



**PREPARED REMARKS OF JAMES H. FREIS, JR.  
DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK  
U.S. DEPARTMENT OF THE TREASURY**

**"GLOBAL MARKETS AND GLOBAL VULNERABILITIES:  
FIGHTING TRANSNATIONAL CRIME THROUGH FINANCIAL INTELLIGENCE"**

Delivered at the Academic Session on "Global Initiatives  
to Avoid the Mis(use) of the Financial System for Illegal Purposes" of the  
Committee on International Monetary Law of the International Law Association  
(MOCOMILA)

**SALAMANCA, SPAIN**

**APRIL 25, 2008**

Today we have gathered in the ancient halls of the University of Salamanca, one of the world's great centers of legal scholarship from centuries past through the present. Among us are some of the leading minds in the fields of international monetary and financial law drawn from about two dozen countries. Your area of scholarship, and the institutions that many of you represent – whether they be central banks, international organizations, leading private sector financial institutions, and the professional corps that supports them – are a testament and daily example of the globalization of the financial markets. But the topic of our academic session today is that the very success of the markets in superseding jurisdictional barriers has also raised vulnerabilities for those who would misuse or abuse the financial system for illegal purposes.

Within the past generation, advances in information technology and telecommunications have been leveraged by the financial industry in this global expansion. Yet the resulting disintermediation has also made it easier for criminals to tap into new institutions and markets without any human contact. Growth in global trade has far outpaced percentage growth in gross domestic product. But does this not also mean that trade-based money laundering – probably the most utilized method for moving illicit value across jurisdictional borders – might be growing in sync? And would this not also open up new avenues for movement of products that could be exploited to produce weapons of mass destruction or their delivery systems? In the currency markets we have seen the successful introduction of the euro and its growing role as a currency for trade, investment and reserves. But do we fully understand the extent to which illicit actors

have altered their cash smuggling from U.S. \$100 banknotes to €500 notes? Immigrant labor has fed demand in fast-growing areas, while sharing some of the benefits back home through increased remittance flows being sent faster and at falling transaction costs. Yet how do we distinguish among these millions of legitimate remittances the transactions that represent repatriation of proceeds from narcotics trafficking or, even worse, contributions to finance terrorist acts?

How do we approach these daunting prospects in attempting to address these global risks and vulnerabilities to money launderers, terrorist financiers and other illicit actors? How can we turn these vulnerabilities of the globalized financial markets into an advantage? I posit to you that there is one small, but specific step in the right direction that we can and must take, but which has not yet been fully appreciated nor broadly understood. As I will explain today, the potential benefit of this tool to address these global risks and vulnerabilities to money launderers, terrorist financiers and other illicit actors has only begun to be exploited (albeit with tremendous initial success) – that is the sharing of financial intelligence through the specialized central agency in each jurisdiction known as a financial intelligence unit (FIU).

The explicit recognition and legal framework for the role of the FIU has become clear only within the past 5 years, and much of the effort to this point has been in capacity building and learning process. Today, I posit that information sharing to combat transnational threats can and should increase enormously in the future.

- With respect to tactical analysis in support of investigations of specific criminal targets, the FIUs have had proven success. In our ever more globalized world, such success will only increase demand, as more countries become actively involved in information sharing, and as law enforcement better understands the power of this unique tool.
- The FIUs need to expand their collaboration beyond mostly reactive work, to be proactive in getting out information about threats to our global partners.
- And finally, but arguably the most important, the greatest benefits for transnational sharing of financial intelligence through FIUs will lie in transnational collaboration on strategic analytical work to understand and begin to address emerging threats and vulnerabilities.

As Director of the Financial Crimes Enforcement Network (FinCEN), the FIU of the United States, I would like today to lay out my vision for the future of how I hope to leverage the resources and authorities at my disposal together with my foreign counterparts as part of global initiatives to combat transnational crime. Before beginning, however, I would like to take a step back and provide an overview of how we have come to where we are today. [I do this with a sense of humility in this great hall, where legal scholars past and present have debated the rule of law with respect to public protection and how police power is one of the most basic principles of organized society.]

## The Relationship Between Money Laundering and Terrorist Financing

I would like to emphasize that for the purpose of today's discussion on the importance of the transnational sharing of financial intelligence, the benefits apply both in the areas of fighting the laundering of money that is the proceeds of crime and in combating the financing of terrorism. A lot of emphasis has been placed upon the fact that terrorism might be financed out of funds that have been derived from legitimate economic activity, moved in transactions that themselves are neither large in value nor out of the ordinary, and as such would not be detectable by financial institutions. Indeed the 9/11 Commission concluded that "[t]he 9/11 plotters eventually spent somewhere between \$400,000 and \$500,000 to plan and conduct their attack."<sup>1</sup> Although the hijackers used U.S. bank accounts in their own names, there was no reason to raise suspicion among the banks involved.<sup>2</sup>

In efforts to detect, prevent and penalize both money laundering and terrorist financing, it is critical to "follow the money." Most criminal activity is motivated by financial gain, which leads to the laundering of proceeds. With respect to terrorist financing, I would like to quote statements from a few weeks ago, on April 1, 2008, by U.S. Treasury Under Secretary for Terrorism and Financial Intelligence, Stuart Levey, in testimony before Congress for the U.S. Senate Finance Committee.<sup>3</sup>

The real value of all of our counter-terrorist financing efforts is that they provide us with another means of maintaining persistent pressure on terrorist networks. Terrorist networks and organizations require real financing to survive. The support they require goes far beyond funding attacks. They need money to pay operatives, support their families, indoctrinate and recruit new members, train, travel, and bribe officials. When we restrict the flow of funds to terrorist groups or disrupt a link in their financing chain, we can have an impact.

With respect to the terrorist group that poses the greatest threat to the United States, al Qaida, we have made real progress. We have disrupted or deterred many of the donors on which al Qaida used to rely. At the very least, these donors are finding it far more difficult to fund al Qaida with the ease and efficiency provided by the international financial system. The same applies to many of the charities that al Qaida previously depended upon as a source of funds. To the extent we can force terrorists and their supporters out of the formal financial system, we force

---

<sup>1</sup> National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report at 169, available at <http://govinfo.library.unt.edu/911/report/index.htm>.

<sup>2</sup> *See id.* at 237 ("The hijackers made extensive use of banks in the United State, choosing both branches of international banks and smaller regional banks. All of the hijackers opened accounts in their own name, and used passports and other identification documents that appeared valid on their face. . . . While the hijackers were not experts on the use of the U.S. financial system, nothing they did would have led the banks to suspect criminal behavior, let alone a terrorist plot to commit mass murder."<sup>16</sup> *and* at 528, n.116 ("Contrary to persistent media reports, no financial institution filed a suspicious activity report (SAR) . . . with respect to any transaction of any of 19 hijackers before 9/11. . . . Nor should they have been filed. The hijackers' transactions themselves were not extraordinary or remarkable.").

