2012

Terrorism Financing Indicators for Financial Institutions in the United States

Richard K. Gordon
Case Western Reserve University School of Law, richard.gordon@case.edu

TERRORISM FINANCING INDICATORS FOR FINANCIAL INSTITUTIONS IN THE UNITED STATES

Richard Gordon[*]

At least since the Financial Action Task Force (FATF) first published its Forty Recommendations, financial institutions in FATF-compliant jurisdictions have been required to implement preventive measures that require FIs to identify customers, establish client profiles, monitor for unusual transactions, review those transactions to see if there was suspicion that they involved the proceeds of crime and, if so, report the transaction to the authorities in the form of a suspicious transaction report (STR). When these requirements were first established, neither financial institutions nor their supervisors/regulators had much experience as to what in a client's profile and the client's patterns of transactions might indicate money laundering. However, based on an expanding knowledge of how criminals tend to launder their money, over time financial institutions have developed increasingly effective detection and reporting systems. By studying known examples of laundering, the FATF, FATF-Style Regional Bodies, and national competent authorities (especially financial intelligence units) have identified patterns or indicators of possible money laundering, and made them available to financial institutions as money laundering typologies. In addition, there has been some feedback from financial intelligence units and other competent authorities to financial institutions with respect to their anti-money laundering programs. Using these sources, financial institutions have been able to develop systems to help them

---

[*] Professor of Law, Case Western Reserve University School of Law; Adjunct Associate Professor of International Studies, Brown University. B.A. Yale (1978). J.D. Harvard Law School (1984). This preliminary report is to be used in the completion of a consolidated report by Professor Nikos Passas of Northeastern University, the Honorable Susan Eckert of Brown University, and Professor Gordon. The consolidated report will include cases from jurisdictions other than the U.S. as well as additional analytical discussion and bibliographical material to be provided by Professor Passas and Ms. Eckert. Professor Passas and Ms. Eckert were equal participants in the scope and planning of the preliminary report on the U.S. and provided significant guidance and editorial assistance in its drafting. Student assistants included Mark Skerry, Jonathan Calka, Daniel Straka, Pratibha Gupta, Jiajia Xu, Al Patel, Dan Tsai, Sam Mimoto, and Sean Stevens. Special thanks are given to Jeffrey Breinhold of the U.S. Justice Department for compiling the list of terrorism-related prosecutions used in the preliminary report and to the numerous Assistant U.S. Attorneys who provided materials relevant to the cases examined. Craig Boise, Willie Maddox, and Emile van de Does de Willebois provided helpful commentary. This study was financed in part by the Financial Market Integrity Group of the World Bank.

determine which transactions carry a materially greater risk that laundering is involved.

Following the terrorist attacks of September 11, 2001, the FATF adopted the VIII Special Recommendations on terrorist financing. Among these new requirements were that financial institutions also report to authorities if they suspected that a transaction involved the financing of terrorism. However, there was little in the way of known patterns of terrorism financing that financial institutions could use to help identify such transactions. While since that time a number of limited typology studies have been made available by the FATF, no comprehensive study of terrorism financing typologies has yet been published. For this reason, the Counter-terrorism Implementation Task Force requested a comprehensive study on past terrorism financing techniques that would add to value to efforts by both financial institutions and governmental authorities in identifying terrorism financing transactions or patterns, also known as typologies.

This preliminary report on prosecutions in the U.S examined 266 instances of prosecutions that involve charges of terrorism, material support of terrorism, or other terrorism-related matters. Of that number, thirty were determined to involve financial institutions. Using only publicly available information, the study found twenty-four where there was sufficient information on financial transactions to see if there were any discernible patterns or typologies for terrorism financing. The study revealed that sixteen of those indicated known typologies of money laundering, although an additional three appear to involve diversion of charitable donations. In only one was there a typology that suggested possible terrorism financing and not laundering. Of the sixteen cases involving suspicious transactions only three appeared to involve criminal proceeds. From these cases, it appears that terrorists often use money laundering techniques to disguise the origins of funds or to prevent competent authorities from tracing payments from end-users to originators, even when the origin is not criminal proceeds. However, because it was not possible to review any STRs (referred to in the U.S. as Suspicious Activity Reports or SARs) that may have been filed by financial institutions with respect to these transactions, it was not possible to determine if financial institutions, in conducting their review of those transactions, had determined that they were suspicious with respect to money laundering or terrorism financing. It was also impossible to know if FinCEN had referred such SARs to law enforcement for further investigation, or if they had added actionable intelligence to the SARs that would suggest either money laundering or terrorism financing. Such reviews would be most helpful in completing the study.

I. THE GLOBAL STANDARD AGAINST MONEY LAUNDERING AND TERRORISM FINANCING[1]

A. Overview

Over the past forty years, anti-money laundering rules have been expanded and refined.[2] The vast majority of the world's jurisdictions now

---

[1] Some of the introductory material for this Report is adopted from Richard K. Gordon, *Trysts or Terrorists? Financial Institutions and the Search for Bad Guys*, 43 WAKE FOREST L. REV. 699 (2008) [hereinafter Gordon, *Trysts or Terrorists?*] and Richard K. Gordon, *Losing the War Against Dirty Money: Rethinking Global Standards on Preventing Money Laundering and Terrorism Financing*, 21 DUKE J. COMP. & INT'L L. 503 (2011).

[2] The first anti-money laundering law enacted in the U.S. was The Currency and Foreign Transactions Reporting Act of 1970. Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. §§ 1829b, 1951–59 (2000), 31 U.S.C. §§ 5311–5314(e), 5316–5530, 5332(2) (2000), and 18 U.S.C. §§1956-1957, 1960 (2009)) [hereinafter Bank Secrecy Act]. Anti-money laundering laws were expanded in 1986, 1988, 1992, 1994, 1998, 2001, and 2004. *History of Anti-Money Laundering Laws*, FINCEN, http://www.fincen.gov/news_room/aml_history.html (last visited May 20, 2012) (FinCEN is the U.S. financial intelligence unit); *see also* Mariano-Florentino Cuéllar, *Criminal Law: The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance*, 93 J. CRIM. L. &

endorse the latest version of the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering (FATF 40 Recommendations)[3] and accompanying Methodology for Assessment.[4]

CRIMINOLOGY 311, 338–69 (2003) (exploring the federal laws and regulations available to prosecute money laundering). The EU's efforts began in 1991 with its first anti-money laundering Directive. Council Directive 91/308/EEC, 1991 O.J. (L 166) 77 (EC). They were expanded significantly with the second and third anti-money laundering Directives in 2001 and 2004. Council Directive 2001/97/EEC, 2001 O.J. (L 344) 76 (EC); Council Directive 2005/60/EEC, 2005 O.J. (L 309) 15 (EC); *see also* Alan E. Sorcher, *Lost in Implementation: Financial Institutions Face Challenges Complying with Anti-Money Laundering Laws*, 18 TRANSNAT'L L. 395, 408–10, 414 (2005) (discussing the development of anti-money laundering law in the EU). The first multilateral convention including anti-money laundering provisions came into force in 1988. U.N. Convention Against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 20, 1988, 1582 U.N.T.S. 95 [hereinafter Vienna Convention]. This was followed by conventions expanding anti-money laundering provisions. *See, e.g.*, The Council of Europe, Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, Nov. 8, 1990, E.T.S. No. 141 (entered into force Nov. 1, 1993) [hereinafter Strasbourg Convention]; U.N. Convention Against Transnational Organized Crime, Sept. 29, 2003, 2225 U.N.T.S. 209. The Financial Action Task Force published its first set of 40 Recommendations on money laundering in 1990. These original Recommendations were revised and expanded in 1996. FIN. ACTION TASK FORCE [FATF], FORTY RECOMMENDATIONS ON MONEY LAUNDERING 2 (June 28, 1996); *see also* FATF, FORTY RECOMMENDATIONS (2003) [hereinafter FATF 40 RECOMMENDATIONS]. Following the attacks of September 11, 2001, the FATF added 8 Special Recommendations against Terrorism Finance; a 9th Recommendation was added in 2004. *History of the FATF*, FATF, http://www.fatf-gafi.org/pages/aboutus/historyofthefatf/ (last visited May 21, 2012). Since the FATF's first set of 40 Recommendations on Money Laundering, the definition of financial institution has been extended, (and certain requirements have been extended to include some persons who are not financial institutions). In addition, rules on record-keeping have been tightened, but the general framework of client identification, recordkeeping, client monitoring, and reporting of suspicious activities has not changed. *Compare* FATF 40 RECOMMENDATIONS, *supra*, at 16 (defining financial institution as any person or entity engaged in specific transactions, such as accepting deposits, lending, transfers, and others), *with id.* at 7 (obligating other institutions, such as casinos, real estate agents, dealers in precious metals, lawyers, and trust and company service providers, to adhere to the same standards).

[3] FATF 40 RECOMMENDATIONS, *supra* note 2, at 2 (noting that 130 countries have endorsed the 40 Recommendations). In 2002, the International Monetary Fund (IMF) endorsed the FATF 40 Recommendations (and the FATF VIII Special Recommendations on Terrorist Financing (2001)), which were amended in 2004 to include Special Recommendation IX. IMF Advances Efforts to Combat Money Laundering and Terrorist Finance, IMF (Pub. Info. Notice No. 02/87, Aug. 8, 2002) [hereinafter IMF Pub. Notice], *available at* http://www.imf.org/external/np/sec/pn/2002/pn0287.htm; *see also* IMF, REPORT ON THE OUTCOME OF THE FATF PLENARY MEETING AND PROPOSAL FOR THE ENDORSEMENT OF THE METHODOLOGY FOR ASSESSING COMPLIANCE WITH THE ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) STANDARD (2002) [hereinafter FATF PLENARY MEETING], *available at* http://www.imf.org/external/np/mae/aml/2002/eng/110 802.pdf (proposing endorsement of the FATF Recommendations to the IMF Executive Board). Because nearly every country in the world is a member of the IMF, this endorsement has significant resonance. *IMF Members' Quotas and Voting Power, and IMF Board of Governors*, IMF,

Starting in 1990, these global standards have required financial institutions[5] to monitor the transactions of their customers, to examine unusual transactions to determine if they might involve the proceeds of crime[6] and since 2001—the financing of terrorism,[7] and to report any suspicious transactions to special government authorities known as financial intelligence units (FIUs). The FIUs then analyze the reports (known as suspicious transaction reports (STRs)), along with other relevant data, and make recommendations to law enforcement as to which clients or transactions should be investigated.[8]

The terrorist attacks of September 11, 2001 resulted in governments greatly intensifying their anti-money laundering activities and prompted an intensified global effort against terrorism financing.[9] In 2002, the International Monetary Fund and the World Bank adopted the FATF 40 Recommendations and the eight new Special Recommendations on Terrorism Financing (Special Recommendations) as a world standard.[10] They, along with the FATF and various regional anti-money laundering groups known as FATF-Style Regional Bodies (FSRBs), also began a joint global compliance program by assessing the extent to which individual

---

http://www.imf.org/external/np/sec/memdir/members.htm (last visited May 21, 2012). More importantly, each member of the FATF and each of the eight FATF associate members and FATF-style regional bodies has endorsed the FATF 40 Recommendations and Special Recommendations on Terrorist Financing the as the global standard for anti- money laundering and combating the financing of terrorism. *See Financial Action Task Force, Members and Observers*, IMF, http://www.fatf-gafi.org/pages/aboutus/membersandobservers/ (last visited May 21, 2012) (listing all members of FATF); *see also* PAUL ALLAN SCHOTT, REFERENCE GUIDE TO ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM, at III-7–III-13 (2d ed. 2006), *available at* http://zunia.org/uploads/media/knowledge/Reference_Guide_AMLCFT_2ndSupplement1.pdf (summarizing FATF's mission and FATF member obligations).

[4] *See* FATF, METHODOLOGY FOR ASSESSING COMPLIANCE WITH THE FATF 40 RECOMMENDATIONS AND FATF 9 SPECIAL RECOMMENDATIONS 73 (2009) [hereinafter METHODOLOGY] (listing the endorsing bodies, including the IMF, World Bank, and a number of regional financial interest groups).

[5] *See generally* FATF PLENARY MEETING, *supra* note 3 (detailing the development of the standards over time).

[6] *See* FATF 40 RECOMMENDATIONS, *supra* note 2, at 7–8 (Recommendations 11–15 directing financial institutions to be aware of certain types of suspicious transactions).

[7] *See generally* FATF, SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (2001) [hereinafter SPECIAL RECOMMENDATIONS] (proposing recommendations focused on terrorism for addition to the original recommendations).

[8] SCHOTT, *supra* note 3, at VII-3–5.

[9] Richard K. Gordon, *On the Use and Abuse of Standards for Law: Global Governance and Offshore Centers*, 88 N.C.L. REV. 501, 564 (2010).

