CURRENT INTERNATIONAL MONEY LAUNDERING TRENDS AND ANTI-MONEY LAUNDERING CO-OPERATION MEASURES

*Jean B. Weld**

I. INTRODUCTION

"Profit is fundamental to the goals of most crime, and therefore criminals make great efforts to move illegally obtained money and other assets in order to convert, conceal or disguise the true nature and source of these funds."[1] Money launderers and supporters of terrorism have demonstrated great creativity in building upon traditional money laundering techniques to develop further complex money laundering schemes designed to thwart the ability of authorities to prevent, detect and prosecute the laundering. Keeping up with the creativity of criminals flush with cash is a full time job requiring the consistent and combined talents of investigators, prosecutors and judges worldwide. Money laundering continues to be a serious global threat as jurisdictions flooded with illicit funds are vulnerable to the breakdown of the rule of law, the corruption of public officials and destabilization of their economies. Thus, the immense social costs of crime require that the global law enforcement community make every effort to stay abreast of the evolving methods and techniques employed by the criminals.

The development of new technologies and linkages between criminal organizations and gatekeepers – such as accountants, attorneys, and bankers – who are willing to assist in the laundering has also exacerbated the challenges faced by the law enforcement community. This paper will explore current global trends of money laundering, with a short note on terrorist financing, and address certain elements of AML/CFT[2] regimes which are, at least in part, effective in stemming the flow and enjoyment by the criminals of their ill-gotten gains.

II. CURRENT MONEY LAUNDERING THREATS AND TRENDS

As a basic concept, money laundering consists of any act which converts money or other property which is acquired through illegal activity into money or property that appears legitimate, thereby concealing its illegitimate source. The financing of much criminal activity, including terrorist acts, originates with laundered proceeds, generally in the form of cash.

In addition to the obvious profit motive of nearly every crime which generates money, "the availability of working capital is also fundamental for both criminals and terrorists to sustain their networks."[3] The distribution of narcotics, arms, and munitions requires a global network of growers and/or manufacturers, processors, couriers, transporters, marketers, maintenance and storage workers, and other personnel essential to the criminal enterprises. These individuals will nearly always be paid in cash because criminal organizations risk discovery and prosecution if records of these transactions are generated and retained.

Criminal enterprises generate funds in a myriad of different ways. But, the primary stages of money laundering remain the same for all crimes: (1) placement of the criminal proceeds into the financial or other transfer system; (2) layering the funds so as to conceal their original source; and (3) integration into

* Senior Trial Attorney, International Unit, Asset Forfeiture and Money Laundering Section, Criminal Division of the U.S. Department of Justice. The views expressed in this article are those of the author and do not necessarily reflect the views or policies of the U.S. Department of Justice.

[1] *Global Money Laundering & Terrorist Financing Threat Assessment* (July 2010) http://www.fatf-gafi.org/dataoecd/48/10/45724350.pdf at p. 12.

[2] The term AML/CFT is used in this paper, as adopted by the Financial Action Task Force ("FATF"), to refer to anti-money laundering and combating of terrorist financing efforts.

[3] http://www.fatf-gafi.org/dataoecd/48/10/45724350.pdf at p. 12.

the legitimate financial markets, such as banks, credit companies, broker dealers, real estate, and many others. The FATF recently noted that "the ML/TF (money laundering and terrorist financing) methods and techniques that most jurisdictions are currently seeing are broadly the same as the ones that have been observed and described in previous FATF exercises," and include cash couriers and cash smugglers.[4] Newly emerging threats detected included a demonstrably increased use of internet-based payment systems and more complex commercial structures and trusts set up and maintained by gatekeepers.[5]

A. Traditional Money Laundering Typologies

1. Structured Transactions Deposited to Financial Institutions

Most major criminal enterprises generate large amounts of cash. This is particularly true of narcotics trafficking organizations, which constituted one of the first areas which law enforcement sought to combat with money laundering prosecutions and confiscations. However, identity fraud, access device fraud, bank fraud, gambling, and smuggling also result in vast quantities of cash which must be integrated into the economy in order to be used.

The most efficient and effective method of transferring cash is the banking system. Bank transfers allow value to be moved electronically and quickly in a secure environment. Banks are generally the criminal's fast track to his or her recently opened account in Switzerland. Wire transfers are an effective way to pay expenses of the criminal enterprise. However, in an effort to thwart the criminal's easy use of the banking system, jurisdictions have adopted statutory and regulatory requirements requiring financial institutions to report cash transactions above a certain amount. To avoid generating these reports, criminals often structure their transactions. For example, the criminal would open accounts at several banks, and make deposits to separate teller windows or ATM machines in amounts less than $10,000, thereby avoiding the filing of any Currency Transaction Reports ("CTRs") by the financial institution.

As these financial reporting requirements have become more stringently enforced, and with the development of required Suspicious Transaction Reporting ("STR"), criminals have begun to look for other methods to launder their illicit funds. STR reporting (called "SAR" reports in the U.S. for Suspicious Activity Report) is required in the U.S. whenever the bank employee has reason to "suspect" that funds come from illegal activity or are disguised, that is, whenever the bank has information that the transaction is structured to evade reporting requirements, appears to serve no known business or apparent lawful purpose, or is being used to facilitate criminal activity even if it has no knowledge of the underlying criminal conduct, it must file a SAR. Moreover, most large banks now have sophisticated AML compliance software installed which will automatically detect many of these type of transactions, keeping the compliance officers quite busy determining whether and when they are obligated to file SARs.

