and supervised by the Charities Commission.

The Prevention of Terrorism Act 1990 made it an offense to contribute to terrorist organizations or to assist a terrorist organization in the retention or control of terrorist funds. The IOM Terrorism (United Nations Measure) Order 2001 implements UNSCR 1373 by providing for the freezing of terrorist funds, as well as by criminalizing the facilitating or financing of terrorism. The Government of the IOM enacted the Anti-Terrorism and Crime Act, 2003, which enhances reporting by making the failure to report suspicious transactions relating to money intended to finance terrorism an offense. All other UN and EU financial sanctions have been adopted or applied in the IOM, and are administered by Customs and Excise. Institutions are obliged to freeze affected funds and report the facts to Customs and Excise. In December 2001, the FSC issued revised AML guidance notes that include information relevant to terrorism. IOM authorities are reviewing additional amendments that will incorporate the most recent FATF recommendations and EU directives.

The IOM has developed a legal and constitutional framework for combating money laundering and the financing of terrorism. In 2003, the International Monetary Fund (IMF) examined the regulation and supervision of the IOM's financial sector and found that "the financial regulatory and supervisory system of the Isle of Man complies well with the assessed international standards."

Application of the 1988 UN Drug Convention was extended to the IOM in 1993. In 2003, the U.S. and the UK agreed to extend to the Isle of Man the U.S.-UK Treaty on Mutual Legal Assistance in Criminal Matters.

The IOM cooperates with international anti-money laundering authorities on regulatory and criminal matters. Under the 1990 Criminal Justice Act, the provision of documents and information is available to all countries and territories for the purposes of investigations into serious or complex fraud. Similar assistance is also available to all countries and territories in relation to drug-trafficking and terrorist

investigations. All decisions for assistance are made by the Attorney General of the IOM on a case-by-case basis, depending on the circumstances of the inquiry.

In October 2007, the IOM signed tax information exchange agreements (TIEAs) with each member of the Nordic Council (Denmark, the Faroe Islands, Finland, Greenland, Iceland, Norway, and Sweden) and received commendation from the Organization for Economic Co-operation and Development for its commitment to international standards. The IOM has a fully operational TIEA with the United States and has established protocols with the Internal Revenue Service (IRS) to ensure that information exchange requests are handled smoothly.

Although not a member of the FATF, the Island fully endorses FATF 40 Recommendations and Nine Special Recommendations. The IOM's experts are assisting the FATF working group that considers matters relating to customer identification and companies' issues. The IOM is a member of the Offshore Group of Banking Supervisors (OGBS) and Offshore Group of Insurance Supervisors (OGIS). The FCU belongs to the Egmont Group.

Isle of Man officials should continue to support and educate the local financial sector to help it combat current trends in money laundering. The IOM should act on the 2007 Consultative paper with the MSB/e-money regulation proposals that authorities have discussed, and implement the most effective. The IOM should also ensure that the obliged entities understand and respond to their new and revised responsibilities as delineated by the 2007 AML Code. To this end, the FSC should work to release the Anti-Money Laundering and Terrorist Financing Handbook as soon as possible in 2008. The authorities also should continue to work with international AML authorities to deter financial crime and the financing of terrorism and terrorists.

Israel

Among its Mediterranean neighbors, Israel stands out economically in terms of its high GDP, per capita income, developed financial markets and diverse capital markets. Nevertheless, Israel is not regarded as a regional financial center. It primarily conducts financial activity with the financial markets of the United States and Europe, and to a lesser extent with the Far East. Israeli National Police (INP) intelligence identifies illicit drugs, gambling, extortion, and fraud as the predicate offenses most closely associated with organized criminal activity. Recent studies conducted by the INP Research Department estimate illegal gambling profits at U.S. \$2-3 billion per year and domestic narcotics profits at U.S. \$1.5 billion per year. Human trafficking is considered the crime-for-profit with the greatest human toll in Israel, and public corruption the crime with the greatest social toll. As such, these areas are the targets of the most vigorous anti-money laundering (AML) enforcement activity. Israel does not have free trade zones and is not considered an offshore financial center, as offshore banks and other forms of exempt or shell companies are not permitted. Bearer shares, however, are permitted for banks and/or for companies.