<sup>3</sup> <http://www.treas.gov/press/releases/hp898.htm>.

them into more cumbersome and riskier methods of raising and moving money, subjecting them to a greater likelihood of detection and disruption.

Terrorist financiers attempt to use the global markets and their vulnerabilities to their advantage in the same fashion as money launderers. In particular, they seek to hide behind anonymity and conceal their sources.<sup>4</sup> This in turn makes them susceptible to some of the same tools in trying to track them down. Moreover, with respect to organized terrorist groups, the differences from organized criminal activity have become blurred in many cases where ill-gotten gains are a major source of funding.<sup>5</sup> In actuality, this has been understood and recognized under international law for some time.

The United Nations General Assembly recognized in 1996 that with respect to measures designed to fight international terrorism that strengthen international cooperation, including information exchange to combat terrorism, among the sources of terrorist funding were organizations “engaged in unlawful activities such as illicit arms trafficking, drug dealing and racketeering, including the exploitation of persons for purposes of funding terrorist activities.”<sup>6</sup>

---

<sup>4</sup> See Paul Allen Schott, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, The World Bank and International Monetary Fund, Washington, DC (2d ed. 2006) at I-5, available at [http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference\\_Guide\\_AMLCFT\\_2ndSupplement.pdf](http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf), (“The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. Funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.”).

<sup>5</sup> See FATF, Terrorist Financing (2008) at 15, available at <http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf>, (“Terrorist use of criminal activity to raise funds ranges from low-level fraud to involvement in serious and organised crime.”). This report provided more details from actual cases provided by multiple countries related to terrorism funding from narcotics trafficking, credit card fraud, check fraud, and extortion of diaspora communities.

<sup>6</sup> See General Assembly Resolution A/RES/51/210, “Measures to eliminate international terrorism” (December 17, 1996), art. 3:

Calls upon all States to adopt further measures in accordance with the relevant provisions of international law, including international standards of human rights, to prevent terrorism and to strengthen international cooperation in combating terrorism and, to that end, to consider the adoption of measures such as those contained in the official document adopted by the group of seven major industrialized countries and the Russian Federation at the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the plan of action adopted by the Inter-American Specialized Conference on Terrorism, held at Lima from 23 to 26 April 1996 under the auspices of the Organization of American States, and in particular calls upon all States:

(f) To take steps to prevent and counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations, whether such financing is direct or indirect through organizations which also have or claim to have charitable, social or cultural goals or which are also engaged in unlawful activities such as illicit arms trafficking, drug dealing and racketeering, including the exploitation of persons for purposes of funding terrorist activities, and in particular to consider, where appropriate, adopting regulatory measures to prevent and counteract movements of funds suspected to be intended for terrorist purposes without impeding in any way the freedom of legitimate capital movements and to intensify the exchange of information concerning international movements of such funds[.]

The United Nations Security Council has created universal obligations upon states to combat the financing of terrorism, but a review of some of the earlier resolutions with respect to Afghanistan and the Taliban shows the connection between the criminal activity related to narcotics trafficking as a source of terrorism funding. UNSCR 1333 of 2000 “Demand[ed] that the Taliban, as well as others, halt all illegal drugs activities and work to virtually eliminate the illicit cultivation of opium poppy, the proceeds of which finance Taliban terrorist activities.”<sup>7</sup> That resolution in part amended UNSCR 1267 of 1999, which was groundbreaking in the obligations placed upon States, which ultimately then fell upon the financial industry, to freeze terrorist funds in particular for listed persons.<sup>8</sup> But even before the obligation to freeze assets, the Security Council had already recognized that much of the Taliban assets were likely derived from illegal narcotics activities.<sup>9</sup>

Yet another example is the Revolutionary Armed Forces of Colombia (FARC), a notorious narco-terrorist organization. Under U.S. law, the FARC has been designated and subjected to sanctions not only as a significant foreign narcotics trafficker, but also as a Foreign Terrorist Organization and as a Specially Designated Global Terrorist.<sup>10</sup>

And even more isolated radical groups may seek to fund terrorist acts from criminal proceeds. Here in Spain, we cannot forget the tragedy of what is known here as 11-M, when four years ago on March 11, a series of bomb blasts on commuter trains left 191 dead and over 1800 injured. Early speculation of ties to al-Qaida or the separatist ETA was later dismissed. A month after the bombings, the global press carried the statements of Ángel Acebes, the Acting Interior Minister (who happens to be a graduate of the University of Salamanca faculty of law, which hosts the event at which I am speaking today) that the terrorists financed their plot, including paying for their

---

Available at <http://www.un.org/documents/ga/res/51/a51r210.htm>.

<sup>7</sup> UNSCR 1333 (2000) art. 9.

<sup>8</sup> See UNSCR 1267 (1999) art. 4: “Decides further that, in order to enforce paragraph 2 above, all States shall:

\* \* \*

“(b) Freeze funds and other financial resources, including funds derived or generated from property owned or controlled directly or indirectly by the Taliban, or by any undertaking owned or controlled by the Taliban, as designated by the Committee established by paragraph 6 below, and ensure that neither they nor any other funds or financial resources so designated are made available, by their nationals or by any persons within their territory, to or for the benefit of the Taliban or any undertaking owned or controlled, directly or indirectly, by the Taliban, except as may be authorized by the Committee on a case-by-case basis on the grounds of humanitarian need.”

<sup>9</sup> See UNSCR 1193 (1998) art. 15 (“Demands the Afghan factions to refrain from harbouring and training terrorists and their organizations and to halt illegal drug activities.”); and UNSCR 1214 (1998) art. 13 (“Demands also that the Taliban stop providing sanctuary and training for international terrorists and their organizations, and that all Afghan factions cooperate with efforts to bring indicted terrorists to justice.”) and art. 14 (“Demands further that the Taliban, as well as others, halt the cultivation, production and trafficking of illegal drugs.”).

<sup>10</sup> See United States Treasury Department Press Release, Treasury Targets FARC Financial Network in Colombia (January 15, 2008), available at <http://www.treasury.gov/press/releases/hp762.htm>.

apartment, with sales of drugs and even swapped narcotics for the explosive materials themselves.<sup>11</sup>

### **Global Threats Require a Concerted National and International Approach**

Faced with the foregoing, it is important that we find ways to best leverage the experience and law enforcement framework that has been developed to combat crime in significant part by tracing the financial proceeds, in ways that can also be used to combat the hopefully less common instances of financing of terrorism. This applies both within each jurisdiction, but increasingly on a transnational scale. I recognize that there is a perception outside the United States that my country takes an aggressive stance in the fight against money laundering and in particular terrorist financing, but I would like to emphasize that the U.S. Government very much favors a multinational approach. Rather than repeating details with which the audience today is very familiar – about the international consensus on the need for global implementation of international anti-money laundering and countering the financing of terrorism (AML/CFT) standards, I would instead wish to reiterate the commitment to them.