2. Cash Couriers and Bulk Cash Smugglers

As banks in jurisdictions with stronger AML/CFT ("Anti-money Laundering/Countering the Financing of Terrorism") regimes have become less friendly to the criminal's cash business, he or she turned to other methods of placement, layering and integrating that currency. The most obvious technique involved employees of the criminal organization smuggling cash from the consumer country of the illegal product to the distributor, or from the criminal to the foreign bank secrecy destination where he or she had arranged for the currency to be invested. Cash smuggling can be subdivided into two categories: (1) cash courier, and (2) bulk cash smuggling ("BCS"). BCS involves large volumes of cash, and smuggling methods usually involve land or sea border crossings through concealed cash in vehicles or cargo containers. Cash couriers are natural persons physically transporting cash on their person or accompanying luggage. The preferred method of transport for cash couriers is by commercial airline.[6] For either type of cash smuggling, larger denomination bank notes are used whenever possible to reduce the weight and size of the cargo. For this reason, many couriers and smugglers will first deposit or exchange smaller bills, through structured transactions, which also eliminate the chance of exposing bills with forensic value to trained drug dogs and to ion-scanning machines.

---

[4] *Id* at p. 9.

[5] "Gatekeeper" is a term used by the FATF to characterize those who "protect the gates to the financial system," through which potential users must pass in order to succeed, and include professional experts who provide financial expertise to launderers, such as lawyers, accountants, tax advisers, trust and service company providers, as well as bankers and investment brokers. *Id.* at p. 44.

[6] http://www.fatf-gafi.org/dataoecd/48/10/45724350.pdf at p. 16.

FATF Special Recommendation IX was designed to require jurisdictions to address the issue of cash couriers at their borders. It requires countries to implement either a declaration or disclosure system for detecting the cross-border transportation of currency and bearer negotiable instruments. In addition, border officials must have the authority to seize such currency or bearer instruments if it is suspected to be tied to terrorist financing or money laundering, or falsely declared or disclosed. Finally, jurisdictions must be able to penalize offenders who provide false disclosures or declarations, and to confiscate the seized currency or instruments if demonstrated to be related to TF or ML.[7] The FATF has issued a Best Practices guidance paper[8] to assist jurisdictions in recognizing "red flags" of suspicious border activity and to adopt procedures which will implement SR IX.

3. Money Service Businesses and Informal Value Transfer Systems

Criminals, and in particular terrorists, will often use non-banking financial institutions or money service businesses because, even in jurisdictions which regulate them, many of these entities are little concerned about AML/CFT compliance. Large global franchise MSBs, such as Western Union or MoneyGram, comply with reporting requirements and co-operate well with law enforcement. However, smaller ethnic-based money services businesses, such as may be operated from a grocery store or travel agency, are less aware of their AML/CFT responsibilities, and are more easily used by the criminal to launder his funds. In addition, many MSBs carry on a multitude of different financial activities, such as wire transmission, foreign exchange, check cashing or selling of money orders, travelers' checks and stored value, within the U.S. and other countries.

Many smaller "informal value transfer systems" ("IVTS") function on a "trust" basis among customers. One such IVTS is the "*hawala*" (also known as "*hundi*"). This large network of money brokers operates chiefly in the Middle East, North Africa, the Horn of Africa, and South Asia. This system allows *hawaladars* from all parts of the world to transfer funds to and from their clients by settling debts between themselves. Little in the way of record keeping is involved, and the commissions charged by the *hawaladars* are generally less than clients would pay to transfer funds abroad through a financial institution. *Hawala* can operate legally within the United States so long as the *hawaladar* obtains the necessary license from the state(s) in which it operates and is registered with the Financial Crimes Enforcement Network (FinCEN). A large portion of *hawala* activity is legitimate, for example remittances from family members in the U.S. to family in Pakistan, and international aid agencies in Afghanistan use *hawala* for humanitarian and emergency relief work.[9]

The key to deciphering legitimate from illegitimate MSB operations lies in the implementation by countries of FATF Special Recommendation VI, which requires that such entities be licensed and registered, and closely regulated to determine compliance with AML/CFT standards. The U.S. takes this approach, and attempts to close down, prosecute, and obtain confiscations from unlicensed money transmitting businesses, and to issue guidance and training to improve transparency and compliance in those which have registered.

4. Trade-based Money Laundering

Trade-based money laundering ("TBML") is another alternative remittance system providing a method by which criminal organizations obtain, transfer and store criminal proceeds, disguised as legitimate trade. In TBML, value is moved by falsifying invoices, or over-invoicing and under-invoicing commodities which are imported or exported. Trade is used by criminal organizations in this process to disguise the movement of money through complex and confusing documentation sometimes associated with legitimate trade activity.