[10] IMF Pub. Notice, *supra* note 3.

countries were implementing those standards.[11] Failure to implement the standards adequately can result in a broad application of sanctions or countermeasures, including bans on doing business with financial institutions located within the borders of non-complying jurisdictions.[12] As a result, millions of STRs have been forwarded to FIUs by financial institutions throughout the world, although how many have resulted in further investigation, prosecution, and conviction is not publically available.[13]

The FATF's 40 Recommendations and the Special Recommendations are designed to "provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing."[14] Together they cover, among other things, the criminalization of money laundering and terrorism financing, the freezing and seizing of criminal proceeds and terrorism funds, key preventive measures against laundering and terrorism financing for financial institutions and other institutions subject to preventive measures, FIUs, and

---

[11] METHODOLOGY, *supra* note 4, at 2–3 (stating that a uniform system of assessment, including a single assessment methodology, was agreed to by the IMF, the World Bank and the FATF in 2002). IMF assessment reports can be found at *Detailed Assessment Reports*, IMF, http://www.imf.org/external/ns/cs.aspx?id=175 (last updated May 24, 2012). World Bank assessments can be found at *Financial Market Integrity – Assessments*, WORLD BANK, http://go.worldbank.org/Y902MD2ZL0 (last visited May 24, 2012). These bodies and each of the eight FATF associate members and FATF-style regional bodies (many of which are undertaken with the participation of the IMF and World Bank) use the uniform assessment system. FATF assessments can be found at *Mutual Evaluations*, FATF, http://www.fatf-gafi.org/topics/mutualevaluations/ (last visited May 24, 2012) and those of regional bodies can be found at *Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) – Assessments*, IMF, http://www.imf.org/external/np/leg/amlcft/eng/aml2.htm#reports (last visited May 24, 2012).

[12] *See* FATF 40 RECOMMENDATIONS, *supra* note 2, at 9 (in particular, Recommendation 21 stating: "[f]inancial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendation . . . Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures."). For example, under Title III, Sec. 311(a) of the USA Patriot Act, if a financial institution is operating with a jurisdiction outside of the U.S. and there is concern about that jurisdiction's money laundering efforts, the Secretary of the Treasury "may prohibit, or impose conditions upon, the opening or maintaining in the U.S. of a correspondent account or payable- through account by any domestic financial institution or domestic financial agency for or on behalf of a foreign banking institution." USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272, 301 (codified as amended at 31 U.S.C. § 5318A(b)(5) (2004)).

[13] E-mail from Boudewijn Verhelst, President, Egmont Group of Financial Intelligence Units, to author (Feb. 27, 2010) (on file with author) [hereinafter Verhelst e-mail].

[14] FATF 40 RECOMMENDATIONS, *supra* note 2 at 2.

international cooperation.[15] The 40 Recommendations have included similar preventive measure requirements since the original 1990 draft.[16] In effect, these Recommendations divide the responsibility for preventing and uncovering money laundering between the private and public sector.

---

[15] The FATF 40 Recommendations are broken down into 4 groups. First is Group A, titled "Legal Systems," which includes the "scope of the criminal offence of money laundering" and "provisional measures and confiscation." *Id.* at 3–4. Second is Group B, titled "Measures to be Taken by Financial Institutions and [certain] Non-Financial Businesses and Professions to Prevent Money Laundering and Terrorist Financing," which includes prohibition on shell banks, customer due diligence and record-keeping (including client identification and transaction monitoring), reporting of suspicious transactions and compliance (including internal training and audit programs), other measures to deter money laundering and terrorist financing (including sanctions for failure to comply with the Recommendations), measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, and regulation and supervision. *Id.* at 4–10. Third is Group C, titled "Institutional and Other Measures Necessary in Systems for Combating Money Laundering and Terrorism Financing," which includes competent authorities and their powers and resources (including the establishment of a financial intelligence unit) and transparency of legal persons and arrangements. *Id.* at 10–12. Fourth is Group D, titled "International Co-operation," which includes international commitment to implement various treaties, mutual legal assistance and extradition, and other forms of co-operation. *Id.* at 12–14. The IX Special Recommendations include: (1) ratification and implementation of UN instruments; (2) criminalizing the financing of terrorism and associated money laundering; (3) freezing and confiscating terrorist assets; (4) reporting suspicious transactions related to terrorism (also required in Recommendation 13); (5) international co-operation, (6) alternative remittance systems; (7) wire transfers; (8) non-profit organizations; and (9) cash couriers. *See generally* FATF, IX SPECIAL RECOMMENDATIONS (2010) [hereinafter IX SPECIAL RECOMMENDATIONS].

[16] Since 1990, there has been a progressive expansion of those persons who must follow the "preventive measures" provisions in the FATF 40 Recommendations. *See* FATF, FORTY RECOMMENDATIONS (1990), *available at* http://www.accessbankplc.com/Library/Documents/Download%20Centre/FATF.pdf; *see also* FATF, 40 RECOMMENDATIONS 1295 (1996), *available at* http://www.fincen.gov/news_room/rp/files/fatf_40_recommendations.pdf. The current definition of financial institutions includes any person who engages in acceptance of deposits and other repayable funds from the public; lending; financial leasing; the transfer of money or value; issuing and managing means of payment (e.g. credit and debit cards, checks, traveler's checks, money orders and bankers' drafts, electronic money); financial guarantees and commitments; trading in: money market instruments (checks, bills, CDs, derivatives etc.), foreign exchange, exchange, interest rate and index instruments, transferable securities, commodity futures trading; participation in securities issues and the provision of financial services related to such issues; individual and collective portfolio management; safekeeping and administration of cash or liquid securities on behalf of other persons; otherwise investing, administering or managing funds or money on behalf of other persons; underwriting and placement of life insurance and other investment related insurance; and money and currency changing. METHODOLOGY, *supra* note 4, at 65–66. Since 2003, most of the preventive measures prescribed for financial institutions have been extended to certain designated non-financial businesses and persons including: casinos (which also includes internet casinos); real estate agents; dealers in precious metals; dealers in precious stones; lawyers; notaries; other independent legal professionals and accountants; and trust and company service providers. *Id.* at 64.

B. Financial Sector Role

1. Overview

FATF Recommendations 5 through 13, plus 21 and 22 (and the relevant materials in the accompanying Methodology for assessment of compliance) set out the part of the preventive measures system that applies financial institutions. Unfortunately these Recommendations are not a model of clarity and are not easy for non-experts to comprehend.[17] However, they are designed to create a five-part requirement:[18] financial institutions must (1) establish and maintain customer identity (including beneficial owner and controller of the legal title holder of the account); (2) create and maintain an up-to-date customer profile;[19] (3) monitor transactions to see if they fit with the customer profile of transactions that are legitimate; (4) if not, examine further any such transaction to see if it might represent the proceeds of crime or financing of terrorism, including by examining the source of funds; and (5) if so, report the transaction to the FIU, along with a description of why the financial institution believes that the transaction is suspicious. Recommendations 18, 19, and 26 through 34 (and the relevant materials in the accompanying Methodology for assessment of compliance) address both the supervisory system to ensure that the financial institution comply with their preventive measures requirements and the criminal investigation and prosecution system.

---

[17] *See* Navin Beekarry, *The International Anti-Money Laundering and Combating of the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law*, 31 NW. J. INT'L L. & BUS. 137, 159–60 (2011) (describing the sometimes contradictory and confusing language in the Recommendations). In 2002 an attempt was made by the IMF to reorganize the preventive measures Recommendations into a more accessible, coherent whole. However, in a series of meetings in 2002 delegations to the FATF rejected the effort.

[18] A working group consisting of the Commonwealth Secretariat, the U.N. Office on Drugs ands Crime, the World Bank, and the IMF has drafted a model regulation for the prevention of money laundering and the financing of terrorism as part of a model law on anti-money laundering and terrorism financing. The Model Regulation implements these FATF Recommendations based on the regulatory frameworks in the U.K., Canada, Australia, and Hong Kong. Article 5.1(a)–(e) of the Model Regulation outlines CDD as the "(a) identification of customers, including beneficial owners; (b) gathering of information on customers to create a customer profile; (c) application of acceptance policies to new customers; (d) maintenance of customer information on an ongoing basis; [and the] (e) monitoring of customer transactions." Model Regulation (2006) (on file with the U.N. Office on Drugs and Crime). Article 10 describes a customer profile as being "of sufficient nature and detail . . . to monitor the customer's transactions, apply enhanced customer due diligence where necessary, and detect suspicious transactions." *Id.*

[19] If a new customer profile suggests that the customer is opening an account with proceeds of crime, the financial institution should go directly to Step 4. *Id.*

The financial institution's role focuses on three basic objectives. The first is to help exclude from the financial system possible criminal and terrorist elements. The FATF 40 and Special IX do this by making financial institutions identify and profile potential—and, periodically, existing—customers to screen out possible criminals and terrorists.[20] The second is to make available to law enforcement financial information that can be used in criminal investigations or as evidence in a prosecution. The FATF 40 + Special IX do this by requiring the private sector to maintain records of the identity of all clients and their transactions.[21] The third is to identify customers who might be criminals or terrorists so that law enforcement can decide whether to investigate and prosecute such persons. The FATF 40 + Special IX do this by requiring the private sector to monitor customer transactions based on their profiles and report to law enforcement those that raise suspicion that criminal proceeds or terrorism financing are involved.

The U.S. largely complies with these requirements through statutory and regulatory measures (although the US does not extend these requirements to all those designated non-financial businesses and persons as defined in the Methodology), as well as through guidance issued to financial institutions.[22] The E.U. also largely complies through both Directives

---

[20] *See infra* Part I.B.2, notes 38–48, and accompanying text.

[21] *See infra* Part I.B.2, notes 49–51, and accompanying text.

[22] *See generally* Bank Secrecy Act, *supra* note 2 (requiring U.S. institutions to assist U.S. government agencies in the detection and preventions of money laundering). *See* M. MAUREEN MURPHY, CONG. RESEARCH SERV., RL31208, INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001,TITLE III OF P.L. 107–56 (2001) (providing an overview of the Patriot Act's role in counterterrorism via anti-money laundering efforts); FATF, THIRD MUTUAL EVALUATION REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM, UNITED STATES OF AMERICA 83–226 (2006) (describing the laws and regulations in the U.S. pertaining to money laundering and evaluating the quality of these standards) [hereinafter U.S. MUTUAL EVALUATION REPORT]; Megan Roberts, *Big Brother Isn't Just Watching You, He's Also Wasting Your Tax Payer Dollars: An Analysis of the Anti-Money Laundering Provisions of the USA Patriot Act*, 56 RUTGERS L. REV. 573, 586–7 (2004) (describing the relevant sections of the Patriot Act and their impact on financial institutions). Regulations on customer identification are found in 31 C.F.R. § 103.121 (2006). 31 U.S.C. § 5314(b) authorizes the Secretary of the Treasury to require financial institutions to report suspicious transactions. It is implemented at 21 C.F.R. § 21.110 (2006). There are similar customer identification rules for securities broker-dealers, mutual funds, and futures commission merchants and introducing brokers in commodities. 31 C.F.R. § 103.121 (2006); 31 C.F.R. § 103.122 (2006); *see also* Financial Industry Regulatory Authority, *Anti-Money Laundering*, NOTICE TO MEMBERS NO. 02–21, at 5–7 (2002) (providing guidance to financial institutions in the implementation of anti-money laundering protocol); Financial Industry Regulatory Authority, *Anti-Money Laundering Customer Identification Programs for Brokers/Dealers*, NOTICE TO MEMBERS NO. 03-34, at 347 (2003) (notifying members of the implementation of the Patriot Act as pertains to financial institutions). Under 31 C.F.R. § 103.137(c) (2006), a life insurer is required to have policies and procedures for obtaining "all relevant customer-related information necessary for an effective anti-money laundering program."

(essentially instructions to members of the Union) and implementing legislation at the member state level.[23] The language used to implement the Recommendations is often similar to that found in the Recommendations.[24]

2. Details

FATF Recommendation 5 requires that financial institutions identify their customers, including the beneficial owner of a customer account, which, in the case of legal persons and other legal arrangements such as trusts, includes taking "reasonable measures" to identify the physical persons who own or control the legal person.[25] Recommendation 12 extends these requirements to certain designated non-financial businesses and persons (known as DNFBPs; for purposes of this Report the term "financial institution" should be read to include DNFBPs), which include casinos (which often deal with cash that can be exchanged for chips and vice versa, providing laundering opportunities), real estate agents (in part because real estate is often of high value, it is often used as an investment vehicle by launderers), dealers in precious metals (included for similar reasons, plus the fact that the ownership of precious metals can be easily transferred), lawyers, notaries, and persons who assist in the setting up of trusts and companies (these are often professionals who assist launderers in hiding assets).[26] Although neither the Recommendation itself nor the Methodology uses the term "client profile," Recommendation 5 requires that the financial institutions determine the purpose and intended nature of the business relationship of a potential—and periodically, of a

---

[23] Sorcher, *supra* note 2 at 408–10 (discussing the various Directives already applied and the structure of the proposed "Third Anti-Money Laundering Directive").

[24] *Compare* FATF 40 RECOMMENDATIONS, *supra* note 2, at 5 (Recommendation 5 describing the measures to be taken in performing customer due diligence), *with* Money Laundering Regulations, 2007, S.I. 2007/2157, art. 5 (U.K.) (adopting language almost identical to FATF Recommendation 5 in describing the measures to be taken for customer due diligence). Furthermore, in the course of their assessment work for the IMF and the World Bank, researchers have reviewed implementing statutory and regulatory language in The British Virgin Islands, Hong Kong, Niger, the Philippines, Rwanda, Sierra Leone, and the U.K. and often found language nearly identical to that used in the Recommendations and Methodology. This may be due to decisions to enact the two verbatim so as to ensure that legislation complies with the standard.