In the recent testimony of Under Secretary Levey which I mentioned earlier,<sup>12</sup> he touched on the critical role that the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, of which FinCEN is a part, plays in protecting U.S. national security; which in turn enhances our economic security and global prosperity.

Given the global nature of the financial system, focusing only on the U.S. financial system and its AML/CFT regime is not sufficient. Safeguarding the U.S. financial system requires global solutions and effective action by financial centers throughout the world. We work toward this objective through multilateral bodies that set and seek to ensure global compliance with strong international standards.

The Treasury Department primarily advances this strategic objective through the Financial Action Task Force (FATF), which articulates standards in the form of recommendations, guidelines, and best practices. The FATF standards have been recognized by more than 175 jurisdictions and have been integrated into the work of international organizations such as the United Nations, the World Bank and the International Monetary Fund.<sup>13</sup> The FATF seeks global implementation of its standards through a

---

<sup>11</sup> See Dale Fuchs, "Spain Says Bombers Drank Water From Mecca and Sold Drugs," The New York Times (April 14, 2004) ("The Islamic terrorists responsible for the Madrid train bombings financed their plot with sales of hashish and Ecstasy and drank holy water from Mecca in ritual 'purification acts' before the attacks, the acting interior minister, Ángel Acebes, said Wednesday. . . . the bombers swapped the drugs for the 440 pounds of dynamite used in the blasts. . . . Mr. Acebes said the man in charge of the group's finances was Jamal Ahmidan, a 33-year-old Moroccan immigrant with an 'extensive criminal record for drug trafficking.' . . . Money from the drug trafficking paid for an apartment hide-out, a car and the cellphones used to detonate the bombs, an Interior Ministry spokesman said.")

<sup>12</sup> <http://www.treas.gov/press/releases/hp898.htm>.

<sup>13</sup> [http://www.fatf-gafi.org/document/28/0,3343,en\\_32250379\\_32236930\\_33658140\\_1\\_1\\_1\\_1.00.html](http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1.00.html)

number of mechanisms. Partnership with the IMF, World Bank and FATF-Style Regional Bodies ensures that every country in the world is assessed against the same standards using the same methodology. AML/CFT is one of twelve core standards used by the IMF to evaluate financial sector stability and is the sole required standard for all countries. As of September 2007, the IMF had conducted 50 assessments -- four of which were done jointly with the World Bank -- of country compliance with AML/CFT standards. These assessments highlight the key deficiencies for countries seeking to improve their AML/CFT standards. We have seen steady progress in legislation by countries to address their deficiencies identified in their assessments. Assessments also highlight deficiencies in a way that is useful to the private sector in assessing risk.

### **Partnership with the Financial Industry in Developing Financial Intelligence**

These international financial standards are premised upon close cooperation between the financial industry and the public sector in order to combat the abuse of the financial system for money laundering, terrorist financing and other illicit activity. It may be a bit of an oversimplification, but to me the obligations and responsibilities upon financial institutions essentially can be grouped into two categories: (i) efforts to make their institutions hostile to abuse by criminal actors, and (ii) the providing of information regarding financial transactions to the government.

The former category includes what is known as customer due diligence – to know the customer to whom the bank or other financial intermediary is providing financial services, as most financial institutions would not wish to promote illicit activity. In order to make this happen, financial institutions are required to develop AML/CFT compliance programs with dedicated and trained professionals, and to provide for independent review of those programs. The AML/CFT programs directly contribute to the quality of the data on financial transactions that are provided to the government – e.g., because a bank has been diligent in requiring proper identification of its customer, a law enforcement agent can often rely on a report from that bank to correctly identify an individual at issue.

Countries differ in the financial information that they require by regulation to be reported by financial institutions. The most universal type of reporting is with respect to suspicious transactions (STRs) or Suspicious Activity Reports (SARs) as they are known in the United States. FATF Recommendation 13 states:

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

It is critical that the financial industry not only be compelled by law to devote the necessary resources to its reporting obligations, but also that the industry understands and is able to take comfort in the specific and necessary purposes for which they bear these

costs and dedication of resources. This requires that the government protect the reported information and use it appropriately, as it contains sensitive commercial and personal information. With respect to SARs, it has been recognized that even greater protections are merited to foster as open a flow of information as possible about suspected illegal or at least unexplainable activity with respect to a given customer. FATF Recommendation 14 provides that financial institutions should be protected under national law from any civil or criminal liability for the filing of a SAR, and should not even reveal the existence of a SAR filing.<sup>14</sup>

Other information that is often reported by financial institutions to the FIU is with respect to cash transactions, often above a certain threshold.<sup>15</sup> This is in recognition of the fact that criminals often try to exploit the anonymity of cash.<sup>16</sup> More recently, certain countries have begun requiring financial institutions to report information on cross-border funds transfers.

This information stream becomes more valuable than the sum of individual data points when government analysts can combine not only the insights of multiple different reporting entities in the financial industry over time, but also leverage information technology and telecommunications to combine this information with other data, whether from law enforcement or intelligence community sources, and other public or commercially available information. It is through careful and experienced analysis that the individual points of data can be turned into financial intelligence that aids in criminal and counterterrorism investigations as law enforcement “follows the money.”

### **Defining the Role of the Financial Intelligence Unit (FIU)**

Now working from the presumption of the value to law enforcement of financial intelligence, how in practice can we put information from the financial industry to use, especially in an international context, to address global vulnerabilities and fight

---

<sup>14</sup> FATF Recommendation 14 provides:

Financial institutions, their directors, officers and employees should be:

- a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.
- b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

<sup>15</sup> For a recent overview of cash transaction reporting requirements in the United States and law enforcement uses of this information, see United States Government Accountability Office, Bank Secrecy Act: Increased Use of Exemption Provisions Could Reduce Currency Transaction Reporting While Maintaining Usefulness to Law Enforcement Efforts (February 2008), available at <http://www.gao.gov/new.items/d08355.pdf>.

<sup>16</sup> See FATF Recommendation 24:

Countries should further encourage in general the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book entry recording of securities, as a means to *encourage the replacement of cash transfers*.

(emphasis added).

transnational crime? A consensus has emerged that a key role in this effort should be played by the respective FIU in each jurisdiction.

It is quite rare that international law prescribe how states should carry out particular sovereign functions, and even rarer that international law would have some limited view into the way a government organizes its agencies to carry out certain sovereign functions. (For many in the audience here today, I must ask you to set aside your expertise in the field of central banking, which in the past generation has grown to be one of the primary exceptions to the general proposition just stated.) Yet while some aspects of international law develop over centuries, the consensus over the specific role for an FIU within a country's legal system, and as a predicate to international cooperation in the AML/CFT area, developed within the past dozen years.