TBML is used extensively by Colombian drug cartels to repatriate drug proceeds through a method commonly known as the Black Market Peso Exchange ("BMPE"). In addition, alternative remittance services, unlicensed MSBs, and *hawaladars* all use a form of TBML to settle their debts arising from foreign remittances. These groups will accomplish settlement by purchasing commodities in one country and then transferring them to another country where the commodity is sold and the proceeds remitted to the intended recipient. Red flag indicators of trade-based money laundering include: (1) vendor payments made

[7] http://www.fatf-gafi.org/document/19/0,3343,en_32250379_32236920_43775315_1_1_1_1,00.html
[8] http://www.fatf-gafi.org/dataoecd/50/63/34424128.pdf
[9] Passas, Nikos, "Demystifying Hawala: A Look into its Social Organization and Mechanics." *Journal of Scandinavian Studies in Criminology and Crime Prevention* (2006), Vol. 7, pp. 46-62.

in cash by unrelated third parties; (2) vendor payments made via wire transfers from unrelated third parties; (3) vendor payments via checks, bank drafts, or postal money orders from unrelated third parties; (4) false invoicing and customs documents: such as commodity misclassification or commodity over-valuation or under-valuation; (5) carousel transactions (the repeated importation and exportation of the same high-value commodity); (6) commodities traded do not match the business involved; (7) unusual shipping routes or transshipment points; (8) packaging inconsistent with commodity or shipping method; and (9) double-invoicing.[10]

The U.S. Department of Homeland Security, Immigrations and Customs Enforcement ("ICE") has established several Trade Transparency Units ("TTUs") which are dedicated to the ongoing analysis of trade data provided through partnership with other countries. Five are positioned in Latin America – three in the tri-border area of Brazil, Argentina and Paraguay, one in Mexico, and one in Colombia. There is a growing international effort to establish TTUs throughout the world which, like the Egmont Group of FIUs, can exchange real time data and information, mentor each other, and assist on an informal basis in criminal investigations.

B. Emerging Technologies

1. Prepaid Value Cards

In October 2006, FATF published a typologies report on new payment methods used for legitimate economic transactions which could be exploited by money launderers. Featured were the increasing role of non-banks in offering prepaid value cards, electronic purses, mobile payments, internet payment services and digital precious metals. Certainly, criminal launderers are motivated to use the anonymity that these services afford. Better than the ATM network (which generally uses surveillance video), these methods provide criminals new methods of avoiding face-to-face contact with financial service providers who could identify them to police. Moreover, they provide prompt and easy access from nearly anywhere in the world.[11]

2. Online Payment Systems

"Crime courses through the internet in ever-expanding variety. Hackers brazenly hawk stolen bank and credit-card information [. . .]. Money launderers make illicit cash disappear in a maze of online accounts. Diverse as they are, many of these cybercriminals have something important in common: e-gold, Ltd."[12] E-Gold Ltd. ("E-Gold") was one of the oldest and best known digital currency dealers before it, along with its operating company Gold and Silver Reserve, Inc. ("G&SR"), its digital exchanger OmniPay, the principal director and CEO, and other officers were indicted in the District of Columbia on charges of conspiracy to operate an unlicensed money transmitting business, conspiracy to commit money laundering, and several other violations. After numerous pre-trial motions, E-Gold and G&SR pled guilty to the conspiracy charges, and three senior officers entered guilty pleas. The court ordered E-Gold to pay a $300,000 fine, to obtain licenses as a money transmission business in all relevant states in which it operated, and to forfeit $1.75 million, which was in addition to $14 million forfeited in related civil forfeiture proceedings.

The dangers of online payment systems, whether as digital currency, virtual banking systems, or other methods are difficult to address. The locations of the operators and websites are often unknown or they are located in jurisdictions which will not render assistance to a criminal investigation. It is 'virtually' impossible to trace the physical location of any value because there really is no such location. "Digital currency is popular as a payment and money laundering method in child pornography, financial fraud, and online extortion schemes. Digital currency dealers and exchangers commonly allow anonymous accounts with no limit on account or transaction value. As with other online payment services, digital currency dealers and exchangers often keep personnel, web hosts, and assets offshore and not always in the same country, complicating regulatory jurisdiction."[13] Since the successful conclusion to the U.S. criminal case, E-Gold is a mere shadow of its former self, but its CEO is working with U.S. financial regulators to try and restructure the company to comply with all applicable regulatory standards.

---

[10] http://www.ice.gov/partners/financial/topics.htm.

[11] *Global Money Laundering & Terrorist Financing Threat Assessment* (July 2010) http://www.fatf-gafi.org at pp. 34-35.

[12] Grow, Brian, "Gold Rush: Online payment systems like E-gold Ltd. are becoming the currency of choice for cybercrooks." *Bloomberg Business Week* (Jan. 9, 2006).

[13] Smith, Susan L. and Ericson, Daniel W., "E-Gold, Ltd." *Money Laundering Monitor,* U.S. Department of Justice, Criminal Division, Asset Forfeiture & Money Laundering Section, Vol. 13, No. 3 (2008) at pp. 1-2.