[25] FATF 40 RECOMMENDATIONS, *supra* note 2, at 5–6 (Recommendation 5 requiring customer due-diligence and record-keeping). The Methodology allows an exception from this latter requirement in the event the legal person is a public company. METHODOLOGY, *supra* note 4, at 17–18.

[26] FATF 40 RECOMMENDATIONS, *supra* note 2, at 7. Recommendation 22 requires that the principles applicable to financial institutions also be applied to branches and majority owned subsidiaries located abroad. *Id.* at 9.

current—client and a "knowledge of the customer, their business and risk profile, including, where necessary, the source of funds."[27]

This serves two purposes. If a financial institution cannot establish a potential client's identity and profile, it must terminate the business relationship.[28] Second, the financial institution can measure future transactions of accepted clients against this baseline of normal or typical transactions. Specifically, financial institutions must "obtain information on the purpose and intended nature of the business relationship . . . [and] conduct ongoing customer due diligence on the business relationship," and undertake a "scrutiny of transactions under taken throughout the course of th[e] relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds."[29] If the financial institution cannot comply, the financial institution should terminate business relations or not undertake a transaction.[30] Second, the client profile allows the financial institutions to monitor client transactions to see if they are unusual compared with the profile.

A key development in the 2003 Recommendations was the adoption of an optional risk-based approach for certain preventive measures. According to the Financial Action Task Force, the adoption of risk sensitivity "involve[s] identifying and categorizing money laundering risks and establishing reasonable controls based on risks identified . . . ."[31] This risk-based program, which apparently does not apply to terrorism financing, contrasts with the previous program, in which each of the FATF Recommendations was to be implemented objectively regardless of relative risk levels.[32] FATF Recommendation 5 now allows financial institutions to

---

[27] *Id.* at 5.

[28] *Id.* at 9. Recommendation 18 also forbids financial institutions to transact business with shell banks and "guard against" establishing relations with those that do. *Id.*

[29] METHODOLOGY, *supra* note 4, at 17.

[30] *Id.* at 19. It should also consider filing a suspicious transaction report to the Financial Intelligence Unit, but is not required to do so. FATF 40 RECOMMENDATIONS, *supra* note 2, at 8.

[31] FATF, GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING: HIGH LEVEL PRINCIPLES AND PROCEDURES 2 (2007) [hereinafter GUIDANCE ON RBA]. The U.S. has adopted a risk-based system. *See* FED. FIN. INST. EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL 11–27, I-1, K-1, M-1, M-1–2 (2006) [hereinafter FFIEC MANUAL] (describing implementation of the Bank Secrecy Act with a risk-based approach).

[32] GUIDANCE ON RBA, *supra* note 31, at 2. According to the FATF, the new focus on risk allows financial institutions and supervisory authorities to be more efficient and effective in their use of resources and minimize burdens on customers, although it does not say exactly how. *Id.* During the years when the FATF was considering the adoption of a risk based-approach disagreement tended to arise at between those FATF delegates from a law enforcement background and those from a regulatory, particularly bank regulatory background,

determine the extent of such measures on a risk-sensitive basis, depending on the type of customer, business relationship, or transaction.[33] Other Recommendations address new technologies and reliance on third parties for due diligence.[34]

Recommendation 10 requires that financial institutions maintain customer records, including identification and transaction records sufficient to permit reconstruction of individual transactions for evidence in a prosecution, and that these records be maintained for at least five years and be available for inspection by competent authorities.[35] Special Recommendation VII provides more detail with respect to wire transfers.[36]

---

with the latter arguing in favor of a risk-based approach. In general, the banking regulators were used to dealing with concepts of risk while law enforcement was not. "Supervisors must be satisfied that banks and banking groups have in place a comprehensive risk management process (including Board and senior management oversight) to identify, evaluate, monitor and control or mitigate all material risks." BASEL COMMITTEE ON BANKING SUPERVISION, CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION 3 (2006), *available at* http://www.bis.org/publ/bcbs129.pdf.

[33] FATF 40 RECOMMENDATIONS, *supra* note 2, at 19. The Methodology goes on to provide certain examples of higher risk categories. METHODOLOGY, *supra* note 4, at 17. Recommendation 6 singles out a particular category of customers, those individuals who are or have been entrusted with prominent public functions in a foreign country, as well as family members or close associates, which are termed politically-exposed persons. FATF 40 RECOMMENDATIONS, *supra* note 2, at 22. It requires financial institutions and DNFBP to have risk management systems to determine if customers are politically-exposed persons and to take reasonable measures to establish the "source of wealth and source of funds" and to "conduct enhanced ongoing monitoring of the business relationship." In other words, if a customer is a politically exposed person the financial institution and certain others must always take measures to establish the source of funds. Recommendation 6 was added in 2003 to address a perceived public backlash against developed country banks that had laundered the proceeds of developed country dictators. *Id.* at 5–6.

[34] Under FATF Recommendation 8, "[f]inancial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies," and recommends that they have "policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions." *Id.* at 6. FATF Recommendation 9 permits financial institutions to rely on third parties to undertake some due diligence measures in certain cases. *Id.*

[35] *Id.* at 7. FATF Recommendation 10 also suggests that financial institutions keep and maintain client account records, and that they "must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity." *Id.* Competent authorities are defined as "all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors." METHODOLOGY, *supra* note 4, at 62. An FIU is a financial intelligence unit. *Id.* at 66.

[36] *See* IX SPECIAL RECOMMENDATIONS, *supra* note 15, at 3 (recommending that countries take actions to enhance their security and gain meaningful originator information for wire transfers).

This, along with Recommendation 5, allows investigative and prosecutorial authorities to "follow the money" of criminal suspects.[37]

Recommendation 11 requires that "[f]inancial institutions pay special attention to complex, unusual large and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose."[38] Financial institutions must examine, "as far as possible," the background and purpose of such transactions, and establish their findings in writing.[39] This requirement is separate from Recommendation 5's requirement for ongoing customer due diligence with respect to "scrutiny of transactions."[40] Recommendation 13 requires that a financial institution report promptly to the governmental FIU if it "suspects" or has "reasonable grounds" to suspect that funds are the proceeds of a criminal activity.[41] The Methodology describes this as filing an STR.[42] Key to the subject of this Report, Special Recommendation IV further requires financial institutions to file reports if they suspect terrorism financing.[43]

Most jurisdictions provide a template or form for filing STRs (or, in the U.S., Suspicious Activity Reports: SARs). The U.S. form requires, in addition to financial institutions, client, and transaction identification information that a box be checked to characterize the suspicious activity. Options include "structuring/money laundering" and "terrorism financing," as well as various boxes relating to fraud, embezzlement, and identity

---

[37] FATF 40 RECOMMENDATIONS, *supra* note 2, at 4–5 (proposing identification requirements that will allow institutions and governments to more easily trace accounts). The U.S. has put in place similar rules. FFIEC MANUAL, *supra* note 45, at 31, 118–22, 261–64 (detailing identification procedures for different types of customers in order to ensure accounts and transactions are traceable).

[38] FATF 40 RECOMMENDATIONS, *supra* note 2, at 7.

[39] *Id.* at 5, 7 (Recommendations 5 and 10 listing necessary information to be kept on file and how files should be managed).

[40] *Id.* at 5; *see also* METHODOLOGY, *supra* note 4, at 25 ("A financial institution should be required by law or regulation to report to the FIU (a suspicious transaction report–STR) when it suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity.").

[41] METHODOLOGY, *supra* note 4, at 25.

[42] *Id.*

[43] SPECIAL RECOMMENDATIONS, *supra* note 7, at 2. Recommendation 21 requires that financial institutions and DNFBP pay "special attention" to business relationships and transactions with persons from countries that do not or insufficiently apply the FATF Recommendations (although it does not say how this is to differ from non-special (or average) attention). FATF 40 RECOMMENDATIONS, *supra* note 2, at 9. This Recommendation raises the costs of doing business with persons from countries that do not sufficiently apply the Recommendations as a whole. This creates a financial incentive for countries to implement the Recommendations, especially as determined by assessment reports. *Id.*

theft.[44] Also required is a narrative description of the suspected violation, including what is unusual, irregular, and suspicious about the reported transaction.[45]

It is these Recommendations, along with Recommendation 5, that create the system requiring financial institutions to monitor customer transactions based on their profiles and to report to law enforcement those that raise suspicion that criminal proceeds or terrorism financing might be involved. Recommendation 15 requires financial institutions to develop internal policies, procedures, and controls for anti-money laundering programs, including compliance management arrangements, internal training, and audit capacities.[46] Recommendation 16 extends most of these requirements to the same designated non-financial businesses and persons as found in Recommendation 12, although not all.[47]

An essential aspect of this part of the preventive measures system should be emphasized. Financial institutions must design and implement their own systems.[48] While the five-part requirement describes what these

---

[44] FinCEN, Suspicious Activity Report, Part III (Mar. 2011), *available at* http://www.fincen.gov/forms/files/f9022-47_sar-di.pdf.

[45] *Id.* Part V.

[46] FATF 40 RECOMMENDATIONS, *supra* note 2, at 8.

[47] *Id.* at 8. Recommendation 14 protects financial institutions from any liability for filing suspicious activities reports and prohibits the reporting person from revealing that such reports are being made (known as the prohibition against tipping off). U.S. rules comply with these requirements, except that DNFBP include casinos only. *See* 31 C.F.R. § 103.18–19 (2006) (describing the types of transactions that require reporting, including funds derived from illegal activity or transactions that have no business or apparent lawful purpose).

[48] *See, e.g.*, FATF 40 RECOMMENDATIONS, *supra* note 2, at 4 (Recommendation 5 stating: "[f]inancial institutions *should undertake* customer due diligence measures . . . but *may determine the extent* of such measures on a risk sensitive basis. . . .") (emphasis added); *id.* at 5 (Recommendation 6 stating that financial systems *should "[h]ave appropriate risk management systems. . . .*") (emphasis added); *id.* at 6 (Recommendation 8 stating: "financial institutions *should have policies and procedures in place* to address any specific risks associated with non-face to face business relationships or transactions") (emphasis added); *id.* at 6 (Recommendation 9 stating: "[a] financial institution *should satisfy itself* that the third party is regulated and supervised for, and has measures in place to comply with [customer due diligence requirements] in line with Recommendations 5 and 10.") (emphasis added); *id.* at 7 (Recommendation 10 stating: "records *must be sufficient* to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.") (emphasis added); *id.* ("Financial institutions *should pay special attention* to all complex, unusual large transactions . . . . The background and purpose of such transactions *should, as far as possible, be examined*, the findings established in writing, and be available to help competent authorities and auditors.") (emphasis added); *id.* at 8 (Recommendation 13 stating: "[i]f 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 to report promptly its suspicions. . . .") (emphasis added); *id.* ("[f]inancial institutions *should develop program[]s* against money laundering and terrorist financing . . . [including] *[t]he development*

systems are supposed to accomplish, it does not provide any detail as to how they are supposed to do it. Financial institutions are not told how to implement those requirements. An exception to this is Recommendation 25, which requires that government authorities establish guidelines and provide feedback to assist financial institutions and others subject to preventive measures, "in particular in detecting and reporting suspicious transactions."[49]

Neither compliance reports nor sanctions reported by supervisory authorities discuss in any detail the design of compliance systems.[50] Financial institutions also do not publicize exactly how they implement these requirements.[51] Clearly, monitoring of transactions to determine if they vary from the expected client profile is the first key. Such monitoring appears to be based first, as required by Recommendation 11, on whether a transaction (or series of transactions) differs in magnitude from that normally expected of the client, based on the client's profile. Further scrutiny of the transaction can determine if something else appears unusual, such as an unusual transferor or transferee.

One aspect of successful transaction analysis is link analysis, a technique used to find associations within data that might have relevance to the particular research question.[52] Link analysis explores associations within collections of data.[53] Increasing the number of data sets available increases the number and types of links that can be identified. There are a number of different types of data sets that could be helpful in money laundering or terrorism financing link analysis. First, personal and financial data (including personal and businesses names, addresses, phone numbers,

---

of internal policies, procedures and controls, including appropriate compliance management arrangements. . . .") (emphasis added).

[49] *Id.* at 10.

[50] *See id.* (Recommendation 25 stating only that guidelines should be established, not what those guidelines should be).

[51] An important barrier to learning more about how firms actually implement their preventive measures is a desire for protecting proprietary information in the context of competitive concerns, something researchers have learned from numerous interviews conducted with compliance officers at financial institutions in the U.S., Hong Kong, The British Virgin Islands, and the Philippines over the past five years. *See Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF): Case Study*, PRICEWATERHOUSECOOPERS, http://www.pwc.com/lu/en/anti-money-laundering/case.jhtml (last visited May 22, 2012) (providing almost no detail on a preventive measures system recommended by an outside consultant).

[52] Cuéllar, *supra* note 2, at 368–69.