In August 2000, Israel enacted its anti-money laundering legislation, the "Prohibition on Money Laundering Law" (PMLL), (Law No. 5760-2000). The PMLL established a framework for an anti-money laundering system, but required the passage of several implementing regulations before the law could fully take effect. Among other things, the PMLL criminalized money laundering and included 18 serious crimes, in addition to offenses described in the prevention of terrorism ordinance, as predicate offenses for money laundering even if committed in a foreign jurisdiction.

The PMLL also provided for the establishment of the Israeli Money Laundering Prohibition Authority (IMPA) under the Ministry of Justice, as the country's financial intelligence unit (FIU). IMPA became operational in 2002. The PMLL requires financial institutions to report "unusual transactions" to IMPA as soon as possible under the circumstances. Financial institutions must report all transactions that exceed a minimum threshold that varies based on the relevant sectors and the risks that may arise,

with more stringent requirements for transactions originating in a high-risk country or territory. IMPA has access to population registration databases, the Real-Estate Database, records of inspections at border crossings, court files, and Israel's Company Registrar.

In 2001, Israel adopted the Banking Corporations Requirement Regarding Identification, Reporting, and Record Keeping Order. The Order establishes specific procedures for banks with respect to customer identification, record keeping, and the reporting of irregular and suspicious transactions in keeping with the recommendations of the Basel Committee on Banking Supervision. The Supervisor of Banks at the Bank of Israel monitors compliance among banking institutions. Bankers and others are protected by law with respect to their cooperation with law enforcement entities.

Subsequent regulations established the methods of reporting to the Customs Authority (a part of the Israel Tax Authority) monies brought in or out of Israel, and criteria for financial sanctions for violating the law, as well as for appeals. The regulations require the declaration of currency transferred (including cash, travelers' checks, and banker checks) into or out of Israel for sums above 80,000 new Israeli shekels (NIS) (approximately U.S. \$20,000). This applies to any person entering or leaving Israel, and to any person bringing or taking money into or out of Israel by mail or any other methods, including cash couriers. Failure to comply is punishable by up to six months imprisonment or a fine of NIS 202,000 (approximately \$50,500), or ten times the amount that was not declared, whichever is higher. Alternatively, an administrative sanction of NIS 101,000 (approximately U.S. \$25,250), or five times the amount that was not declared, may be imposed by the Committee for Imposition of Financial Sanctions. In 2003, the Government of Israel (GOI) lowered the threshold for reporting cash transaction reports (CTRs) to NIS 50,000 (approximately U.S. \$12,250), lowered the document retention threshold to NIS 10,000 (approximately U.S. \$2,500), and imposed more stringent reporting requirements.

Clarifications to the PMLL were approved in Orders 5761-2001 and 5762-2002 requiring that suspicious transactions be reported by members of the stock exchange, portfolio managers, insurers or insurance agents, provident funds and companies managing a provident fund, providers of currency services, and the Postal Bank. Portfolio managers and members of the stock exchange are supervised by the Chairman of the Israel Securities Authority; insurers and insurance agents are under the authority of the Superintendent of Insurance in the Ministry of Finance; provident funds and companies managed by a provident fund are overseen by the Commissioner of the Capital Market in the Ministry of Finance, and the Postal Bank is monitored by the Minister of Communications. The PMLL does not apply at this time to intermediaries, such as lawyers and accountants.