Another online phenomenon which creates the potential for laundering criminal proceeds is "Second Life," operated by a U.S. corporation located in California. Over 18,000,000 users, called "Residents," move about and intermingle with other residents via a cartoon/human-like character called an "Avatar." The Avatars move about in the Metaverse (3D virtual reality world), which includes an island beach resort or shopping mall, just to name a few. Avatars may buy or sell virtual items and/or services, and virtual real estate. Second Life has created its own currency called Linden dollars (named after the game developer, Linden Lab) which can be exchanged for US dollars. Once a value is placed on an object (no matter what that object is, real or virtual) criminals may find a way to abuse it by fraud and/or money laundering because anything of value can be laundered. A player/resident may use any credit or debit card or prepaid card (including those stolen or obtained by fraud or identity theft) to purchase online money which may be redeemed for virtual items or actual money with another player in another country in that country's unit of currency. This creates new opportunities for transferring funds anonymously, in order to evade detection by law enforcement and taxing authorities. As with E-Gold, all that is required to open an account is an unverified name and verified email address. If stolen or fraudulent credit cards are used, "Second Life" absorbs the value into cyberspace, and ends the paper trail. "Second Life" has tried to address these concerns by banning gambling after internet gaming became illegal in the U.S. As a U.S. law enforcement officer has noted, "While Second Life and other virtual MMOGs (massively multiplayer online games) have built a virtual global village complete with entertainment, business commerce and education, they have neglected to incorporate a virtual global police department."[14]

3. Increased Use of Gatekeepers to Establish Sophisticated Trusts

Gatekeepers have become a greater money laundering threat than in previous years. These professional accountants, lawyers, and company service providers engage in both self-laundering and third-party laundering. FATF considers Politically Exposed Persons ("PEPs") as gatekeepers because they have access to funds and systems in their country which they can manipulate to personal advantage, and because they have the power to change financial legislation or rules for their own benefit. These individuals often engage in self-laundering of state funds which they have extracted for themselves.[15]

Trust company service providers are responsible for much of the tangled web of complex trusts registered in offshore jurisdictions such as the Cayman Islands, the British Virgin Islands, the Cook Islands, Guernsey, and Jersey, where deciphering the true beneficial ownership of the trust vehicles is difficult, if not impossible. Many trusts and private investment companies ("PICs") formed in multiple jurisdictions function as successful tax evasion or avoidance vehicles. The trust company functions as the actual owner of the assets, and the trustee controls their investment, thus creating a separation between the criminal and his or her accumulated illicit funds which is difficult for law enforcement to pierce. The professional "gatekeepers" shield their clients' interest in the assets and conceal their own involvement behind their professional confidentiality protections.

III. TOOLS TO COMBAT INTERNATIONAL MONEY LAUNDERING

A. United States' Anti-Money Laundering Laws

1. Basic Money Laundering Statute – 18 U.S.C. § 1956

First enacted in 1986, this statute provides U.S. prosecutors with their most effective weapon against money launderers. It criminalizes any financial transaction involving the actual proceeds of any of over 200 federal, state or foreign "specified unlawful activities" (SUAs) by someone who knows that the funds constitute criminal proceeds and conducts the financial transaction in order to accomplish any one of four objectives: (1) to promote the carrying on of SUA; (2) to evade taxes; (3) to conceal or disguise the nature, source, location, ownership or control of the proceeds; or (4) to avoid any Federal or State transaction reporting requirement. The statute also reaches the international movement of funds or monetary instruments, where the funds have passed out of, into, or through the United States for the purpose of promoting an SUA; concealing or disguising the proceeds of an SUA; or to avoid a Federal or State transaction reporting requirement. In addition, the statute expressly permits prosecution of anyone who

[14] Sullivan, Kevin (New York State Police Investigator), "Virtual Money Laundering and Fraud – Second Life and Other Online Sites Targeted by Criminals." http://www.bankinfosecurity.com/articles.php?art_id=809&search_keyword=virtual+money+laundering&search_method=exact (April 3, 2008).

[15] http://www.fatf-gafi.org/dataoecd/48/10/45724350.pdf at p. 44.

launders funds "*represented to be* the proceeds of specified unlawful activity" which permits undercover money laundering operations by law enforcement.

The key to a Section 1956 prosecution is that the funds must be the proceeds of one of the recognized SUAs. Section 1956(c)(7)(B) covers certain foreign predicate crimes for money laundering; thus, if funds are laundered to or through the U.S. which were generated by any of the listed foreign predicates, a money laundering offence can be charged in the United States. "Financial Transaction" is defined in the statute as a transaction affecting foreign or interstate commerce which involves the movement of funds by wire or other means, any transaction involving monetary instruments, any transaction involving the use of a financial institution, and also any transaction involving the transfer of title to real property, a vehicle, a vessel, or aircraft. Thus, all transactions involving the purchase or sale of conveyances, as well as transactions occurring in cash, are covered by the statute. "Proceeds" is defined as "any property derived . . . through some sort of unlawful activity, including the gross receipts of such activity." This definition was added by Congress in 2009 to address the U.S. Supreme Court's decision in *United States v. Santos*, 553 U.S. 507 (2008), which determined that the term "proceeds," as applied to laundering the proceeds of gambling, meant "net profits."

Section 1956 applies to the myriad of reporting requirements under the U.S. Bank Secrecy Act (31 U. S.C. § 5311, et seq.), including SARs, CTRs, Currency or Monetary Instruments Reports (CMIR), and Foreign Bank account Registrations. It also covers I.R.S. Form 8300, which requires that anyone engaging in a commercial transaction involving more than $10,000 in cash must report the transaction to the Internal Revenue Service.