[53] FINCEN, FEASIBILITY OF A CROSS-BORDER ELECTRONIC FUNDS TRANSFER REPORTING SYSTEM UNDER THE BANK SECRECY ACT 10 (2006), *available at* http://www.fincen.gov/news_room/rp/files/CBFTFS_Complete.pdf [hereinafter FINCEN, CROSS-BORDER ELECTRONIC FUNDS]; *see also* Cuéllar, *supra* note 2, at 368–69. Much of the information in the following two paragraphs of text has been provided by Boudewijn Verhelst. Verhelst e-mail, *supra* note 13.

names of beneficial owners and controllers, bank accounts, deposits, funds transfers) would link people and businesses through their financial transactions. For example, this can establish that person A has a relationship with company B and person C.

Next, descriptive links can be established with databases that describe the type of business activities normally conducted by the persons within the link. Such data includes customer identification/profiles and other information such as that which is found in business directories like Dunn and Bradstreet. Links can also be made to data that include money laundering or terrorism financing indicators, such as law enforcement data, case files, or STRs, can also be made.

Once such descriptive links are established, further analysis can help determine if a transaction between identified persons looks unusual or suspicious. For example, if person A has a terrorism-related record or has made past suspicious transactions, payments to company B or C could raise suspicion that payments might be related to terrorism financing. This suspicion could be raised further if person A owns or controls company B and company B itself has no known business, and if B itself is located in a jurisdiction where terrorism is known to be active. If C has a record as a terrorist or terrorist organization, a stronger suspicion might be raised that the payments were made to finance terrorism. Obviously, the greater the amount of relevant data and data types, the more extensive will be the link analysis. However, financial institutions and DNFBPs are restricted in their access to some useful data sets.

Such use of descriptive links and analysis is also described as data mining and the use of red flags.[54] Such "red flags" or "indicators" are based on laundering or terrorism financing typologies. Such typologies are those typically provided by the FATF or local competent authorities (sometimes, they result from international financial institutions' own FIU efforts). Without such typologies it is difficult for financial institutions to know if a transaction or series of transaction is, in fact, an indicator of laundering or terrorism financing.

Some financial institutions contract out some of their customer identification and client monitoring programs to third-party service providers. A review of some of their programs provides some insight into services offered. For example, some firms assist in customer identification and profiling by providing a risk-screening service to check individual or entity names against a comprehensive data set.[55] Firms can also supply

---

[54] G. S. Vidyashankar, Rajesh Natarajan & Subhrangshu Sanyal, *Mine Your Way to Combat Money Laundering, Part 2*, INFO. MGMT. (Oct. 1, 2007, 1:00 AM), http://www.information-management.com/specialreports/20071009/1093416-1.html?zkPrintable=true.

[55] *E.g.*, WORLD-CHECK ONLINE, http://www.world-check.com/ (last visited May 22, 2012).

transaction monitoring services. One firm "monitors and detects" suspicious transactions "across all business lines" using "a fully integrated dynamic and adaptive multidimensional intelligent engine [which] detects suspicious activities."[56] This is accomplished using "risk modeling" and "risk-based algorithms" to "analyze and investigate suspicious activities effectively and efficiently."[57] Presumably, they use link analysis combined with red-flag analysis to help determine which transactions warrant the filing of a report.

C. Public Sector Role

Recommendations 18, 19, and 26 through 32 (and the relevant materials in the accompanying Methodology for assessment of compliance) address both the supervisory system—to ensure private sector compliance with its preventive measures requirements—and the criminal investigation and prosecution system for state law enforcement authorities.[58] The public sector's role focuses on three basic objectives. The first objective is to ensure the private sector's compliance with their preventive measure responsibilities. Essentially, governmental authorities must supervise and regulate financial institutions to ensure compliance. This must include both guidance and examination functions, including the potential application of sanctions. The second objective is to ensure that STRs lead to the investigation of appropriate cases of suspected crime and terrorism. Essentially, a FIU receives and analyzes these reports along with other key information. It then decides which should be further investigated, and it forwards them to the appropriate government agency (typically the police). The FIU then decides, sometimes in consultation with state prosecutors, whether and how to go forward.

Recommendation 25 requires that government authorities establish guidelines and provide feedback to assist financial institutions "in detecting and reporting suspicious transactions."[59] The Methodology goes further by

---

[56] Press Release, GlobalVision Systems, Inc., American Bankers Association Endorses PATRIOT OFFICER® as #1 AML/BSA Solution (Dec. 19, 2005), http://www.gv-systems.com/2010/06/08/american-bankers-association-endorses-patriot-officer%C2%AE-as-1-amlbsa-solution/ [hereinafter ABA Endorses PATRIOT OFFICER®]. *See generally PATRIOT OFFICER® for Banks*, GLOBALVISION SYSTEMS, INC., http://www.gv-systems.com/products-solutions/patriot-officer-for-banks/ (last visited June 11, 2012) (providing anti-money laundering and anti-terrorist financing monitoring software designed to comply with the USA Patriot Act and other anti-laundering regulations).

[57] ABA Endorses PATRIOT OFFICER®, *supra* note 56.

[58] Recommendations 18 and 19 are listed under the preventive measures section of the FATF Recommendations; 26 through 32 are under "C. Institutional and Other Measures Necessary in Systems for Combating Money Laundering and Terrorist Financing: Competent authorities, Their Powers and Resources." FATF 40 RECOMMENDATIONS, *supra* note 2, at 9–11.

[59] *Id.* at 10.

stating that authorities should provide a description of money-laundering and terrorism-financing techniques and methods and any additional measures to ensure that the systems are implemented by financial institutions.[60] This includes information on current techniques, methods and trends (typologies);[61] examples of actual money laundering cases; and case-by-case feedback, including if an STR was found to relate to a legitimate transaction.

In order to ensure compliance with the preventive measures, Recommendation 23 requires that financial institutions be subject to adequate regulation and supervision to ensure implementation of the preventive measures,[62] while Recommendations 29 and 17 require that supervisors have adequate powers to ensure compliance including the imposition of sanctions.[63] Recommendation 26 requires that countries establish an FIU[64] to serve as a national center for the receipt, analysis, and

---

[60] METHODOLOGY, *supra* note 4, at 33.

[61] *See Methods and Trends*, FATF, http://www.fatf-gafi.org/topics/methodsandtrends/ (last visited May 22, 2012).

> The methods used for laundering money and the financing of terrorism are in constant evolution. As the international financial sector implements the FATF standards, criminals must find alternative channels to launder proceeds of criminal activities and finance illicit activities. The FATF identifies new threats and researches money laundering and terrorist financing methods. FATF Typologies reports describe and explain their nature, thus increasing global awareness and allowing for earlier detection.

Id.

[62] FATF 40 RECOMMENDATIONS, *supra* note 2, at 9–10. Recommendation 24 extends this requirement to designated non-financial businesses and persons. *Id.* at 10.

[63] *Id.* at 9, 11. U.S. laws also comply with these requirements. *See* 31 C.F.R. § 103 (2004) (addressing "financial recordkeeping and reporting of currency and foreign transactions"); *see also* 17 C.F.R. § 240.17a-1 (1980) (requiring recordkeeping of financial transactions). The U.S. has levied significant fines, as well as other supervisory and regulatory orders, against financial institutions and casinos. *See* David Zaring & Elena Baylis, *Sending the Bureaucracy to War*, 92 IOWA L. REV. 1361, 1414–15 (2007).

> Since September 11, FinCEN has imposed a staggering number of fines on banks for failing to meet its reporting requirements. Moreover, those fines have been extraordinarily large. ABN AMRO, a large European bank, has been hit with a $30 million fine (and more from state regulators). Western Union has also been hit with a $30 million fine for its record-keeping failures. And the Department of Justice has brought criminal prosecutions for anti-money-laundering violations, which resulted in a $50 million civil monetary penalty against AmSouth and $43 million in combined criminal and civil fines against Riggs Bank, which put the bank out of business.

Id. (footnotes omitted).

[64] FATF 40 RECOMMENDATIONS, *supra* note 2, at 10–11. The line between what some countries formally refer to as their financial intelligence unit and other law enforcement agencies is often blurry. This Report refers to the financial intelligence unit using a function-

dissemination of STRs and other information regarding potential money laundering or terrorist financing. It further states that the FIU should have timely access, directly or indirectly, to the financial, administrative, and law-enforcement information that it requires to properly undertake its functions, including the analysis of STRs.[65] Recommendation 10 states that competent authorities (including FIUs) should have access to records kept by financial institutions and DNFBPs.[66] Finally, Recommendation 40 states that countries should ensure that their competent authorities provide the widest possible range of international cooperation to their foreign counterparts, including information relating to money laundering, provided that controls and safeguards are in place to ensure that information exchanged is used only in a manner consistent with obligations concerning privacy and data protection.[67] The Methodology further states that FIUs should be authorized to allow foreign intelligence units to search their own databases, including law enforcement databases, subject to confidentiality safeguards limiting the use of the data.[68] This is the only substantive Recommendation relating to FIUs.[69]

---

al definition. *See What is an FIU?*, THE EGMONT GROUP FINANCIAL INTELLIGENCE UNITS, http://www.egmontgroup.org/about/what-is-an-fiu (last visited May 22, 2012) (describing the different types of FIUs); The Egmont Group, The Egmont Definition of a Financial Intelligence Unit 1–2 (interpretive note, last visited May 22, 2012), *available at* http://www.egmontgroup.org/library/download/8 (providing a functional definition of FIU not cabined to any particular sort of law enforcement).

[65] FATF 40 RECOMMENDATIONS, *supra* note 2, at 10–11. For example, FinCEN has access to numerous databases. These include several databases of criminal reports sourced from the Immigration and Customs Enforcement's TECS II system, the FBI's National Criminal Information Center, the Drug Enforcement Administration's Narcotics and Dangerous Drugs Information and NDIC Systems, the U.S. Secret Service database, and the U.S. Postal Inspection Service. It also has access to the Office of Foreign Assets Control's list of Specially Designated Nationals, the Social Security Administration's Death Master File, and the State Department's list of Designated Foreign Terrorist Organizations. It also has access to commercial database services from organizations such as Dun & Bradstreet, LEXIS/NEXIS, and credit bureaus as well as commercially available lists of "Politically Exposed Persons." FinCEN also maintains its own database of investigations and queries conducted through FinCEN's systems. FINCEN, CROSS-BORDER ELECTRONIC FUNDS, *supra* note 53, at 9–10.

[66] FATF 40 RECOMMENDATIONS, *supra* note 2, at 7.

[67] *Id.* at 13–14.

[68] METHODOLOGY, *supra* note 4, at 46.

[69] *See generally* FATF 40 RECOMMENDATIONS, *supra* note 2, at 13. The draft methodology included a significant number of criteria spelling out in detail the duties of financial intelligence units, including most of those described in *infra* notes and accompanying text. However, during a meeting in Basel in February, 2002 representatives of the Egmont Group, an informal association of financial intelligence units, objected to the spelling out in such detail of the purposes and activities of FIUs because of the difficulty of finding consensus on such a large amount of detail from such a large group. Nevertheless, the representatives largely concurred that the criteria in the methodology described an effective financial intelligence unit. IMF, ANNUAL REPORT 2002, at 38 (2002). The U.S. largely complies with these re-

Dividing the task of determining suspicious and *really* suspicious transactions between the private sector and public FIUs usually begins with the receipt of an STR, after which the FIU engages in a two-part analysis. In the first part, known as "tactical analysis," the FIU looks for additional information on the persons and transactions involved or other elements involved in a particular case to provide the basis for further analysis.[70] A key element of such tactical analysis is link analysis, which has been discussed at length above in the context of transaction monitoring and suspicious transaction reporting. Financial intelligence units typically have available various types of data, including those publicly available databases to which the private sector has access. An FIU can also have access to nonpublic databases such as tax records, police records, immigration and customs records, vehicle registries, and supervisory findings, as well as investigation reports for ongoing investigations, criminal records (which are nonpublic in many countries), currency transaction reports, currency and monetary instrument reports, and related-party data (same address or telephone number, known associates, etc.).[71]

Following tactical link analysis, the FIU typically undertakes operational analysis. Operational analysis uses tactical information to formulate different hypotheses on the possible activities of the suspect to produce operational intelligence for use by investigators. It uses:

> [A]ll sources of information available to the FIU to produce activity patterns, new targets, relationships among the subject and his or her accomplices, investigative leads, criminal profiles, and—where possible—indications of possible future behavior. One of the techniques of operational analysis used in some FIUs is financial profiling.[72]

Based on such analysis, the FIU may or may not disseminate a report for further investigation.[73] In recommending an SAR for further investigation, FIUs may include a description of what they had learned from these different types of analysis. This is often called "actionable intelligence" that can assist law enforcement in conducting a further investigation.

Another important function of the FIU is strategic analysis, or the development of relevant knowledge on laundering or terrorism-financing techniques. Examples include the identification of evolving criminal patterns in a particular group or the provision of broad insights into

---

quirements. *See* U.S. MUTUAL EVALUATION REPORT, *supra* note 22, at 226-40 (describing the U.S. laws that fulfill FIU obligations).

[70] *See* SCHOTT, *supra* note 3, at VII-5–6 (describing the analytical role of FIUs); *see also* IMF, FINANCIAL INTELLIGENCE UNITS: AN OVERVIEW 57–58 (2004) [hereinafter IMF, FIUs].