In June 1995, a group of government agencies and international organizations gathered at the Egmont-Arenberg Palace in Brussels to discuss money laundering and ways to confront this global problem. They established a Legal Working Group to examine obstacles to the cross-border exchange of financial intelligence. In 1996, they adopted a definition of an FIU (slightly revised in 2004 to extend the focus from money laundering to explicitly reference terrorism financing):

A central, national agency responsible for receiving, (and as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information:

- (i) concerning suspected proceeds of crime and potential financing of terrorism, or
- (ii) required by national legislation or regulation, in order to combat money laundering and terrorism financing.<sup>17</sup>

The few agencies in place that acted more or less consistently with this definition continued meeting on an informal basis after the 1995 gathering in what became known as the "Egmont Group" (discussed in more detail below).

The United Nations Convention Against Transnational Organized Crime (Palermo Convention) of 2000 essentially adopted this definition and urged countries, among other measures, to combat money laundering and, in particular, the exchange of information internationally to create an FIU. Article 7 of the Convention states that each Member State "shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering."<sup>18</sup> That UN Convention entered into force on September

---

<sup>17</sup> See Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit, available at [http://www.egmontgroup.org/files/library\\_egmont\\_docs/egmont\\_final\\_interpretive.pdf](http://www.egmontgroup.org/files/library_egmont_docs/egmont_final_interpretive.pdf).

<sup>18</sup> See United Nations Convention Against Transnational Organized Crime, available at <http://untreaty.un.org/English/notpubl/18-12E.htm>. Article. 7, "Measures to combat money-laundering," reads in relevant part: "1. Each State Party:

"(b) Shall, without prejudice to articles 18 and 27 of this Convention, ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money-laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and

29, 2003 and currently has 147 signatories and 143 parties that have completed ratification.<sup>19</sup> The United Nations Convention Against Corruption of 2003 contains identical language with respect to the potential role of the FIU.<sup>20</sup>

While the original FATF Recommendations from 1990 as revised in 1996 stated that countries should “consider” the concept of a “national central agency” to receive reports of financial transactions,<sup>21</sup> it was in the 2003 revisions that the specific role of the FIU was made explicit. FATF Recommendation 26 now reads:

Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

Once again, somewhat unique in international law, there has been a global effort to establish FIUs as operational entities within countries. The Anti-Money-Laundering Unit (AMLU) of the United Nations Office on Drugs and Crime (UNODC), as part of its Global Programme against Money-Laundering (GPML), provides AML/CFT technical assistance consistent with UN-related instruments and worldwide accepted standards. The GPML has developed, in collaboration with UNODC's Legal Advisory Section and International Monetary Fund (IMF), model laws for both *common law* and *civil law* legal systems that include the establishment of an FIU.<sup>22</sup>

In the United States, FinCEN was established in 1990 as an office within the Department of the Treasury.<sup>23</sup> It was under the USA PATRIOT Act of 2001, however, that its functions were statutorily formalized as a bureau within the Treasury Department.<sup>24</sup> FinCEN's responsibilities to receive, analyze, and disseminate financial

---

exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering.”

<sup>19</sup> See United Nations Convention Against Corruption, art. 14(1)(b), available at <http://www.unodc.org/unodc/en/treaties/CTOC/signatures.html>.

<sup>20</sup> See [http://www.unodc.org/pdf/corruption/publications\\_unodc\\_convention-e.pdf](http://www.unodc.org/pdf/corruption/publications_unodc_convention-e.pdf).

<sup>21</sup> See 1996 FATF Recommendation 23:

Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerized data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information.

Available at <http://www.fatf-gafi.org/dataoecd/15/51/40262612.pdf>.

<sup>22</sup> See <http://www.unodc.org/unodc/en/money-laundering/Model-Legislation.html>.

<sup>23</sup> Treasury Order 105-08, “Establishment of the Financial Crimes Enforcement Network,” (April 25, 1990).

<sup>24</sup> See Treasury Order 180-01, “Financial Crimes Enforcement Network,” (September 26, 2002), art. 1 (“By virtue of the USA PATRIOT Act of 2001 (Pub. L. No. 107-56, Title III, Subtitle B, Section 361(a)(2), 115 Stat. 272, 329-332), and by the authority vested in me as Secretary of the Treasury, it is hereby ordered that

intelligence for AML/CFT purposes and to coordinate with foreign FIUs were codified into law.<sup>25</sup>

Within the European Union, all Member States had an agency conducting some FIU functions by no later than 2000.<sup>26</sup> In 2005 this was more formally enshrined in Community law in the Third Money Laundering Directive, which states unequivocally: “Each Member State shall establish a FIU to combat money laundering and terrorist financing.”<sup>27</sup>

## The Egmont Group – An International FIU Network

As per the above definition, the FIU is responsible for receiving, analyzing and disseminating to other government authorities - in particular law enforcement investigatory agencies and criminal prosecutorial authorities - the financial information

---

the Financial Crimes Enforcement Network (“FinCEN” or the “Bureau”) is re-established as a bureau within the Department.”).

Pub. L. 107-56 (2001), art.

<sup>25</sup> See 31 U.S.C. § 310(b) Director.—

(1) Appointment.— The head of FinCEN shall be the Director, who shall be appointed by the Secretary of the Treasury.

(2) Duties and powers.— The duties and powers of the Director are as follows:

\* \* \*

(B) Maintain a government-wide data access service, with access, in accordance with applicable legal requirements, to the following:

(i) Information collected by the Department of the Treasury, including report information filed under subchapter II of chapter 53 of this title (such as reports on cash transactions, foreign financial agency transactions and relationships, foreign currency transactions, exporting and importing monetary instruments, and suspicious activities) . . . .

\* \* \*

(C) Analyze and disseminate the available data . . . to—

(i) identify possible criminal activity to appropriate Federal, State, local, and foreign law enforcement agencies;

\* \* \*

(v) determine emerging trends and methods in money laundering and other financial crimes;

(vi) support the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism; and

(vii) support government initiatives against money laundering.

\* \* \*

(H) Coordinate with financial intelligence units in other countries on anti-terrorism and anti-money laundering initiatives, and similar efforts.

<sup>26</sup> See Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information. O.J. L 271, 24 October 2000, p. 4–6, available at [http://eur-lex.europa.eu/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000D0642&model=guichett](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000D0642&model=guichett), perambulatory para. 2 (“All Member States have set up financial intelligence units (FIUs) to collect and analyse information received under the provisions of Directive 91/308/EEC with the aim of establishing links between suspicious financial transactions and underlying criminal activity in order to prevent and to combat money laundering.”).