Because this conference is focused on targeting transnational organized crime and corruption, it should be noted that Section 1956 was used recently to prosecute numerous defendants in a corruption investigation arising out of Haiti's state-owned national telecommunications company, Teleco. On June 1, 2010, Robert Antoine, of Miami and Haiti, formerly the director of international affairs for Teleco, was sentenced to four years imprisonment for conspiracy to launder bribes which he accepted from three U.S. telecommunications companies. To disguise the bribery proceeds, he laundered them through intermediary companies. Several of the U.S. companies involved, and their officers, have been charged with or convicted of violations of the Foreign Corrupt Practices Act ("FCPA") (15 U.S.C. § 78d-2) and money laundering. The FCPA (enacted in the post-Watergate period of 1977) does not provide for forfeiture. However, forfeitures were ordered based upon the money laundering convictions, including a $1,852,209 forfeiture judgment against Antoine.[16]

2. Spending Statute – 18 U.S.C. § 1957

U.S. prosecutors use 18 U.S.C. § 1957 to prosecute "monetary transactions" involving "criminally derived property" of a value in excess of $10,000. We call this the "Spending Statute" because the term "monetary transactions is broadly defined to include any "exchange, in or affecting interstate or foreign commerce" which is by, through or to a financial institution. The definition of a financial institution is not limited to a banking institution but includes a number of other entities such as an automobile dealership, pawn broker, all types of money service businesses, casinos, dealers in real estate, and dealers in precious metals. Because Section 1957 is a "general intent" crime, as opposed to "specific intent" crime such as Section 1956, U.S. prosecutors use it in cases where the evidence may not support an inference that the defendant acted with any of the specific intent requirements of Section 1956, such as to promote the unlawful activity, or to conceal or disguise the source of the funds. As in Section 1956 prosecutions, the property must be the proceeds of a "specified unlawful activity."

Examples of uses of Section 1957 include prosecutions for purchases of property with over $10,000 in cash, or traveller's checks, or transfer of a conveyance for over $10,000. Section 1957 has no "sting"

[16] Section 1956 is also used to prosecute the laundering of funds to suspected terrorist organizations where the terrorist financing charge cannot be proven beyond a reasonable doubt. For example, in 2008 Saifullah Anjum Ranjha, of Washington, D.C., received a sentence of nine years' imprisonment and was ordered to forfeit $2,208,000 in funds which he laundered through his money remitter business - Hamza, Inc. During an undercover "sting" operation in which the defendant was provided with ostensibly drug money, he claimed that he handled money from drug trafficking, cigarette smuggling and weapons trafficking, and that he channelled funds to al Qaeda; however, the al Qaeda connection was not conclusively established. The defendant had bank accounts in Canada, Spain, England, Pakistan, Japan, and Australia using "*hawala*".

provision, so the property involved in the charged transaction must, in fact, be the proceeds of an identified SUA. Section 1957 carries a lesser sentence, 10 years as opposed to the 20 year sentence under Section 1956.

3. Money Laundering Prosecutions Under IEEPA – 50 U.S.C. § 1705

In recent years, the U.S. Department of Justice has vigorously employed the criminal, civil and forfeiture provisions of the International Economic Emergency Powers Act ("IEEPA"), the Trading With the Enemy Act, and the Bank Secrecy Act ("BSA") to prosecute large international financial institutions that have continued to do business with clients in jurisdictions which are listed on the U.S. Office of Foreign Assets Control ("OFAC") list. Some of these cases were investigated by the Federal Bureau of Investigation ("FBI"), some by the IRS, some with assistance from the New York County District Attorney's Office, and a recent case against ABN AMRO with assistance from the U.S. Attorney's Office for the District of Columbia.

IEEPA (50 U.S.C. § 1705) criminalizes any violation of regulations issued under the Act which require the blocking of transactions from sanctioned countries such as Iran, Sudan, Libya, and Burma. The Act also requires banks to maintain adequate programmes to detect and report suspicious activity indicative of money laundering, terrorist financing, and other crimes. Instead of applying the statutorily required AML/CFT protections, these banks actively engaged in conduct to defeat their application, such as: (1) altering references from outgoing transactions that identified sanctioned countries, banks, or persons; and (2) stripping data from certain fields for incoming transactions to conceal the origin as any sanctioned entity. Through the stripping and alterations, the banks ensured that the payments were fully processed undetected through filters at any U.S. financial institutions.

In 2009 and 2010, four international banks were charged and entered into deferred prosecution agreements with the Department of Justice. The agreements provided for stiff fines and forfeitures, and mandated remedial AML/CFT procedures immediately with oversight from the government and the court. In 2009, Lloyds TSB admitted in a DPA that its London, Tokyo, and Dubai offices had been stripping wire transfer information to conceal references to Iran, Sudan, and other sanctioned entities, bypassing AML filters at U.S. banks. Lloyds forfeited $350,000,000 for the violations. Credit Suisse Bank also entered into a DPA in 2009 for similar violations, and forfeited $536,000,000. In 2010, ABN AMRO and Barclays Bank PLC entered into similar DPAs, forfeiting $500,000,000 and $298,000,000 respectively.