[71] Verhelst e-mail, *supra* note 13.

[72] IMF, FIUs, *supra* note 70, at 60.

[73] *Id.* at 61.

emerging patterns of criminality, including transactions particular to a given group, ideology or geographic location.[74] The FIU can then use these for its own operational analysis of STRs through linking as well as to develop guidelines, typologies etc. for use by financial institutions.[75] This generally follows the system used by FinCEN in the U.S.[76]

II. DETECTION OF TERRORISM FINANCING

A. Overview

As discussed above, the FATF adopted the Special Recommendations in November, 2001, after the previous month's terrorist attacks against the U.S. However, that the financing of terrorism should be so closely tied to anti-money laundering was by no means completely obvious. While terrorism had existed before 9/11, the original FATF 40 made no reference to it. Anti-money laundering laws *were designed to stop criminals from taking criminal proceeds and running them through the financial system in a series of transactions to hide their criminal origins and/or actual ownership. On the other hand, terrorism financing need not involve criminal origins but only a particular type of criminal destination: terrorism.*

Of course, there were some obvious connections. As discussed above, identifying the financial institution's clients was a key aspect of anti-money laundering preventive measures. These measures could also be used to identify whether the client was a terrorist, provided of course that the financial institution or the authorities knew who the terrorists were. This proved to be a valuable avenue for combating terrorism-financing measures. Before the 9/11 attacks, the U.N. Security Council had passed resolutions requiring all states to freeze accounts held by members of al-Qaeda and the Taliban and had set up the al-Qaeda and Taliban Sanctions Committee.[77] The Committee created a consolidated list of entities and officials associated with these organizations, as submitted by members. Subsequent

---

[74] *See* SCHOTT, *supra* note 3, at VII-3 (discussing definitions of FIUs that emphasis specificity to each nation's needs and characteristics); *see also* IMF, FIUs, *supra* note 70, at 59–60 (noting that unusual transactions develop the basis for further investigation by the financial intelligence units).

[75] IMF, FIUs, *supra* note 70, at 60.

[76] *See generally* U.S. MUTUAL EVALUATION REPORT, *supra* note 22, at 126–36 (discussing record keeping rules for the banking, securities, insurance, and money services business sectors to combat money laundering and requirements to report unusual, suspicious transactions).

[77] S.C. Res. 1267, ¶ 4, U.N. Doc. S/RES/1267 (Oct. 15, 1999).

resolutions strengthened this original commitment.[78] Resolution 1373—passed as a result of the 9/11 attacks—extended the requirement of states to freeze accounts to terrorists other than al-Qaeda and the Taliban.[79] The General Assembly had also adopted a Convention on Suppression of Terrorism Financing, although it did not go into force until April, 2002.[80] The convention requires contracting states to take appropriate measures "for the identification, detection and freezing or seizure of any funds used or allocated for the purpose of committing [terrorist offenses as defined in the convention] as well as the proceeds derived from such offences, for purposes of possible forfeiture."[81]

Assuming that someone could come up with a list of possible terrorists, financial institutions could compare that list to their account holders to see if there was a match, much as they could now do with known criminals. However, as discussed above, the new anti-terrorism financing regime required financial institutions to profile clients and monitor transactions to see if they might have some involvement in the financing of terrorism, and to report those cases as well. When the FATF first published its 40 Recommendations, financial institutions in most FATF member countries were in the process of implementing a client identification-,

---

[78] *Id.* ¶ 6; *see also Security Council Committee Pursuant to Resolutions 1267 (1999) and 1989 (2011) Concerning Al-Qaida and Associated Individuals and Entities*, U.N. SECURITY COUNCIL, http://www.un.org/sc/committees/1267/ (last visited May 22, 2012) (explaining subsequent resolutions modified and strengthened policies by designating sanction measures to specific individuals and entities associated with Al-Qaeda).

[79] S.C. Res. 1373, ¶ 1, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

[80] *See generally* International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, 2178 U.N.T.S. 197 [hereinafter Suppression of Financing Convention] (prohibiting the financing of terrorism).

[81] *Id.* art 8. The Treaty defined terrorism as acts described in any treaty in the Annex, and:

> 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, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

Id. art. 2(1)(b). The treaties listed in the Annex include unlawful seizure of aircraft, unlawful acts against the safety of civil aviation, crimes against internationally protected persons (including diplomatic agents), the taking of hostages, the unlawful acquisition or threat to nuclear material, unlawful acts of violence at airports serving international civil aviation and against the safety of civil aviation, unlawful acts against the safety of maritime navigation, unlawful acts against the safety of fixed platforms located on the continental shelf, and terrorist bombings. *Id.* Annex; *see also* G.A. Res. 164, Annex, U.N. Doc A/52/164 (Jan. 9, 1998) (attaching the International Convention for the Suppression of Terrorist Bombings for adoption by the General Assembly). With certain limited exceptions in each convention, the terrorists must be nationals of a different state than the state in which the terrorist act took place. *See* Suppression of Financing Convention, *supra* note 80, art. 3; *see also* G.A. Res. 164, *supra* note 81, annex, art. 2.

resolutions strengthened this original commitment.[78] Resolution 1373—passed as a result of the 9/11 attacks—extended the requirement of states to freeze accounts to terrorists other than al-Qaeda and the Taliban.[79] The General Assembly had also adopted a Convention on Suppression of Terrorism Financing, although it did not go into force until April, 2002.[80] The convention requires contracting states to take appropriate measures "for the identification, detection and freezing or seizure of any funds used or allocated for the purpose of committing [terrorist offenses as defined in the convention] as well as the proceeds derived from such offences, for purposes of possible forfeiture."[81]

Assuming that someone could come up with a list of possible terrorists, financial institutions could compare that list to their account holders to see if there was a match, much as they could now do with known criminals. However, as discussed above, the new anti-terrorism financing regime required financial institutions to profile clients and monitor transactions to see if they might have some involvement in the financing of terrorism, and to report those cases as well. When the FATF first published its 40 Recommendations, financial institutions in most FATF member countries were in the process of implementing a client identification-,

---

[78] *Id.* ¶ 6; *see also Security Council Committee Pursuant to Resolutions 1267 (1999) and 1989 (2011) Concerning Al-Qaida and Associated Individuals and Entities*, U.N. SECURITY COUNCIL, http://www.un.org/sc/committees/1267/ (last visited May 22, 2012) (explaining subsequent resolutions modified and strengthened policies by designating sanction measures to specific individuals and entities associated with Al-Qaeda).

[79] S.C. Res. 1373, ¶ 1, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

[80] *See generally* International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, 2178 U.N.T.S. 197 [hereinafter Suppression of Financing Convention] (prohibiting the financing of terrorism).

[81] *Id.* art 8. The Treaty defined terrorism as acts described in any treaty in the Annex, and:

> 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, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

Id. art. 2(1)(b). The treaties listed in the Annex include unlawful seizure of aircraft, unlawful acts against the safety of civil aviation, crimes against internationally protected persons (including diplomatic agents), the taking of hostages, the unlawful acquisition or threat to nuclear material, unlawful acts of violence at airports serving international civil aviation and against the safety of civil aviation, unlawful acts against the safety of maritime navigation, unlawful acts against the safety of fixed platforms located on the continental shelf, and terrorist bombings. *Id.* Annex; *see also* G.A. Res. 164, Annex, U.N. Doc A/52/164 (Jan. 9, 1998) (attaching the International Convention for the Suppression of Terrorist Bombings for adoption by the General Assembly). With certain limited exceptions in each convention, the terrorists must be nationals of a different state than the state in which the terrorist act took place. *See* Suppression of Financing Convention, *supra* note 80, art. 3; *see also* G.A. Res. 164, *supra* note 81, annex, art. 2.

profiling-, monitoring-, and STR-reporting system for criminal proceeds reflecting the system required by the FATF 40. But when the system was extended to terrorism financing, neither financial institutions nor their supervisors had much, if any, relevant experience. While they had not originally been in the business of finding criminal proceeds, at least financial institutions had years of learning how to do so, as well as considerable typology guidance from competent authorities, the FATF, and FSRBs.

B. Terrorism Typologies/Indicators/Red Flags

As discussed above, financial institutions implement their STR-reporting requirements by, among other things, identifying clients (including determining exactly who they really are), creating client profiles, monitoring client transactions with respect to those profiles to identify large or unusual transactions, performing link analysis, and comparing transactions to known typologies of money laundering and terrorism to see if any red flags are raised.

Such typologies are provided by domestic competent authorities, as well as by the FATF or FSRBs. But what are those terrorism typologies, indicators and red flags?

Soon after the FATF adopted the Special Recommendations, the FATF Secretariat published *Guidance for Financial Institutions in Detecting Terrorist Financing*, stating that that "[i]t should be acknowledged…that financial institutions will probably be unable to detect terrorist financing as such."[82] While there was mention of charities as being of special concern, there was no attempt to tie these to any special type of charity, or to charities sending payments to locations known to have terrorism concerns. The National Commission on Terrorist Attacks upon the U.S.'s *Staff Report on Terrorist Financing*, published two years after the adoption of the Special IV, concluded that:

> [Financial institutions] can be most useful in the fight against terrorist financing by collecting accurate information about their customers and providing this information . . . to aid in terrorism investigations. . . . However, the requirement that financial institutions file SARs does not work very well to detect or prevent terrorist financing, for there is a fundamental distinction between money laundering and terrorist financing.

---

[82] FATF, GUIDANCE FOR FINANCIAL INSTITUTIONS IN DETECTING TERRORIST FINANCING 3 (2002).

> Financial institutions have the information and expertise to detect the one but not the other.[83]

In its sixth report, the U.N. Security Council's Monitoring Team was not enthusiastic about the effectiveness of preventive measures in deterring terrorism financing, in part because of lack of guidance. "The volume of suspicious transaction reports has increased tremendously, though the procedure suffers from a lack of guidance as to what to look for. . . . Only a small proportion of the reports are related to terrorist financing and hardly any have been associated with Al-Qaida."[84]

Early in 2008, the FATF released its most comprehensive report to date on terrorist financing.[85] The Report stated that "[d]espite the challenge in developing generic indicators of terrorist financing activity financial institutions may nevertheless identify unusual characteristics about a transaction that should prompt the filing of a suspicious transaction report."[86] However, the cases and examples dealt almost entirely with individuals or organizations identified as having terrorism connections rather than through terrorism financing indicators (including "media coverage of account holder's activities,"[87] presumably when the media reveals that someone may be connected to terrorism in some way). The only uniquely terrorism financing indicators noted in the Report were charity and relief organizations sending to or receiving funds from "locations of specific concern."

While there has so far been relatively little guidance to financial institutions as to indicators or typologies of greater risk of terrorism financing, they are still required to implement Special IV, VI, and VII. Anecdotal evidence gathered largely from informal interviews with compliance officers at financial institutions in the U.S. has indicated that at least some financial institutions have implemented "defensive" systems based largely on whether a client or potential client is a charity that makes payments to charities based in terrorism "hot spots;" this includes not accepting the charity as a client or filing STRs after a charity makes any

---

[83] JOHN ROTH, DOUGLAS GREENBURG, & SERENA WILLE, NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, MONOGRAPH ON TERRORIST FINANCING, STAFF REPORT TO THE COMMISSION 52–54 (2004).

[84] Sixth Report of the Analytical Support and Sanction Monitoring Team, transmitted by letter dated Mar. 8, 2007 from the Chairman of the Security Council Comm. established pursuant to resolutions 1526 (2004) and 1617 (2005) concerning Al-Qaeda and the Taliban and associated individuals and entities, at 24, U.N. Doc. S/2007/132 (Mar. 8, 2007).

[85] *See generally* FATF, TERRORIST FINANCING (2008) (exploring issues of terrorist requirements for fund, how terrorists raise and move fund, and the international response to terrorist financing).

[86] *Id.* at 29.

[87] *Id.* at 31.

large transaction. If true, this would not only raise costs to financial institutions, but would also reduce financial services to needy clients. It would also suggest that financial institutions' STRs included at least a high number of false positives (and perhaps a high number of false negatives), which would raise costs to FIUs and law enforcement without improving capacity to deter or prevent terrorism financing.

III. STUDY TO IDENTIFY TERRORISM FINANCING INDICATORS

A. Overview

This preliminary study on terrorism-related prosecutions in the U.S. was completed by Professor Richard Gordon of the Case Western Reserve University, with assistance from students at Case Western. It is to be used in the completion of a final report by Professor Nikos Passas of Northeastern University and the Honorable Susan Eckert of Brown University, which will include cases from other jurisdictions, additional analytical discussion, and bibliographical material.

The objective of the U.S. study is to identify red flags or indicators of terrorism that financial institutions can use in implementing their duties to monitor client transactions and report those that raise a suspicion of terrorism financing. The study research methodology included five steps:

(1) We selected terrorism cases that were successfully prosecuted.

(2) We examined those cases to determine which involved a transaction though a regulated financial institution, and we collected the relevant client identification, profiling, and transaction data.

(3) We examined the data to identify any possible indicators of terrorism financing.

(4) We determined if any SARs were filed by financial institutions with respect to those transactions. We reviewed the SARs to see why they were filed, including by examining the SAR narrative to determine what, if any, additional information the reporting institution had uncovered.