<sup>27</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, O.J. L 309 /15 (25 November 2005) art. 21(1).

that has been reported by financial institutions for AML/CFT purposes. There are different models under which an FIU can be incorporated within the governmental structure of a particular jurisdiction. The most common, and the form of my agency, FinCEN, is the “Administrative Model.” “The Administrative Model is a centralized, independent, administrative authority, which receives and processes information from the financial sector and transmits disclosures to judicial or law enforcement authorities for prosecution. It functions as a ‘buffer’ between the financial and the law enforcement communities.”<sup>28</sup> Many administrative FIUs are situated within the government framework of the finance ministry or central bank, particularly where the central bank also retains supervisory functions.

The next most common model is the “Law Enforcement Model [which] implements anti-money laundering methods alongside already existing law enforcement systems, supporting the efforts of multiple law enforcement or judicial authorities with concurrent or sometimes competing jurisdictional authority to investigate money laundering.”<sup>29</sup> Additionally, there are judicial and hybrid models. The point to be stressed, however, is that each jurisdiction must have a single government agency to carry out the responsibilities with respect to information exchange with FIU counterparts from other jurisdictions.

The Egmont Group has grown considerably from its first gathering in June 1995, as the FIUs increasingly focused on nurturing the exchange of information available within their respective countries. In its Statement of Purpose, adopted at the fifth plenary meeting in 1997, the Egmont Group agreed to pursue among its priorities the stimulation of information exchange and to overcome the obstacles preventing cross-border information sharing. In the Principles for Information Exchange adopted in 2001, the Egmont Group stated, *inter alia*:

FIUs should be able to exchange information freely with other FIUs on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and the requesting party. Such exchange, either upon request or spontaneously, should produce any available information that may be relevant to an analysis or investigation of financial transactions and other relevant information and the persons or companies involved.<sup>30</sup>

The membership continued to focus on progress on the legal and practical aspects of promoting information exchange, as exhibited in the 2004 Best Practices for the Exchange of Information Between Financial Intelligence Units.<sup>31</sup> They focused on the development of standard Memoranda of Understanding, which albeit is non-binding as a matter of law, formalized the importance of reciprocity of treatment. Among the

---

<sup>28</sup> See Egmont Information Paper on Financial Intelligence Units and the Egmont Group (September 2004) at 2, available at [http://www.egmontgroup.org/files/library\\_egmont\\_docs/info\\_paper\\_final\\_oct\\_2004.pdf](http://www.egmontgroup.org/files/library_egmont_docs/info_paper_final_oct_2004.pdf).

<sup>29</sup> See *id.*

<sup>30</sup> Egmont Group, Principles for Information Exchange Between Financial Intelligence Units and Terrorism Financing Cases, The Hague, 13 June 2001, art. 9, available at [http://www.egmontgroup.org/princ\\_info\\_exchange.pdf](http://www.egmontgroup.org/princ_info_exchange.pdf).

<sup>31</sup> Available at <http://www.egmontgroup.org/bestpractices.pdf>.

resources they created was the Egmont Secure Web, a secure internet-based mechanism (hosted by FinCEN) for the exchange and communication of sensitive information. Similar systems are now being developed, such as FIU.Net, for use among the EU Member State FIUs. The Egmont Group is working in collaboration with this system in order to maximize information sharing.

The de facto recognition of the initial success and potential for the FIU model of information sharing came to be reflected in the international financial standards mentioned above. For example, as the attention turned to this newly defined need for an FIU five years ago, the IMF undertook a review, the purpose of which was “to respond to the need for information on FIUs.”<sup>32</sup> The IMF concluded:

FIUs are an essential component of the international fight against money laundering, the financing of terrorism, and related crime. Their ability to transform data into financial intelligence is a key element in the fight against money laundering and the financing of terrorism. The place of FIUs is now well established in the arsenal of measures to combat these serious crimes.<sup>33</sup>

In addition to the 2003 FATF Recommendation 26 specifically calling for each country to create an FIU, the Interpretative Note to Recommendation 26 states:

Where a country has created an FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.

Moreover, the 2003 FATF Recommendations were significantly revised to focus on international information sharing among competent authorities including FIUs, specifically in Recommendation 40:

Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. . . .<sup>34</sup>

---

<sup>32</sup> See International Monetary Fund, *Financial Intelligence Units: An Overview* (2004), available at <http://www.imf.org/external/pubs/ft/FIU/index.htm>, at 2 (“The purpose of this handbook is to respond to the need for information on FIUs.”)

<sup>33</sup> See *id.* at 91.

<sup>34</sup> See also Interpretative Note to Recommendation 40, para. 4:

FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

In 2007, membership in the Egmont Group had grown to 106 members, reflecting the dramatic increase in the number of jurisdictions from which either newly established or significantly enhanced agencies have sought recognition of their operational status as financial intelligence units. The informal model of coordination had also become increasingly unwieldy. For that reason, the members decided to establish a more formal structure.

At the 2007 plenary, the member FIUs adopted a Charter which states the following as the “Objectives of the Egmont Group”:

The goal of the Egmont Group is to provide a forum for FIUs around the world to improve co-operation in the fight against money laundering and financing of terrorism and to foster the implementation of domestic programs in this field.

This support includes:

- expanding and systematizing international co-operation in the reciprocal exchange of information;
- increasing the effectiveness of FIUs by offering training and promoting personnel exchanges to improve the expertise and capabilities of personnel employed by FIUs;
- fostering better and secure communication among FIUs through the application of technology, such as the Egmont Secure Web (ESW);
- fostering increased coordination and support among the operational divisions of member FIUs; and
- promoting the establishment of FIUs in conjunction with jurisdictions with an AML/CFT program in place or in areas with a program in the early stages of development.

The Egmont Group also created a permanent Secretariat located in Toronto, Canada, on the basis of a host arrangement of the Government of Canada granting the Secretariat and its officials privileges and immunities.

Supported by the permanent Secretariat, the Egmont Group Charter has now institutionalized the working framework for its membership. The Egmont Committee, a group of 14 members, is an intermediary group between the 106 Heads of member FIUs and the five Egmont Working Groups. This Committee addresses the administrative and operational issues facing Egmont and is comprised of seven permanent members and seven regional representatives based on continental groupings (i.e., Asia, Europe, the Americas, Africa and Oceania). Egmont’s five Working Groups are broken down into

---

Searching its own databases, which would include information related to suspicious transaction reports.

Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

Where permitted to do so, FIUs should also contact other competent authorities and financial institutions in order to obtain relevant information.

Legal, Operational, Training, Information Technology and Outreach (responsible for potential candidate FIUs).