4. Money Laundering in Support of Terrorist Financing

Terrorist financing is, in some respects, the reverse of typical money laundering.[17] In most money laundering cases, the perpetrators have "dirty" money which they are seeking to "clean" or "wash" sufficiently to reintegrate it into the global economy so that they can enjoy its use. In terrorist financing, often the sources of the funds are "clean" or legitimate, but the final uses to which the funds are put constitute heinous violent and destabilizing crimes against humanity. Supporters and members of terrorist organizations are not selective in the types of criminal activity from which they will accept proceeds. The proceeds of drug trafficking, extortion, fraud, currency counterfeiting, cigarette smuggling, and human trafficking conducted in and laundered to all parts of the world have found their way into the coffers of terrorist organizations. Sympathizers and supporters also contribute clean money to terrorist financing.

The tools for combating terrorist financing are essentially the same as those used to combat money laundering. Co-operation between law enforcement and intelligence agencies, including the FIUs, aggressively prosecuting cases when appropriate, penalizing financial institutions which attempt to bypass the UN sanctions lists, bilateral and multilateral diplomacy, and capacity building in jurisdictions which are most vulnerable to this activity. Terrorist organizations have transitioned to smaller, decentralized groups (cells) which do not require large expenditures of funding to prepare and carry out their missions.

[17] The UN Convention Against Terrorist Financing (1999) (Terrorist Financing Convention) defines terrorist financing as "the providing or collecting of funds by any means, directly or indirectly, . . . with the intention that they should be used or in the knowledge that they are to be used, . . . (a) to carry out an act which constitutes the offense of terrorism; (b) to carry out any other act intended to cause death or serious bodily injury to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, . . . is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act; or (3) by any terrorist or terrorist organization (for any purpose)."

The perpetrators of the London 7/7 (7 July 2005) bombings of three underground trains and a bus killing 52 people were self-funded through street-level drug dealing. The 9/11 terrorist acts only required a few hundred thousand dollars. Such low level cash financing is nearly impossible to detect as it is normally outside the regulated financial system, often involves stolen or fictitious identities, and does not generally arouse suspicion in any entity that would generate a suspicious activity report.

U.S. laws against terrorist financing are comprehensive, and they criminalize: (1) providing, or concealing or disguising the nature, location, source or ownership of "material support or resources,"[18] knowing that they may be used to carry out a terrorist act, 18 U.S.C.

§ 2339A (enacted in 1994); (2) the provision or attempted provision of "material support" (as defined in Section 2339A) to a foreign terrorist organization,[19] 18 U.S.C. § 2339B (enacted in 1996); and (3) providing or collecting, directly or indirectly, "funds"[20] knowing or intending that they be used to carry out any act listed in the various conventions, protocols and treaties covered by the Terrorist Financing Convention, or any act intended to cause death or serious bodily injury to a civilian, or any person not taking an active part in the hostilities of a situation of armed conflict to intimidate a populations, to compel a government or international organization to do or abstain from doing any act, 18 U.S.C. § 2339C (enacted in 2002).

Traditionally, the most common terrorist financing prosecution in the United States was a "clean money" prosecution, in which funds were raised for organizations constituting "fronts" for FTOs. "Clean money" prosecutions generally involve groups which raise money ostensibly for charitable overseas work, but actually channel the funds to FTOs. In these cases, the prosecution must show that contributors had reason to know that the so-called "charity" was a front for an FTO.[21]

In "dirty money" prosecutions, U.S. prosecutors target FTO agents who engage in criminal behaviour to support their presence in the United States and generate funds which are sent back to family members and trusted friends to jurisdictions which are weak on AML/CFT compliance, and are often state sponsors of terrorist organizations. Often because of lack of available legal assistance from these jurisdictions, U.S. prosecutors cannot establish the precise use of the funds in the foreign country; however, the criminal nature of their origin, and the lack of any apparent legitimate endeavour may give rise to sufficient inference of terrorist activity.[22]

---

[18] "Material support or resources" is defined as "any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel [. . .], and transportation, except medicine or religious materials." 18 U.S.C.U.S.C. § § 2339A(b)(1).

[19] "Terrorist organization" is defined as an entity designated as a Foreign Terrorist Organization ("FTO") by the Secretary of State. An FTO must threaten the security of U.S. nationals *or* the security (national defence, foreign relations, or economic interests) of the United States. There are currently 46 entities so listed. 18 U.S.C.U.S.C. § § 2339B(g)(6).

[20] "Funds" is defined as assets of every kind, tangible or intangible, movable or immovable, legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including coin, currency, bank credits, travellers checks, bank checks, money orders, shares, securities, bonds, drafts, and letters of credit. 18 U.S.C.U.S.C. § § 2339C(e)(1).