(5) Finally, we determined if FinCEN had referred the SAR for further investigation.

While it was relatively easy to complete steps 1 and 2, difficulties arose with completing the other steps. In particular, with respect to step 3 it proved difficult to acquire actual records of most of the identified transactions and impossible to acquire client identifying and profiling information, although in a number of cases it proved possible to acquire sufficient descriptive information to make some tentative conclusions about possible indicators. With respect to step 4, while research was continuing,

FinCEN proposed a new regulation (which became final in December 2010) that changed previous law, which had permitted a financial institution to release an SAR, provided that it did not "tip off" persons involved in the suspicious transaction. (This would have been an impossibility in the cases we were reviewing because all the persons had already been prosecuted.) The new regulation made step 5 in our methodology impossible to implement.

As a result, the findings of this study are more tentative than was expected at the outset. However, the study suggests some alternatives that might be pursued that could help rectify the deficiencies in the current study that arose due to the inability to implement steps 4 and 5.

B. Steps 1 & 2: Terrorism Case Selection, Identification of those Involving Financial Transactions and Collection of Transaction Records

In December, 2008, Jeffrey Breinholt[88] of the U.S. Department of Justice (DOJ) provided the project with a list of 230 U.S. cases that he, in consultation with and other DOJ officials had identified as involving a prosecution in which the U.S. alleged that the defendants(s) may have been involved in supporting terrorism or some form of terrorist activity.[89] This list did not include the 9/11 case, which had been reviewed extensively by the U.S. 9/11 Commission and which did not turn up any apparent terrorism-financing indicators. This list was supplemented in October, 2010 with an additional thirty-three cases to bring the list up-to-date.

By reviewing DOJ press releases, news stories, and published court opinions, researchers identified forty-seven cases as possibly involving terrorism financing. Each involved either deposit-taking institutions or money-transfer agents. Researchers then collected and reviewed relevant court documents that were either published or made available free of charge through the Internet. These often included pleadings and motions, including bills of indictment and requests for warrants, freezing orders, material witness orders, and supporting affidavits. On rare occasions, some evidence submitted during the trial was also located and reviewed. Of considerable help to locating such materials is The Nine Eleven Finding Answers Foundation (NEFA), which maintains a website that includes many publically available documents on terrorism-related criminal and civil

---

[88] Mr. Breinholt has been Deputy Chief, Counterterrorism Section and Coordinator, Terrorist Financing Task Force of the U.S. Department of Justice.

[89] In many of the prosecutions, charges were not brought for either terrorism or material support, but in all instances charges were brought for some other offence, including: making false statements; immigration fraud; money laundering (including structuring or operation or use of unlicensed MSBs); threats other than terrorist threats; hoaxes; and air violence. Material witness orders that involved no criminal charge were also included.

cases.[90] From the group of forty-seven, researchers identified thirty that might involve both terrorism financing and a regulated financial institution. For these cases, researchers attempted to collect and examine documents and evidence not published or available for free on the internet.

Researchers first attempted to obtain copies of client identification, profiling information, and transaction records from the banks and transfer agents in question. However, these reporting persons refused to share such records, citing the expense involved in collecting and providing us with such information and the concern that doing so might breach FinCEN's SAR confidentiality rules.[91] They made this later point even though we did not mention SARs themselves and even though no law or regulation made reference to the confidentiality of information that may have given rise to the filing of an SAR.

Failing in this attempt, researchers then turned to records made available as evidence in prosecution of the terrorism cases. In theory, all publicly available case documents, including all evidence submitted for trial, can be obtained in two ways: (1) in hard copy from the relevant court (mostly for cases that are older than ten years); or (2) through the online federal court filing and retrieval system known as PACER. However, in many cases the number of pages of documents filed from beginning to end run to the tens of thousands. The court keeps a docket of filings for each case, but the docket entries themselves rarely identify exactly what kind of evidence, if any, is included in the filing. As a result, it becomes necessary to individually examine documents to identify those that relate to financial transactions. For documents filed with the court in hard copy, this requires physically visiting the court, requesting documents from the court clerk, and reviewing them on-site. For most relevant documents filed through PACER, this requires downloading each page at a cost of $ 0.10 per page.

After attempting and failing to identify relevant documents by reviewing court dockets filed on PACER, researchers contacted via e-mail and telephone[92] those DOJ personnel who prosecuted each case for assistance identifying relevant documents. Follow-up e-mails and telephone calls were made where appropriate. Prosecutors had to divert their time from other pressing work to assist researchers with work that would not (at

---

[90] *See Featured Legal Cases*, NINE ELEVEN FINDING ANSWERS [NEFA] FOUNDATION, http://nefafoundation.org//index.cfm?pageID=29 (last visited May 22, 2012) (providing a portal to domestic criminal and civil and international cases on terrorism).

[91] Given the nature of the refusals given by the first few approached, researchers gave up without pursuing the rest, deeming any additional efforts to be pointless.

[92] Each e-mail described the nature and purpose of the project, summarized the available details of the case, and requested any information regarding financial transactions, especially PACER document numbers.

least directly) assist in the prosecution of cases, current or future.[93] Not surprisingly, in many instances prosecutors were not able to respond to requests for assistance.[94] In many instances, prosecutors informed us that for various reasons (including decisions not to charge defendants with crimes requiring financial transaction evidence or the entrance of guilty pleas to such crimes prior to the introduction of evidence) no relevant documents were admitted into evidence, and therefore they could not be shared with researchers. As a result, only in a few cases have prosecutors been able to share with researchers actual documentary evidence of financial transactions. In those instances, however, thousands of pages representing tens of thousands of transactions have been provided.

Of those thirty cases, researchers found sufficient financial information to draw conclusions in twenty-four. A description of these cases, and of the relevant information obtained with respect to financial transactions are included in the Annex.

C. *Step 3: Analysis of Transactions for Indicators*

As discussed above, in order to determine if a transaction is suspicious it is necessary for the financial institution to identify and profile the client, to monitor the client's transactions, and to examine transactions. However, in the initial review of the thirty cases for evidence of suspicious transactions, it was not possible to consult client identification and profiling information. Nevertheless, in the vast majority of instances it was possible to take educated guesses, based on publicly available information concerning the client in question, to determine if payments would fit an assumed client profile as being legitimate. This is because most transactions fall into three types: (1) those that are too small to be consequential; (2) those that are consequential but that appear to be between individuals or entities with no obvious legitimate connection that would render the transaction suspicious; and (3) those that appear to be between individuals or entities with a legitimate reason to make the transaction.

---

[93] Case Western Reserve University researchers discussed this matter with a number of prosecutors. Some noted that while the results of our research project might help future financial institution compliance officers and/or investigators in identifying terrorism financing suspects, the results would be unlikely to help those who ultimately *prosecuted* those cases. Some also suggested that they believed that, from their experience, there were no "terrorism indicators," and that the project was unlikely to be of any assistance to law enforcement.

[94] In a few instances prosecutors had left the DOJ for private practice. In these cases they did respond to e-mail inquiries but were unable to assist in finding relevant documents.

D. Step 4: Review any SARs Filed

As discussed above, part of a reporting institution's preventive measures obligation is to examine any unusual transaction to determine if there is an actual suspicion that it concerns terrorism financing. Because the methods by which reporting persons implement these requirements are expensive and proprietary, they are understandably reticent to share any details. We sought instead to obtain copies of any SARs filed so that we could examine the narratives and determine if link analysis, reference to any publically available information on the clients, or typologies might have played a role in uncovering relevant indicator information. We were not successful.

The Intelligence Reform and Terrorism Prevention Act of 2004 states that "[t]he global war on terrorism and cutting off terrorist financing is a policy priority for the U.S. and its partners, working bilaterally and multilaterally through the U.N., the U.N. Security Council and its committees…and other multilateral fora."[95] Under § 5318(g) of the USA Patriot Act,[96] a financial institution and its agents are prohibited from notifying any person who is the subject of an SAR either that an SAR was filed or of the circumstances surrounding the filing. Congress apparently included this provision in order to prevent the tipping off of launderers and terrorists, which could spoil any current or future investigation. There was, however, no prohibition on release of information that an SAR had been filed or of the SAR itself that applied to government authorities. The implementing regulations essentially restated the statutory language.[97] Also, courts had held that SARs were not strictly confidential and that disclosure of an SAR in a case where the subject of the report has already been convicted will not compromise an ongoing law enforcement investigation, or provide information to a criminal wishing to evade detection.[98] This was clearly the situation with respect to the cases we were investigating.

Based on such policy, law, and precedent, researchers requested copies from the DOJ of any SARs filed with respect to the thirty cases that we had identified, but with any information concerning innocent persons redacted. Officials at the DOJ were sympathetic and prepared to release

---

[95] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7701, 118 Stat. 3638, 3858 (2004).

[96] 31 U.S.C. § 5318(g)(2)(A) (2006).

[97] *See* 12 C.F.R. § 21.11(k) (2011) (providing similar guidance in the administrative regulation as in the enacting legislation).

[98] *See* Whitney Nat'l Bank v. Karam, 306 F. Supp. 2d 678, 680 (S.D. Tex. 2004) (noting that SAR disclosure poses a threat when a suspect is still at large); *see also* BizCapital & Indus. Corp. v. Comptroller of Currency, 467 F.3d 871, 873 (5th Cir. 2006) (noting that SARs are not categorically privileged under certain circumstances).

redacted SARs to researchers, but then FinCEN issued a new regulation that prohibits private or public sector persons from revealing if an SAR was filed, or any contents of that SAR, to anyone in any circumstances.[99] While there appears to be no statutory authority for such a regulation (and therefore that it may be *ultra vires*, the statute may therefore be invalid), its issuance prevented DOJ from releasing any redacted SARs to researchers.

Because we were unable to review the SARs, it was impossible for researchers to obtain the information necessary to determine if financial institutions had in fact used their knowledge of customer information, customer transactions, and link analysis, typologies, etc. to conclude that a transaction was suspicious. It also made it impossible for researchers to determine if FinCEN had referred such SARs to law enforcement for further investigation, or if they had added actionable intelligence to the SARs that would suggest either money laundering or terrorism financing.

E. Response to New Regulation Preventing Implementation of Step 4

While the new Regulation prevents both public and private sectors from revealing if SARs have been filed or the contents of those SARs, it also made clear that "[w]ith respect to the SAR confidentiality provisions only, institutions may disclose underlying facts, transactions, and documents for any purpose, provided that no person involved in the transaction is notified and none of the underlying information reveals the existence of an SAR."[100] For this reason, financial institutions should no longer be concerned with SAR confidentiality issues, and they should only be concerned about the costs of releasing identification, profiling, and transaction documents. Financial institutions may, however, continue to be reticent about releasing any link analysis that might lead a reviewer to believe that an SAR had, in fact, been filed.

In order to encourage reporting persons to release identification, profiling and transaction data with respect to the identified cases, researchers have approached a number of financial institutions and requested that they create a committee to assist the Counterterrorism Task Force in identifying terrorism financing methodologies (CACTF). The Committee would encourage reporting persons in question to release the relevant documents, and it would provide technical assistance where needed. We expect CACTF to be up and running by End May, 2011.

---

[99] *See* FinCEN; Confidentiality of Suspicious Activity Reports, 75 Fed. Reg. 75593, 75598 (Dec. 3, 2010) (to be codified as 31 C.F.R. § 103) (explaining exceptions for connected parties and certain other government officials).

[100] *Id.* (citations omitted).

F. New Step 5: Review Documents released by Reporting Persons

Researchers are working with the initial members of CACTF to plan a workshop sometime in the fall of 2011 to review any released documents. The workshop will include AML/CFT compliance officers from member banks. It is hoped that this conference will help deepen our understanding of the nature of the cases identified in this Report.

IV. CONCLUSIONS

Based on assumptions concerning client identification and profiles, researchers examined transactions to determine if there was anything unusual in those transactions that would raise a suspicion of terrorism financing. In doing so, we did not indicate instances where a person was identifiable as a terrorist or terrorist organization, in that this was not an "indicator" but a fact.

In the twenty-four cases where sufficient financial information was available to draw a conclusion, fourteen indicated instances of *classic money laundering typologies, including placement, layering, integration, or an unlicensed money service business*. Only three of these cases involved criminal proceeds, although an additional three appear to involve diversion of charitable donations to terrorists which could have, in effect, constituted theft of legitimate donations. In eight cases there was no suspicious transaction of any kind (other than a party to a transaction was a known terrorist), although in two of these, criminal proceeds were involved. Only one indicated a possible set of transactions that might be a unique indicator for terrorism financing.

Terrorist financers appear to be using classic money laundering typologies regardless of whether they are trying to launder the proceeds of crime. It appears that they do so either to hide the origins of the funds or the recipient of the funds without leaving a directly traceable transaction between origin and recipient. In other words, they are acting in a fashion similar to that of former New York Governor Eliot Spitzer, who used classic structuring transactions to hide that he was making payments to prostitutes.[101]

Therefore, simply by using standard anti-money laundering typologies financial institutions should have been able to identify fourteen of the twenty-four instances of terrorism financing as being suspicious, though not on their face to raise suspicion of terrorism financing. What we can tell from examining the cases is that it might have been possible for the

---

[101] *See generally* Gordon, *Trysts or Terrorists?*, *supra* note 1 (explaining how SARs exposed governor Eliot Spitzer's political scandal involving money laundering and prostitution).

reporting institution to have discovered terrorism connections during the examination process, or for FinCEN to have done so when receiving the SAR. However, because researchers did not have access to this information it is impossible to determine at this time.