Other subsequent changes to the PMLL authorized: the issuance of regulations requiring financial service providers to identify, report, and keep records for specified transactions for seven years; the establishment of a mechanism for customs officials to input into the IMPA database; the creation of regulations stipulating the time and method of bank reporting; the creation of rules on safeguarding the IMPA database; and rules for requesting and transmitting information between IMPA, the INP and the Israel Security Agency (ISA, or Shin Bet). The PMLL also imposed an obligation on financial service providers to report any IMPA activities perceived as unusual.

Order 5762 added money services businesses (MSB) to the list of entities required to file cash transaction reports (CTRs) and suspicious transaction reports (STRs) by size and type, and required that they preserve transaction records for at least seven years. The PMLL mandates the registration of MSBs through the Providers of Currency Services Registrar at the Ministry of Finance. A person engaging in the provision of currency services without being registered is liable to one year of imprisonment or a fine of NIS 600,000 (U.S. \$150,000). In 2004, Israeli courts convicted several MSBs for failure to register with the Registrar of Currency Services, and a number of indictments are still pending. The INP and the Financial Service Providers Regulatory Authority maintain a high level

of coordination, routinely exchange information, and have conducted multiple joint enforcement actions.

On July 11, 2007 a draft bill for PMLL (Amendment No. 7) 5776-2007 was published for the purpose of extending Israel's AML regime to the trade in precious stones (including Israel's substantial diamond trading industry). The bill passed the first vote in the Knesset on August 16, and has been submitted to committee for review. The amendment defines "dealers in precious stones" as those merchants whose annual transactions reach NIS 50,000 (approximately U.S. \$11,800). It places significant obligations on dealers to verify the identity of their clients, report all transactions above a designated threshold (and all unusual client activity) to IMPA, as well as to maintain all transaction records and client identification for at least five years. The Customs Authority continues to intercept unreported diamond shipments, despite the fact that Israel imposes no tariffs on diamond imports.

In October 2006, the Knesset Committee on Constitution, Law and Justice approved an amendment to the Banking Order and the Regulations on the Prohibition on Financing Terrorism. The Order and Regulations were additional steps in the legislation intended to combat the financing of terrorism while maintaining correspondent and other types of banking relationships between Israeli and Palestinian commercial banks. Although the amendment to the Order and the Regulations impose serious obligations on banks to examine clients and file transaction reports, banks are still exempted from criminal liability if, inter alia, they fulfill all of their obligations under the Order (though they are not protected from civil liability). The Banking Order was expanded to cover the prohibition on financing terrorism and includes obligations to check the identification of parties to a transaction against declared terrorists and terrorist organizations, as well as obligations to report by size and type of transaction. The Banking Order sets the minimum size of a transaction that must be reported at NIS 5,000 (approximately U.S. \$1,180) for transactions with a high-risk country or territory. The order also includes examples for unusual financial activity suspected to be related to terrorism, such as transfers from countries with no anti-money laundering or counterterrorist finance (AML/CTF) regime to nonprofit organizations (NGOs) within Israel and the occupied territories.

In 2007, Israel took steps to implement Cabinet Decision 4618, passed on January 1, 2006, by creating an interagency "fusion center" and six interagency task forces for pursuing financial crimes. The regulation explicitly instructs the INP and the Shin Bet to target illicit proceeds as a primary objective in the war on organized crime. As Israel does not have legislation preventing financial service companies from disclosing client and ownership information to bank supervisors and law enforcement authorities, the new regulation establishes conditions for the use of such information to avoid its abuse and to set guidelines for the police and security services.

Israel has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets, as well as assets derived from or intended for other serious crimes, including the funding of terrorism and trafficking in persons. The law also allows for civil forfeiture when ordered by the District Court. The identification and tracing of such assets is part of the ongoing function of the Israeli intelligence authorities and IMPA. The INP has responsibility for seizing assets and the State Attorney's Office has authority to freeze assets. Banking institutions cooperate fully, and often freeze suspicious assets according to guidance from the INP and Ministry of Defense. Israel's International Legal Assistance Law enables Israel to offer full and effective cooperation to authorities in foreign states, including enforcement of foreign forfeiture orders in terror financing cases (both civil and criminal).