### **FIU Information Sharing in Action**

I will now turn to more practical examples of what it means in practice to share financial intelligence among FIUs and the benefits to this mechanism for combating global threats of money laundering and terrorist financing. In summary, the advantages of FIU exchanges can be characterized by a common purpose, but also financial analytical expertise, speed, and confidentiality.

With respect to analytical work, FIUs must be experts in understanding and interpreting the financial information that is reported to them from financial institutions in the context of all other data available to them. The importance of this specialization over time cannot be underestimated, particularly as compared to the FIU's domestic counterparts in law enforcement and prosecutorial authorities who are often generalists dealing with a range of criminal cases without necessarily specializing in financial transactions. This has become increasingly apparent as the financial markets become ever more complex in a globalized world. Moreover, vulnerabilities to criminal abuse are increasingly seen in emerging payment technologies and there has been an increased focus in recent years on AML/CFT compliance obligations for banks with respect to correspondent banking.<sup>35</sup>

There is a generally accepted distinction between what is known as tactical and strategic analysis, with the application of financial expertise having the potential to become geometrically more valuable with respect to the latter. Tactical analysis in its simplest form involves the matching of data. For example, if the police have identified a criminal suspect, they will seek to search against all available databases to obtain further identifier information, such as full name, address, date of birth, social insurance, passport or other unique identifier number. In addition to any of the foregoing, the databases of financial information available to FIUs may also contain with respect to that suspect information on bank accounts, including co-owners, and specific transactions. This information can be immensely valuable in "following the money" and in identifying ill-gotten gains for civil or criminal forfeiture proceedings.

While sometimes fairly straightforward, tactical information can be very difficult to obtain with respect to a foreign suspect were it not for the assistance of a foreign FIU. For example, if a suspected criminal is wiring funds from his bank to the account of a corporation abroad, it would be incredibly useful to law enforcement to know whether the recipient is a legitimate entity as opposed to a front company for which the criminal himself is a disguised beneficial owner merely seeking to hide funds overseas.<sup>36</sup>

---

<sup>35</sup> See, e.g., FATF Revised Interpretative Note to Special Recommendation VII: Wire Transfers (February 2008), available at <http://www.fatf-gafi.org/dataoecd/16/34/40268416.pdf>.

<sup>36</sup> For a description of how FinCEN processes requests from foreign FIUs, see FATF, Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism: United States of America (June 23, 2006), paras. 1196, 1997, available at <http://www.fatf-gafi.org/dataoecd/44/9/37101772.pdf>.

In its Fiscal Year 2007, FinCEN reached an all-time record of 855 information sharing requests received from other Egmont Group FIUs. In a strong effort to eliminate a backlog of requests carried over from the previous year, FinCEN actually responded to 949 separate FIU requests. For many FIUs, FinCEN is a significant partner in terms of volume of exchange of information, reflecting in significant part the size and importance of the U.S. financial markets and transactions in dollars. Additionally, FinCEN works with U.S. law enforcement agencies to initiate requests of foreign FIUs to obtain additional intelligence from abroad for ongoing financial crime cases and investigations. Last year there were a total of 167 such requests from U.S. domestic law enforcement that resulted in 323 referrals (one case might lead to a referral to more than one FIU in different jurisdictions) to a total of 82 different FIUs over the course of the year.<sup>37</sup>

In contrast to tactical analysis, strategic analysis is undertaken not with respect to a particular criminal target, but rather to analyze or discover particular trends or patterns, such as on a regional basis, over time, or with respect to vulnerabilities in particular products or industries. Examples where FinCEN has made public its analysis (in addition to many non-public studies containing more sensitive analysis for law enforcement) include recent studies with respect to mortgage fraud,<sup>38</sup> suspicious activity reporting by the insurance industry,<sup>39</sup> and domestic limited liability companies.<sup>40</sup>

With respect to the timing of cross-border information sharing, it is particularly illuminative to consider what other options might be available for a law enforcement authority to obtain information from a counterpart in another jurisdiction. I caution that the Egmont exchange of information is generally limited to lead information (analogous to a “tip”) that is not necessarily admissible in court as evidence, meaning that the FIU request will not necessarily end the resort to other means, but the FIU sharing process most certainly is meant to facilitate quick assistance in support of criminal investigations.

---

1196. After the initial screening process is complete, an analyst is assigned to the case. The assigned FinCEN analyst is responsible for making all relevant queries on the subjects named in the request, expanding their research as necessary (and as agreed upon) to include any ‘new’ entities that are identified through the research. Queries are made on all commercial databases, financial databases and law enforcement databases to which FinCEN has access. If other agencies have requested data on the same entities (and all parties agree), FinCEN can facilitate networking amongst the agencies involved (i.e. by sharing the contact names and telephone numbers of the other requesting agencies).

1197. In general, based on the needs of the requesting agency, FinCEN can provide a foreign FIU with three types of data: commercial data (public record information); financial data (BSA information); and law enforcement data (foreign travel, criminal history, and driver history records). FinCEN prepares a report that summarizes its findings and forwards it to the requester.

<sup>37</sup> See FinCEN, Annual Report for 2007, at 33, available at

<http://www.fincen.gov/AnnualReportFY2007.pdf>.

<sup>38</sup> FinCEN, Mortgage Loan Fraud: An Update of Trends Based Upon an Analysis of Suspicious Activity Reports (April 2008), available at <http://www.fincen.gov/MortgageLoanFraudSARAssessment.pdf>.

<sup>39</sup> FinCEN, Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings (April 2008), available at [http://www.fincen.gov/Insurance\\_Industry\\_SAR.pdf](http://www.fincen.gov/Insurance_Industry_SAR.pdf).

<sup>40</sup> FinCEN, The Role of Domestic Shell Companies in Financial Crime and Money Laundering: Limited Liability Companies (November 2006), available at [http://www.fincen.gov/LLCAssessment\\_FINAL.pdf](http://www.fincen.gov/LLCAssessment_FINAL.pdf).

In recognition of the first speaker at today's session, Mr. Mariano Simancas, Head of Serious Crime at Europol, I should note that the European Council has decided explicitly that in promoting the exchange of information among Member State FIUs, that this would not substitute for the Member State obligations towards Europol.<sup>41</sup> It remains the case, however, that a request under a Mutual Legal Assistance Treaty or from one judicial authority to another pursuant to letters rogatory could take months or even years for a response. In comparison, under the Egmont Group's Best Practices, a response should be provided within a month, with urgent requests such as those related to terrorism investigations often answered within a matter of days.

I am proud to be able to say here today that FinCEN "worked closely with the Spanish FIU following the Madrid bombing."<sup>42</sup> It is also public information that FinCEN "offered assistance to the British FIU following the subway and bus bombings in London" on July 7, 2005 ("7/7").<sup>43</sup> "FinCEN routinely serves as an intermediary between U.S. law enforcement and its FIU counterparts by requesting information on terrorism-related investigations. All requests from foreign FIUs relating to terrorism or terrorist funding receive immediate attention and comprehensive research and analysis."<sup>44</sup> The dedicated men and women of FinCEN need no encouragement in this role,<sup>45</sup> and we will continue to do the utmost within our authority together with our law enforcement and intelligence community partners to collaborate with counterpart FIUs to prevent and investigate terrorist attacks.