The one case indicating a possible set of transactions that might be a unique indicator for terrorism financing involved repeat purchases from a military equipment store. To determine if this should raise a suspicion of terrorism finance, it would be necessary to see if such purchases are, in fact, sufficiently unusual to distinguish them in a meaningful way from non-terrorism related purchases. This could perhaps be done by comparing them with other purchases from similar stores. Researchers will attempt to locate such information for the final Report.

SUMMARY TABLE

DATA, TYPE OF TRANSACTION(S), SUSPICIOUS TRANSACTION

Case #	**Data Available**	**Type of Transaction(s)**	**Suspicious Transaction(s) [ST]? If yes, type Proceeds of crime [PC]?**
1	Detailed information on wire and check transactions.	Multiple significant wire transfers among charities with bank accounts in various jurisdictions; final withdrawal of cash transferred to terrorist organization. No obvious legitimate connection.	ST: Yes. ML: Layering, integration. PC: No.
2	General description only.	Single significant wire transfer from a personal bank account in the US to a personal bank account in Canada. No obvious legitimate connection.	ST: Yes. ML: Placement, layering. PC: Yes.
3	No description.	Unknown.	Unknown.
4	General description only.	Cash deposits to personal bank account followed by a series of small denominated checks paid to a business unrelated to the payor. No obvious legitimate connection.	Yes. ML: Placement, layering, possible integration. PC: No.

Case #	Data Available	Type of Transaction(s)	Suspicious Transaction(s) [ST]? If yes, type Proceeds of crime [PC]?
5	General description only.	Large wire transfers from personal accounts in one jurisdiction to multiple accounts in another. No obvious legitimate connection.	Yes. ML: Placement, layering and/or unlicensed MSB. PC: No.
6	Detailed information on wire and check transactions.	Wire and check transfers from company account controlled by one person in one jurisdiction to a personal account controlled by the same person in another jurisdiction.	ST: No. PC No.
7	General description only.	Significant cash deposits and wire transfers from various personal accounts to a single person's account, followed by transfers to a charity in another jurisdiction, followed by further transfers to multiple accounts in other jurisdictions. No obvious legitimate connection.	ST: Yes. ML: Placement, layering, possible integration, and/or unlicensed MSB. PC: No.
8	General description only.	Wire or check transactions from one charity to numerous accounts of unknown control, receipt of a very large amount from a foreign account of unknown control to a charity. No obvious legitimate connection.	ST: Yes. ML: Possible placement (depending on nature of deposits), layering. PC: Diversion of charitable donations.
9	General description only.	Significant cross border wire transaction from company in one jurisdiction with possible ownership/control held by possible terrorists to numerous accounts in other jurisdictions of unknown control. No obvious legitimate connection.	ST: Yes. ML: Possible placement (depending on nature of deposits), layering. PC: No.

Case #	Data Available	Type of Transaction(s)	Suspicious Transaction(s) [ST]? If yes, type Proceeds of crime [PC]?
10	Sale of stolen telephone cards.	Unknown.	ST: Unknown. PC: Yes.
11	General description only.	Cash deposits, large international wire transfers from personal bank accounts under false name to money transfer companies with unknown account names/owner or controller. No obvious legitimate connection.	ST: Yes. ML: Placement, layering, and/or unlicensed MSB. PC: Yes.
12	General description only.	Large number of cash deposits under different business names at various banks to a single account at one business with no obvious business connection, large wire transfers from that business to different bank accounts in other jurisdictions. No obvious legitimate connection.	ST: Yes. ML: Placement, layering, and/or unlicensed MSB. PC: No.
13	General description only.	Numerous deposits made to various individual accounts, then transferred to single accounts in different jurisdiction, then checks paid to individuals in a third jurisdiction. No obvious legitimate connection.	ST: Yes. ML: Placement, layering, possible integration. PC: Diversion of charitable donations.
14	Detailed information.	Small amounts sent via wire transfers from a bank account in one jurisdiction to various individual bank accounts in another jurisdiction. No obvious legitimate connection.	ST: No.

Case #	Data Available	Type of Transaction(s)	Suspicious Transaction(s) [ST]? If yes, type Proceeds of crime [PC]?
15	Some detailed information on wire and check transactions, some actual transaction records.	Large international wire transfers from various charitable and personal accounts in one jurisdiction to personal accounts in another jurisdiction (some in the name of the same individual) in another jurisdiction. No obvious legitimate connection in all cases.	ST: Yes. ML: Layering, possible integration. PC: Diversion of charitable donations.
16	General description only.	Small MSB wire transfers by a person in one jurisdiction to a person in another jurisdiction.	ST: No. PC: No.
17	General description only.	Large bank transfers from accounts in one jurisdiction to multiple accounts held by one person at multiple banks in another jurisdiction. Large numbers of transfers from one personal bank account in that jurisdiction to many different recipient accounts in the same jurisdiction. No obvious legitimate connection.	ST: Yes. ML: Layering, possible integration. PC: Unclear.
18	General description only.	Direct bank transfers from a charity in one jurisdiction to two charities in another jurisdiction.	ST: No. PC: Diversion of charitable donations.
19	Detailed information.	Large transfers from a number of individual bank accounts in one country to a number of individual bank accounts in other countries. No obvious legitimate connection.	ST: Yes. ML: Placement, layering. PC: Yes.

Case #	Data Available	Type of Transaction(s)	Suspicious Transaction(s) [ST]? If yes, type Proceeds of crime [PC]?
20	General description only.	Wire transfers from personal accounts in one jurisdiction to the personal accounts of the same individual in other jurisdictions. Large wire transfers from one personal account in the US to the personal account of an unconnected individual in another jurisdiction. No obvious legitimate connection?	ST: Possible. ML: Large transfers to unrelated person may not fit client profile raising suspicion of layering. PC: No.
21	No description.	Unknown.	ST: Unknown. No.
22	Some detailed information.	Large wire transfers from company account in one jurisdiction to account in another. Because a sting operation, unknown if recipient account was profiled by bank.	ST: Unknown. PC: Presumed no.
23	General description only.	Size and origin of MSB wire transfers unknown.	ST: Unknown. PC: Yes.
24	Court documents provide detailed information on wire and check transactions including payment records.	Small deposits to charity bank account in one jurisdiction, wire transfers to large number of unrelated individual bank accounts in another jurisdiction, then wire transfers to large number of unrelated individual bank accounts in various additional jurisdictions, then cash withdrawn. No obvious legitimate connection.	ST: Yes. ML: Layering, integration. PC: No.
25	General description only.	Deposits.	ST: No.

Case #	Data Available	Type of Transaction(s)	Suspicious Transaction(s) [ST]? If yes, type Proceeds of crime [PC]?
26	General description only.	Cross border payments of unknown type, single small cross border wire transfer.	ST: Unknown.
27	General description only.	Small number of small MSB wire transfers from one jurisdiction to several individuals in multiple jurisdictions.	ST: No. ST: No.
28	General description only.	Fraudulent credit card application, credit card payments.	ST: No. PC: Yes.
29	General description only.	Debit card payments to a designated terrorist organization and to high-tech military equipment companies; medium sized cross-border wire transfer to an unknown person.	ST: Possible. TF: Repeat purchases from military equipment store? PC: No.
30	General description only.	Medium-sized cross border wire transfer.	ST: No. PC: No.

ANNEX: TTERRORISM INDICATORS

Definitions

Placement: is the first stage of the money laundering process, and is used to "introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement."[1] This can be accomplished by depositing cash into a bank account. The exchange of one currency into another, as well as the conversion of smaller notes into larger denominations may occur at this stage. Furthermore, illegal funds may be converted into financial instruments, such as money orders or checks, and commingled with legitimate funds to divert suspicion. Furthermore, placement may be accomplished by the cash purchase of a security or a form of an insurance contract.[2]

Layering: is the second stage of the money laundering process, moving funds through the financial system to "create confusion and complicate the paper trail."[3] The second money laundering stage occurs after the ill-gotten gains have entered the financial system, at which point the funds, securities or insurance contracts are converted or moved to other institutions, further separating them from their criminal source. Such funds could then be used to purchase other securities, insurance contracts or other easily transferable investment instruments and then sold through yet another institution. The funds could also be transferred by any form of negotiable instrument such as check, money order, bearer bond, or the funds can be transferred electronically to other accounts in various jurisdictions. The launderer may also disguise the transfer as a payment for goods or services or transfer the funds to a shell corporation.[4]

Integration: is the "ultimate goal of the money laundering process." Following the layering stage, "the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds."[5]

---

[1] FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL 12 (April 2010), hereinafter BSA/AML MANUAL.

[2] Paul Allan Schott, REFERENCE GUIDE TO ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM: SECOND EDITION AND SUPPLEMENT ON SPECIAL RECOMMENDATIONS I-7 (2006), hereinafter Schott, REFERENCE GUIDE, *available at* http://www.Reference_Guide_AMLCFT_2ndSupplement.pdf.

[3] BSA/AML MANUAL, *supra* note 1 at 12.

[4] Schott, REFERENCE GUIDE, *supra* note 2 at I-8.

[5] BSA/AML MANUAL, *supra* note 1 at 12.

Smurfing: is a strategy commonly employed by money launderers in the placement and layering stages, where large amounts of cash are broken into smaller, less conspicuous amounts that are below the country's reporting threshold and deposited over time in different offices of a single financial institution or in multiple financial institutions.[6]

Cases[7]

1. Abdulrahman Alamoudi.

The Holy Land Foundation for Relief and Development ("HLF") was a non-profit corporation organized in 1989, with its headquarters in Richardson, Texas.[8] It was originally incorporated under the name Occupied Land Fund, and changed its corporate name to Holy Land Foundation for Relief and Development in 1991. HLF was designated a Specially Designated Global Terrorist Entity ("SDGT") in 2001 for funding Hamas. The Success Foundation was a US-registered charity with bank account in Bank of America. The Happy Hearts Trust was an Isle of Man trust with bank accounts at Bank Mercantile in Um-El-Fahem, Israel, and Harbisons Bank, UK. The Humanitarian Relief Association ("HRA"), with a bank account at Bank Mercantile, Humanitarian Appeal International ("HAI"), a corporation located in Onex, Switzerland, with a bank account at Harbisons Bank.[9]

Alamoudi had signature rights at Success, Happy Hearts, HRA, and HAI. Wire transfers and check payments were made among HLF, Success, Happy

---

[6] Schott, REFERENCE GUIDE, *supra note* 2 at VI-25.

[7] Case documents are on file with the author.

[8] Terrorist financing often involves the "improper use of charitable or relief funds." BSA/AML MANUAL, *supra* note 1 at 13. FinCEN has identified the "use of unfamiliar charity/relief organization[s] as a link in transactions" and "wire transfer activities to and from multiple relief and/or charitable organizations, domestic and foreign" as indicators of terrorism finance and money laundering. John J. Byrne & David M. Vogt, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, August 2002, pg. 20, *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_04.pdf. As noted in the BSA/AML Examination Manual, "[b]ecause NGOs can be used to obtain funds for charitable organizations, the flow of funds both into and out of the NGO can be complex, making them susceptible to abuse by money launderers and terrorists. BSA/AML MANUAL, *supra* note 1 at 320. Furthermore, FATF recognizes that charities are particularly susceptible to terrorism financiers because: (1) "they enjoy the public trust"; (2) they "have access to considerable sources of funds"; (3) "their activities are often cash-intensive"; (4) they often "have a global presence"; (5) they are "often in or near areas most exposed to terrorist activity"; and (6) they are "subject to significantly lighter regulatory requirements than financial institutions or publicly-held corporate entities." FATF, *Terrorist Financing*, Feb. 2008, pg 11, *available at* http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf. As such, the *Special Recommendations* require countries to implement laws and regulations designed to prevent non-profit organizations from being used by terrorist financiers. Schott, REFERENCE GUIDE, *supra* note 2 at IX-12.

[9] *Id.*

Hearts, HRA, and HAI finally to Association Secours Palestinian, a foundation located in Basel, Switzerland and with a bank account there.[10] Cash was finally distributed to Hamas, also a SDGT.[1112] *See also* Holy Land Foundation and Benevolence International Foundation cases below.

Data: Court documents provide detailed information on wire and check transactions among these organizations. Actual payment records were not available as they were not themselves admitted as evidence.

Type of Transaction(s): Multiple wire transfers among charities with bank accounts in various jurisdictions, with final withdrawal of cash transferred to terrorist organization.[13] Ownership, control etc. of each charity is not immediately obvious.[14]

Suspicious Transaction(s)? Type: Yes. Layering, integration.

Proceeds of Crime? No.