[21] Examples of "clean money" cases include: *United States v. Enaam Arnaout,* 431 F.3d 994 (7th Cir. 2005) (defendant, CEO of the Benevolence International Foundation ("BIF") was convicted of RICO charges for duping donors who sent $400,000 which actually went to Chechnyan rebels and the Bosnia military); *United States v. Oussama Kassir*, 2009 WL 2913651 (SDNY 2009) (defendant convicted of violating 18 U.S.C.U.S.C. §§ 2339A and 2339B for providing training and other resources to young men for *jihad* in the Pacific Northwest at both a Seattle mosque and a camp site in Bly, Oregon); *United States v. Rafil Dhafer, Help the Needy Endowment, et al.*, 577 F.3d 411 (2d Cir. 2009) (Dhafer, an Iraqi-born New York oncologist, was convicted of IEEPA violations, promotional ML, fraudulent Medicare billings, and tax fraud as a result of using contributions received by his unregistered charitable organization - Help the Needy - to violate the Iraqi Sanctions Regulations; he was sentenced to 22 years' imprisonment).

[22] Examples of "dirty money" cases include: *U.S. v. Mohamed Hammoud, et als,* 381 F.3d 316 (4th Cir. 2004) (pre-9/11 prosecution against Lebanese men discovered by a local sheriff conducting a massive interstate cigarette smuggling enterprise in Charlotte, North Carolina – Hammoud and associates had ties to Hezbollah before coming to the U.S. on false visas in 1992; Hammoud was convicted of providing "material support" under 18 U.S.C. § 2339B, RICO conspiracy, money laundering, cigarette smuggling, immigration violations, and was sentenced to 155 years imprisonment); *U.S. v. Syed Mustajab Shah, et al*, 02CR 2912 (S.D.Cal. 2002) (charged with conspiracy to distribute 600 kilos of heroin and five metric tons of hashish, and with

IV. CO-OPERATION IN AML INVESTIGATIONS, CO-OPERATION BETWEEN FIUs, AND "OPERATION MANTIS"

Co-operation in anti-money laundering investigations must begin domestically, even in transnational crime and corruption cases. Law enforcement, intelligence, and prosecution agencies should collaborate and co-operate on the home front before an outreach to international partners for assistance. Some of the cases mentioned in this paper involved several levels of international assistance, such as police-to-police and prosecutor-to-prosecutor. For example, the Haitian Teleco corruption case required dedicated co-operation between ICE-Miami and Haiti's FIU, the Unité Centrale de Renseignements Financiers ("UCREP"), also the Bureau des Affaires Financières et Economiques (a division of the Haitian National Police), and the Ministry of Justice and Public Security. FIUs are an essential component of any team to combat money laundering. Egmont membership brings access to the Egmont Secure Web, which opens up the possibility of obtaining financial intelligence from 121 member countries.

A. United States' Suspicious Activity Report (SAR) Review Teams

A model of law enforcement co-operation for transnational crime and money laundering cases in the United States has become the SAR Review Team. Each federal district has been requested to establish such a team comprising a designated Assistant U.S. Attorney, agents from all federal law enforcement agencies within the district, and state and local investigators who have jurisdiction over money laundering or other crimes (such as gambling and narcotics) which often give rise to money laundering. The objective is to meet on a regular basis, but no less than once a month, and analyse certain pre-selected Suspicious Activity Reports (SARs). The SAR information is sent to the SAR team leader once a month by FinCEN, and the team leader may divide up the review of the SARs to various members of the team. The team's mission is to evaluate and prioritize the SARs for investigative purposes. Like many FIUs, FinCEN became overwhelmed with the sheer number of SARs being filed, and this proactive approach was necessary in order to maximize the intelligent use of these mandatory reports.

Prior to each team meeting, all members will have cross-referenced the current list of SARs against any databases maintained by that agency. The team should prioritize the illegal activities it most wishes to have investigated. Developing criminal cases beyond the SARs themselves is difficult because it can be nearly impossible at first to identify an SUA underlying a reported financial transaction. Investigating every SAR consumes significant investigatory time in an inefficient manner, resulting in few cases. Based on the experience of the U.S. teams, prioritizing the crimes of structuring transactions and unlicensed money transmitting businesses have proven to be the best use of the team. Some of these cases have spun into larger, more complex and serious investigations, and have led to deportations and possible disruption of some terrorist financing operations. The teams generally focus on transactions occurring within the last twelve months. Numerous cases of substantial merit have evolved from SAR Review Teams, involving structured transactions, tax evasion, check kiting on real estate investment accounts, drug trafficking, mortgage fraud, pyramid real estate schemes, fraudulently obtained health care and insurance fraud payments, and laundering of gambling proceeds.

B. "Operation Mantis" – G8 Roma/Lyon Initiative for Bulk Cash Smuggling

The G8 Roma/Lyon Group was formed in 1997 by the Group of Seven Industrialized Countries ("G7") – which included Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. Russia was invited later and the group became the "G8." The Roma/Lyon Group is an Anti-Crime and Counter-terrorism experts group. It has evolved into several working groups that meet three times a year to discuss, debate, and develop strategies to address public security issues surrounding terrorism and transnational crime. The Group primarily concentrates on combating criminal organizations' use of the global transport system to further illegal activity.

---

negotiating to purchase four Stinger anti-aircraft missiles to sell to al Qaeda in Afghanistan; defendants were arrested in, and extradited from, Hong Kong); *U.S. v. Uwe Jenson, Carlos Ali Romero Varela, et al* H-02-1008M (S.D.Tex. 2002) (high ranking members of the AUC (Armadas Unidades de Colombia) charged with drug conspiracy and conspiracy to provide material support to the AUC, a designated FTO; Costa Rican officials arrested defendants following an undercover weapons-for-drugs "sting" contemplating $25 Million in weapons to be provided to the AUC in exchange for cash and cocaine).