Finally, it is critical to emphasize the importance of confidentiality and protection of the sensitive commercial, financial, and personal information that is entrusted to FIUs. While initially one might consider this a problem for international sharing among FIUs, instead the Egmont Group has worked to ensure protections that have led to the promotion of the FIU channels as a preferred legal means for the cross-border sharing of information.

FATF Recommendation 4 states that "Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations."

---

<sup>41</sup> See Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information. O.J. L 271, 24 October 2000, p. 4-6, available at [http://eur-lex.europa.eu/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000D0642&model=guichett](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000D0642&model=guichett), art. 8 ("This Decision shall be implemented without prejudice to the Member States' obligations towards Europol, as they have been laid down in the Europol Convention.").

<sup>42</sup> FATF, Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism: United States of America (June 23, 2006), para. 1190, available at <http://www.fatf-gafi.org/dataoecd/44/9/37101772.pdf>.

<sup>43</sup> See *id.*

<sup>44</sup> *Id.*

<sup>45</sup> See White House News Release – President Announces Crackdown on Terrorist Financial Network; Remarks by the President in Announcement on Financial Aspects of Terrorism, delivered at the Financial Crimes Enforcement Network (FinCEN) (November 7, 2001), available at <http://www.whitehouse.gov/news/releases/2001/11/20011107-4.html> (President George W. Bush: "You're doing some imaginative work here at the Financial Crimes Enforcement Network, and I want to thank all the fine Americans who are on the front line of our war [against terror], the people who work here.").

Furthermore, FATF Recommendation 40, clause b, states “Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.” The EU Data Protection Directive specifically allows Member States to provide exceptions in order to promote criminal investigations.<sup>46</sup>

In addition to the focus on confidentiality outlined above, the Egmont Group is very clear in this regard. For example, the Principles for Information Exchange state, *inter alia*:

7. FIUs should work to encourage that national legal standards and privacy laws are not conceived so as to inhibit the exchange of information, in accordance with these principles, between or among FIUs.
11. Information exchanged between FIUs may be used only for the specific purpose for which the information was sought or provided.
12. The requesting FIU may not transfer information shared by a disclosing FIU to a third party, nor make use of the information in an administrative, investigative, prosecutorial, or judicial purpose without the prior consent of the FIU that disclosed the information.
13. All information exchanged by FIUs must be subjected to strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with national provisions on privacy and data protection. At a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving FIU.

### **The Future – Realizing the Potential of Information Sharing and Strategic Analysis**

A recurring theme throughout this presentation thus far has been a building or growing process, which I like to refer to as a type of capacity building. I should not forget to mention in this context the technical assistance and training efforts conducted by FinCEN not only in conjunction with the Egmont Group, but in close conjunction with others in the Departments of the Treasury and State. Some examples were included in FinCEN’s 2007 Annual Report, including: “Mentored the Nigerian FIU in an 8-month effort during which five FinCEN employees went to Nigeria to provide guidance to the new FIU on regulatory, analytical, and information-technology-related matters.”<sup>47</sup> To me personally, such a significant dedication of FinCEN’s resources reflects both hope for the

---

<sup>46</sup> See Directive 95/46EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281 (23 November 1995) art. 13 (“Member States may adopt legislative measures to restrict the scope of the obligations and right provided . . . when such restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences . . .”). See also, *supra*, Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information. O.J. L 271, 24 October 2000, p. 4–6.

<sup>47</sup> See FinCEN, Annual Report for 2007, at 33, available at <http://www.fincen.gov/AnnualReportFY2007.pdf>.

Nigerian people that the FIU will be among the government entities leading an emergence from a past marred by corruption and mismanagement, and also an expectation that an investment in the FIU of Africa's most populous country will be leveraged through joint cooperation with Nigeria's neighbors. Indeed the Nigerian FIU, which itself only became an Egmont Group member in May 2007, is co-sponsoring the Kenyan, Ghanaian, and Tanzanian FIUs for eventual membership in the Egmont Group. Other examples of recent analytical training that FinCEN has conducted for FIU staff and related officials has been with respect to countries that FinCEN is sponsoring to help become eligible as a functioning FIU for future membership in the Egmont Group, including Afghanistan and Saudi Arabia.<sup>48</sup>

So where are we heading? International financial standards in the AML/CFT have been initiated and matured. The legal frameworks have been determined and are being implemented. Technical assistance in AML/CFT matters is being promoted both by individual countries and international organizations such as the IMF and World Bank. Individual jurisdictions have established the requisite framework, in particular with the development of FIUs, along with the human and IT resources necessary for them to function. An understanding of the importance of AML/CFT efforts is growing, in terms of those responsible for compliance in financial institutions and supervisory authorities, and with respect to the ability of FIU analysts, law enforcement and prosecutorial authorities to understand illicit financial activity and hold criminals accountable. Data is being collected, and over time trends and patterns will emerge under the guise of skilled analysts. The value of financial intelligence to combat money launderers, terrorist financiers and other illicit actors is growing. What does this all mean with respect to the preferred model that I have laid out for cross-border information sharing through FIUs?

***The floodgates of information sharing are about to open.***

There can be no other conclusion. In fact, this is what we have all hoped for and should expect, as the reason that we have been building capacity from an international viewpoint is to provide for transnational sharing in order to combat the increasingly global threats of money laundering, terrorist financing, and other illicit activity. We have established the processes; now we must put them to work.

With respect to tactical analytical requests, it is obvious that as the number of jurisdictions with active FIUs increases, the number of inquiries can only go up. Moreover, as law enforcement and prosecutorial authorities come to better understand the unique avenue for requesting foreign information via FIU channels, they will certainly increase the number of requests they initiate. (I am personally convinced of this and have spent a significant part of my efforts in educating domestic U.S. law enforcement agencies of the investigative tools that FinCEN can offer them, including with respect to processing requests to foreign FIUs.) Moreover, for all parties, increasing familiarity and evidence of success will lead to greater interest to use the tools available to them.

---

<sup>48</sup> See *id.* at 34.

As an international community, we have up to this point failed to adequately take full advantage of the opportunity to make “spontaneous” or “voluntary” disclosures. For example, through analysis of reporting my agency receives from U.S. banks, we may become aware that one or more transactions involved the transfer of significant funds to a third country with no apparent personal or commercial motive for the known parties involved. This might not merit opening a case file in the United States, especially when compared with all of the competing claims on law enforcement resources. But shouldn't we at least consider sharing an appropriate subset of that information with the FIU of that foreign country? If the situation were reversed, wouldn't we want to know if that third country FIU were to become aware of unexplained transactions of funds entering the United States? To my knowledge, such voluntary disclosures continue to represent a very small percentage of the total transnational flow of financial intelligence; however, resources permitting, increasing their volume and quality is in the global community's common interest.