In December 2004, the Israeli Parliament adopted the prohibition on terrorist financing law 5765-2004, which is geared to further modernize and enhance Israel's ability to combat terrorist financing and to cooperate with other countries on such matters. The Law went into effect in August 2005, criminalizing the financing of terrorism as required by United Nations Security Council Resolution (UNSCR) 1373. The Israeli legislative regime criminalizing the financing of terrorism includes

provisions of the Defense Regulations State of Emergency/1945, the Prevention of Terrorism Ordinance/1948, the Penal Law/1977, and the PMLL. Under the International Legal Assistance Law of 1998, Israeli courts are empowered to enforce forfeiture orders executed in foreign courts for crimes committed outside Israel.

In December 2007, the Knesset Law Committee approved new regulations enabling the declaration by a ministerial committee of foreign designated terrorists, and legally requiring financial institutions to comply with the foreign designations. The National Security Council legal counsel has responsibility for referring foreign designations to the committee for adoption under Israeli law, and is expected to include entities on the UNSCR 1267 Sanctions Committee consolidated list and entities on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. Once designated, identifying information for the terrorist entity is to be published on the Ministry of Defense website, in two daily newspapers, the Official Gazette of the Israeli Government, and distributed by email to financial institutions. Israel already enforces UNSCR 1267 under its Trade with the Enemy Ordinance of 1939, and regularly notifies financial institutions of restricted entities.

The ISA is responsible for investigating terrorist financing offenses, while the Israel Tax Authority handles investigations originating in customs offenses. Under Israeli law, it is a felony to conceal cash transfers upon entry to the West Bank or Gaza, and the agencies coordinate closely to track funds that enter Israeli ports. Customs and the Ministry of Defense also cooperate in combating trade-based terrorist financing, including goods destined for terrorist entities in the West Bank or Gaza.

The INP reports no indications of an overall increase in financial crime relative to previous years. In 2007, IMPA reported 56 arrests and five prosecutions relating to money laundering and/or terrorist financing. In 2007, IMPA received 10,597 suspicious transaction reports. During this period IMPA disseminated 552 intelligence reports to law enforcement agencies and to foreign FIUs in response to requests, and on its own initiative. In addition, eight different investigations yielded indictments (some of them multiple indictments) and ten resulted in convictions or plea bargains. In 2007, the INP seized approximately U.S. \$9 million in suspected criminal assets, a decrease from U.S. \$12 million in 2006 and U.S. \$75 million seized in 2005.

Israel is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. In December 2006 Israel ratified the UN Convention against Transnational Organized Crime. The IMPA is a member of the Egmont Group, and Israel has been an active observer in MONEYVAL since 2006. Israel has signed but not yet ratified the UN Convention against Corruption. Israel is the only nonmember of the Council of Europe to become a party to the European Convention on Mutual Assistance in Criminal Matters (in 1967) and its Second Additional Protocol (in 2006), which is designed to provide more effective and modern means of assisting member states in law enforcement matters. There is a Mutual Legal Assistance Treaty in force between the United States and Israel, as well as a bilateral mutual assistance agreement in customs matters. Customs, IMPA, the INP and the Israel Securities Agencies routinely exchange information with U.S. agencies through their regional liaison offices, as well as through the Israel Police Liaison Office in Washington. In 2007, Israel provided unprecedented assistance in sharing evidence critical to the prosecution of terrorist financing cases in the United States, allowing for the first time the testimony of intelligence agents in U.S. courts.

The Government of Israel continued to make progress in strengthening its anti-money laundering and terrorist financing regime in 2007. Israel should continue the aggressive investigation of money laundering activity associated with organized criminal operations and syndicates. Israel should also continue its efforts to address the misuse of the international diamond trade to launder money by approving draft legislation. Under the new terrorist financing amendment, Israel should adopt appropriate foreign designations of terrorist entities in a timely manner.