During a three day period in 2009, the Roma/Lyon Group conducted a multinational enforcement action known as "Operation Mantis." This was a multilateral initiative conducted by officials from seven of the eight members to specifically address bulk cash smuggling. Focusing on commercial airline travellers, the objectives were interdiction, investigation, and intelligence-gathering and sharing in order to identify, disrupt and dismantle trans-border criminal networks using cash couriers to smuggle illicit cash. Because similar operations are likely to be repeated in the future, at least on a regional basis, the specific dates were not announced. Over 500 flights were examined, tens of thousands of passengers were interviewed, and tens of thousands of bags were inspected. The operation netted over $3.5 million from 81 cash seizures and discovered another $4.2 million in undeclared currency at various ports of entry. Cash couriers are a transport of choice for many criminal syndicates and terrorist cells, and commercial airlines are a preferred means of transport because foreign destinations can be reached quickly with little or no pre-planning.

Operation Mantis resulted from two years of planning within the G8 with the stated objective of supporting FATF Special Recommendation IX, which addresses issues of cash couriers and border security. Participating officials collected and shared real time information and intelligence, which should prove helpful in future targeting and interdiction of cash couriers. Airports throughout the world have employed different methods to detect cash carried in baggage, on travellers, or in shipments, such as currency detection dogs, X-ray and gamma ray equipment, body searches, and ion mobility scanners. At least one arrest was publicly acknowledged as a result of Operation Mantis, that of a 17-year old female flying from London to Vietnam. She was arrested carrying £380,000 (US $550,000) in her checked luggage. Subsequent searches at her UK residence revealed additional £12,000 (US $17,000).

C. United States' Laws on Cash Couriers and Bulk Cash Smuggling

Title 31 of the United States Code, Section 5316 and its implementing regulation, 31 C.F.R. § 103.23, enacted in 1982, imposes an obligation on all persons to file a Currency Monetary Instrument Report (CMIR) with the U.S. Customs Service[23] upon transporting, mailing, or shipping into or out of the United States domestic or foreign currency, or monetary instruments (such as traveller's checks, money orders, bearer instruments) in an amount exceeding $10,000 at one time. This was the traditional provision used by Customs officials to arrest or seize undeclared currency at the U.S. border. Civil and criminal forfeiture is available for "all property, real or personal, involved in" the CMIR violation and all property traceable to that property. This is the language prominently displayed on U.S. Customs signs at airports and other ports of entry.

In 2001, as part of the USA PATRIOT Act, Congress enacted the Bulk Cash Smuggling ("BCS") Statute, 31 U.S.C. § 5332. A violation of the BCS law requires proof of: (1) an intent to evade the reporting requirement; (2) knowing concealment of over $10,000 in monetary instruments on one's person, in a container such as luggage, or in a conveyance; and (3) the transportation or transfer of the currency or monetary instruments to or from the United States. This statute is now used to prosecute couriers transporting large amounts of cash at or near any of the U.S. borders, and it used to criminally and civilly forfeit the seized currency.[24]

V. CONCLUSION

The volume and variety of global money laundering challenges faced by investigators and prosecutors seems infinite. As FATF and other international bodies have succeeded in raising awareness and competency throughout the world to combat money laundering and terrorist financing, the criminals seem to always stay one step ahead. They will continue to exploit new technologies, weak AML/CFT jurisdictions, financial secrecy jurisdictions (from which it remains difficult to obtain mutual legal assistance), greedy and gullible victims, and underground value transfer systems.

---

[23] After 9/11, the Customs Service was transformed into the Customs and Border Patrol (CBP) and Immigration and Customs Enforcement (ICE). CMIRs are filed with CBP.

[24] In the case of *United States v. Jose*, $114,948 in U.S. currency was seized from the defendant's luggage on a flight departing Puerto Rico to St. Maarten, Netherlands Antilles. The cash was in tissue paper-wrapped bundles, hidden in a pair of sneakers and other bundles were wrapped in carbon paper and hidden inside a set of bed sheets. Customs officials advised Jose about the currency reporting requirements for transported amounts in excess of $10,000; he reported that he had $1,400 in cash with him. The final forfeiture judgment was for the full amount seized less the $1,400 which he declared.

Co-operation among nations, and among domestic law enforcement officials within each nation, is, therefore, imperative to stem the immense and rising tide of laundered organized crime and corruption proceeds. International organizations such as the UNODC, the FATF, the Asian Pacific Group, Moneyval, the IMF, and the OAS must continue to press for member compliance with international AML/CFT standards and take a strong stance against continued noncompliance resulting from lack of political will. The powerful tool of asset forfeiture should be used, also, to help fund the fight against transnational crime. As an old police friend of mine, who was also a hunter, used to say, "Sometimes you get the bear, sometimes the bear gets you." We will never fully eradicate transnational crime, but without the continued effort, personal accountability and the rule of law will be seriously undermined. We must not give up the fight.