To illustrate proactive, voluntary sharing by FinCEN with foreign FIUs on a broader level which I can discuss publicly, I will describe recent sharing of FinCEN guidance to U.S. financial institutions regarding money laundering threats. The first example is with respect to the Republic of Uzbekistan, which through a series of decrees in recent months has suspended implementation of its AML/CFT law, which had only come into effect in 2006 consistent with international standards. Among other measures, Uzbekistan strengthened bank secrecy and actually prohibited law enforcement from inquiring about cash deposits of any size. On March 20, 2008, FinCEN issued guidance that U.S. financial institutions "should take the risk arising from the deficiencies in Uzbekistan's AML/CFT regime into account for increased due diligence."<sup>49</sup>

FinCEN issued another piece of public guidance that same day, which followed passage of United Nations Security Council Resolution 1803 of March 3, 2008 calling on all States to exercise vigilance over activities of financial institutions in their territories with all banks domiciled in Iran and their branches and subsidiaries abroad.<sup>50</sup> The guidance recalled Security Council Resolutions 1737 and 1747 designating Iranian entities involved in proliferation of weapons of mass destruction and their delivery systems, as well as two expressions of concern by FATF regarding deficiencies in the Iranian AML/CFT regime that represent a significant vulnerability in the international financial system. FinCEN provided further information on the Iranian institutions for which the UN obligation of increased vigilance apply. With respect to each of the foregoing pieces of guidance, I immediately shared them with my Egmont Group counterparts around the world, who similarly would wish to take actions to educate their respective domestic financial institutions of these global risks and obligations to mitigate them."

---

<sup>49</sup> See FinCEN Guidance to Financial Institutions on the Money Laundering Threat Involving the Republic of Uzbekistan at <http://www.fincen.gov/fin-2008-a004.html>

<sup>50</sup> See FinCEN Guidance to Financial Institutions on the Increasing Money Laundering Threat Involving Illicit Iranian at [http://www.fincen.gov/guidance\\_fi\\_increasing\\_mlt\\_iranian.html](http://www.fincen.gov/guidance_fi_increasing_mlt_iranian.html)

Finally, and perhaps most importantly, I wish to turn to the potential for bilateral and multilateral international collaboration in strategic analysis. All of the understood benefits of strategic analysis domestically – e.g., proactive investigation to get a “big picture” of emerging and larger threats or vulnerabilities – can only be multiplied by the prospects of transnational collaboration through the ability to join expertise and information.

In my first year as Director of an FIU, I have often analogized too much of my career as a central banker. In working for a government agency that by definition is one-of-a-kind in any jurisdiction, one must look abroad to learn from the best practices of counterparts. At FinCEN, I have already put this conviction into practice with respect to our regulatory responsibilities, through very fruitful discussions with our counterpart financial intelligence units and AML/CFT regulators. We gained insights, for example, in our ongoing attempts to focus both financial industry and government supervisory authority efforts on risks: in Canada by the Financial Transactions Reports Analysis Centre (FINTRAC) and the Office of the Superintendent of Financial Institutions (OSFI), and by the United Kingdom in the Serious Organised Crime Agency (SOCA) and the Financial Services Authority (FSA). I expect that we will be able to incorporate some of what we have learned into future efforts to make our domestic regulatory framework more efficient and effective.

It is time to similarly engage in strategic analytical work in collaboration with other FIUs, something that FinCEN has not yet accomplished on any project of significant scale. It is a priority to now make that happen.

This past week, I met in person with my counterpart director of the Mexican FIU, and, separately two days later, my counterpart director of the Canadian FIU. In each case we explored the possibility and specific options for joint strategic analytical projects to combine the expertise of our analysts and consider what answers might arise from posing the same queries through the respective data available to us. I believe that this is exactly what the American people would want – to work with our counterparts to gain any clues that might help us together with our neighbors to secure and protect the homeland’s southern and northern borders. If nothing else, wouldn’t it be interesting to know about discrepancies between the financial data reported on the respective sides of the border, and, however limited those data sets might be, whether such discrepancies might yield clues or leads for possible illicit activity? We will never know if we don’t query the available data.

Two days ago when I arrived in Madrid, I visited the Spanish FIU and posed the same types of questions and explored analogous possibilities for joint strategic analytical work. Here, the options might be more complicated, but even more intriguing. Do the historical, economic, linguistic and cultural ties dating back centuries to the glory days of Salamanca where we gather today for this session somehow contribute to vulnerabilities that criminals are able to exploit? Perhaps we need a trilateral effort among the United States, Spain, and some of our key Latin American partner FIUs to find out. I will leave Spain with a strong impression of the FIU's central role in the active use of financial

intelligence to combat organized crime and terrorist financing, as well as not only reaffirmation of the importance of, but also their commitment to join FinCEN in furthering, proactive sharing of information among FIUs and joint strategic analytical work.

I look forward to the next Egmont Group plenary meeting in Seoul, Korea next month together with the leadership of the FIUs of over a hundred other jurisdictions. We will most surely discuss the positive developments with respect to capacity building around the globe, as well as how the financial market outlook has shifted, and some of the new criminal typologies that are emerging. I personally will also advocate for greater information sharing, particularly with respect to voluntary disclosures and possible joint strategic analytical work. It's our responsibility in combating money laundering and terrorist financing.

## **Conclusion**

Criminals and terrorists do not respect laws; we should not expect them to respect borders. Financial markets are global. Financial intelligence can help governments turn vulnerabilities to our advantage in efforts to protect the public from serious crime and terrorist acts. We must use this powerful tool available to us to extend law enforcement's reach beyond jurisdictional limitations through transnational cooperation.

An international consensus has emerged that a key role in such efforts should be played by a designated central agency to serve as each jurisdiction's financial intelligence unit. FIUs can bridge the gap by receiving certain information from financial institutions subject to controls and protections; and applying their expertise to develop financial intelligence that is accessible and applicable to law enforcement investigations. FIUs have been given unique legal authority and have developed the infrastructure necessary to transcend jurisdictional borders to appropriately share financial intelligence. Benefits from such sharing have been well proven in tactical support of actual law enforcement investigations. Now it is time to unleash the potential for proactive information sharing and joint strategic analytical work. In our increasingly globalized world, we must take FIU information sharing to this higher plane to realize its potential to further transnational efforts to combat the global threats of money laundering, terrorist financing, and other illicit activity.

◇ ◇ ◇