2. Abdul Tawala Ibn Ali Alishtari (aka Michael Mixon)

Ali Alishtari ("Alishtari") was the administrator of a loan investment program. Alishtari was under FBI surveillance which used a sting operation. He secretly tried to send $152,000 stolen through fraud from the investment program to the Middle East to buy equipment such as night vision goggles for a terrorist training camp in Afghanistan.[1516] As part of this he wire-transferred about

---

[10] Layering.
[11] Integration.
[12] Wire transfers among shell companies can be indicative of money laundering transactions. As noted by FinCEN, "[many] suspicious wire transfer patterns involve shell companies—i.e., corporations that engage in no apparent business activity and that only serve as a conduit for funds or securities. Often, the activities also involve foreign transactors located in jurisdictions considered non-compliant or problematic." John J. Byrne & David M. Vogt, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, October 2000, pp 11-12 *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_01.pdf. For a list of risk factors that make transactions among shell companies suspicious and indicate money laundering, *see* BSA/AML MANUAL, *supra* note 1 at F-7. *See also* John J. Byrne & David K. Gilles, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, August 2004, pg. 3-9, *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_07.pdf (discussing shell corporations and potential indicators of possible shell corporation and shell bank misuse).
[13] See supra text accompanying note 7.
[14] See supra text accompanying note 11.
[15] Placement.
[16] FinCEN notes that "[t]errorist organizations [may] use alternative and less obvious means to acquire and move capital. Those means may involve committing crimes that, in the past, were not immediately associated with terrorist fundraising and financing schemes." John J. Byrne & David K. Gilles, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, August 2004, pg. 3, *available*

$25,000 from his personal bank account in New York to a personal bank account in Montreal, Canada, where he believed the money would be transferred to Afghanistan.[17] Alishtari plead guilty in September, 2009 to material support. However, because of the plea agreement, no direct evidence regarding the transfers was admitted.

Data: Court documents describe payment forms only in generalities.

Type of Transaction(s): Single significant wire transfer from a personal bank account in the US to a personal bank account in Canada.[18]

Suspicious Transaction(s)? Type: Yes. Placement, layering.

Proceeds of Crime? Yes.

3. Amawi, El-Hindi, and Mazloum.

Beginning in June 2004, Mohammed Zaki Amawi, Marwan El-Hindi and Wassim Mazloum allegedly engaged in a conspiracy to kill or maim persons outside the United States, including U.S. armed forces personnel in Iraq, and to kill then President George Bush. The three defendants allegedly provided material support, including money, training, communications equipment, computers and

---

at http://www.fincen.gov/news_room/rp/files/sar_tti_07.pdf. Suspicious activity reporting has uncovered similar investment fraud schemes in the U.S. *See* John J. Byrne & David M. Vogt, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, October 2000, pg. 16, *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_01.pdf; John J. Byrne & David K. Gilles, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, November 2003, pg. 46, *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_06.pdf.

[17] Layering.

[18] Moving money by wire transfer is a "primary technique for moving terrorist funds." FATF, Money Laundering & Terrorist Financing Threat Assessment, July 2010, pg 24, *available at* http://www.fatf-gafi.org/dataoecd/48/10/45724350.pdf. Indeed, wire transfers are one of the top three activities described in U.S. Suspicious Activity Reports filed as a result of a name match with a government terror list. John J. Byrne & David M. Vogt, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, August 2002, pg. 26, *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_04.pdf. For a list of risk factors that make fund transfers suspicious and indicate money laundering, see Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual, April 2010, pp. F-2-3, F-10. *See also* John J. Byrne & David K. Gilles, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, April 2005, pg. 25, *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_08.pdf (reporting the discovery of terrorism finance where Defendants engaged in a series of overseas financial transactions, but funneling all money through a U.S. branch of a bank headquartered in the Middle East). Terrorism-related wire activity is often to and from Middle Eastern countries. John J. Byrne & David M. Vogt, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, February 2003, pg. 22, *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_05.pdf.

personnel, including themselves, to unnamed co-conspirators in the Middle East, knowing that the materials would be used in waging violent jihad against the U.S. military and Coalition forces in Iraq and elsewhere. The object of the conspiracy was allegedly to obtain funds from the LITC federal grant program through ESFS, a Toledo-based non-profit charitable organization, to divert the grant funds.[19] On Feb. 19, the Treasury Department ordered U.S. banks to freeze the assets of ESFS; other items seized by federal agents during the arrests included bank accounts.

In September 2008 the defendants were convicted. No documents concerning financial transactions were introduced into evidence.

Data: Court documents do not describe payment forms.

Type of Transaction(s): Unknown.

Suspicious Transaction(s)? Type: Unknown.

4. Yassin Muhiddin Aref and Mohammed Mosharref Hossain.

In 2005, Yassin Muhiddin Aref ("Aref") and Mohammed Mosharref Hossain ("Hossain") were indicted for conspiracy to engage in money laundering and substantive acts of money laundering and material support. They agreed to work with an informant in a scheme to conceal the source of $50,000.[20] The cooperator told the defendants that the money came from the sale of a surface-to-air missile to a designated terrorist group called Jaish-e-Mohammed.

A cooperating witness ("CW") proposed a scheme to provide the $50,000 cash proceeds from the importation of the SAM to Hossain who would, in turn, provide monthly checks written to the CW's business, Hay's Distributors, in the total amount of $45,000.[21] Hossain would keep the remaining $5,000. CW provided cash payments totaling $40,000 in the form of five deliveries between January 2, 2004 and June 9, 2004.[22] Each time, Aref received and counted the cash and then gave it to Hossain. Aref provided receipts to the CW for the cash. Hossain deposited the amounts to his personal bank account. He then wrote checks ten checks made payable to Hay's Distributors between January 2, 2004 and August 3, 2004.[23]

---

[19] *See supra* text accompanying note 7.

[20] Money Laundering can be "The conversion or transfer of property, knowing that such property is derived from any [drug trafficking] offense or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;" Schott, REFERENCE GUIDE, *supra note* 2 at 21.

[21] *See supra* text accompanying note 15.

[22] Placement; Smurfing.

[23] Layering; Smurfing

Defendants were charged with conspiracy and attempt to commit money laundering and to provide material support to a designated terrorist organization. The Government alleged that the defendants agreed to work with a cooperator in a scheme to conceal the source of $50,000. The cooperator told the defendants that the money came from the sale of a surface-to-air missile to a designated terrorist group called Jaish-e-Mohammed. The missile was to be fired at a target in New York City. In 2007 Hossain was convicted on all twenty-seven counts against him. Aref was convicted on ten counts and acquitted on the others. While prosecutors have agreed to provide documentation on payments they have yet to do so.

Data: Court documents describe transactions only in generalities. Additional documents expected.

Type of Transaction(s): Significant number of cash deposits to personal bank account followed by a series of small denominated checks paid to a business unrelated to the payor.

Suspicious Transaction(s)? Type: Yes. Placement, layering, possible integration.

Proceeds of Crime? No.

5. Mohammad Anvari-Hamedani.

According to prosecutors Anvari-Hamedani was a hawaladar who engaged in a series of transactions involving wire transfers of approximately $4 million in funds and equipment to Iran, using his account at Merril Lynch in the United States, to intermediary banks Great Britain, Hong Kong, and then to the United Arab Emirates then to Iran.[24][25] He pleaded guilty in 2006 for operating an unlicensed money service business.[26] Details on payments were not admitted as evidence.

---

[24] *See supra* text accompanying note 17.

[25] *See supra* text accompanying note 11.

[26] With limited exceptions, many MSBs are subject to the full range of BSA regulatory requirements, including the anti-money laundering program rule, suspicious activity and currency transaction reporting rules, and various other identification and recordkeeping rules.253 Existing FinCEN regulations require certain MSBs to register with FinCEN.254 Finally, many states have established supervisory requirements, often including the requirement that an MSB be licensed with the state(s) in which it is incorporated or does business. BSA/AML MANUAL, *supra* note 1 at 309. FinCEN notes that "Personal accounts used as "layering" points involving wire transfers sent into those accounts from unregistered and/or unlicensed MSBs and then transferred abroad". Indeed, it also mentions "a subject engaged in the suspected operation of an unlicensed MSB conducting numerous outgoing wire transmissions out of his personal account". *See* John J. Byrne

Data: Court documents describe payment forms only in generalities.[27]

Type of Transaction(s): Large wire transfers from personal accounts in one jurisdiction to multiple accounts in another.

Suspicious Transaction(s)? Type: Yes. Placement, layering and/or unlicensed MSB.

Proceeds of Crime? No.

6. Khalid Awan

In May 2004, Khalid Awan ("Awan") was being held at the Metropolitan Detention Center in Brooklyn, New York, where he encountered Harjit Singh ("Singh"), another inmate who was awaiting sentencing, who became a cooperating witness. During their conversations, Awan told Singh that he knew a Pakistani terrorist named Paramjit Singh Panjwar leader of the Khalistan Commando Force ("KCF"), a Sikh terrorist organization which had conducted violent attacks against people and property in India. Awan assisted in transferring his own money and assisting others in transferring money to the KCF. Awan accomplished this in part by wire transferring/sending checks from the Tee Jay's Fashion account in moderate amounts at HSBC bank, controlled by his friend Mr. Butt, to an account controlled by Mr. Butt at Habib Bank in Pakistan.[28] Prosecutors provided details of these transactions as well as additional evidence in the form of recorded conversations but actual payment records were not available as they were not themselves admitted as evidence.

Data: Court documents providing detailed information on wire and check transactions among these organizations. Actual payment records were not available as they were not themselves admitted as evidence.

& David K. Gilles, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, November 2003, pg. 7&8, *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_06.pdf.

[27] Reports indicating excessive outbound wire activity were common in Suspicious Activity Reports filed by the securities and futures industries. Preliminary indicators are that individuals who engage in this activity within one year of establishing a brokerage account were more likely to send funds outside of the U.S. John J. Byrne & David K. Gilles, FinCEN, *The SAR Activity Review: Trends, Tips & Issues*, October, 2005, pg. 14 *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_09.pdf. *See also id.* at 37 (defendants deposited drug proceeds into more than 50 bank accounts in the name of front companies, and then transferred the funds to various countries).

[28] *See supra* text accompanying note 17.

Type of Transaction(s): Wire and check transfers from company account controlled by one person in one jurisdiction to a personal account controlled by the same person in another jurisdiction. Could be distribution of profits.

Suspicious Transaction(s)? Type: No.

Proceeds of Crime? No.

7. Al-Barakat, Abdirahman Isse and Abdillah Abdi.

Abdirahman Isse ("Isse") and Abdillah Abdi ("Abdi") received cash funds from customers; they deposited the funds in multiple accounts of businesses controlled by them at various branches of banks in Northern Virginia. To avoid the $10,000 threshold for reporting transactions, they always deposited the amounts with the banks in sums of less than $10,000, usually between $9,000 and $9,990, and on some days, they made several such deposits.[29][30] Because the deposits were in cash amounts less than $10,000, they did not prompt the banks to file currency transaction reports. Isse and Abdi then wired the funds from the bank accounts to the Al-Barakat headquarters in the United Arab Emirates, a registered charity.[31][32] Following this, transfers were made from the account to personal and other bank accounts in Somalia, Ethiopia, Kenya, and Sudan.[33] As compensation for each transmission of funds for a customer, the defendants generally retained 1% of the deposit and remitted another 3% to Al-Barakat, of which Al-Barakat kept two-thirds (2% of the total deposit) and remitted the remaining one-third (1% of the total deposit) to the agent in the receiving country.[34] Mohammad Hussein was involved in similar activity in Al-Barakat's Boston operations. Isse and Abdi pled guilty to structuring in 2003. No detailed transaction records were offered as evidence.

Data: Court documents provide only general description. Proceeds of Crime? No.

Type of Transaction(s): Significant cash deposits and wire transfers from various personal accounts to a single person's account, followed by transfers to a charity

[29] Placement.
[30] Smurfing.
[31] Layering; see supra text accompanying note 17.
[32] See supra text accompanying note 7.
[33] Layering.
[34] Possible integration.

in another jurisdiction, followed by further transfers to multiple accounts in other jurisdictions.

Suspicious Transaction(s)? Type: Yes. Placement, layering, possible integration, and/or an MSB.

8. Benevolence International Foundation, Enaam Arnaout

The Benevolence International Foundation ("BIF") claimed to be a nonprofit, religious, humanitarian, charitable organization funded by donations from individuals, businesses, and other Islamic organizations and dedicated to assisting individuals afflicted by war, natural disaster, and extreme poverty.[35][36] Also according to BIF, since 1992, it had administered essential humanitarian aid to the poor in needy areas of the world, by distributing food, clothing, and medical services in places such as Afghanistan, Bosnia, China, and Pakistan, and by operating hospitals, medical and dental clinics, and orphanages in places such as Tajikistan, Azerbaijan, Daghestan, and Ingushetia, using payments to accounts of foreign branch offices. BIF, was an Illinois corporation with offices in Illinois and New Jersey and approximately ten offices overseas. Allegedly Enaam Arnaout ("Arnaout"), who in 1993 assumed formal management of BIF, had secretly (i.e. concealed from many donors to BIF) used a portion of the money raised by BIF to support Mujahideen, including al-Qaeda, engaged in armed confrontations and violence overseas, such as in Chechnya and Bosnia-Herzegovina. Arnaout allegedly transferred funds from BIF's checking accounts in Illinois to various bank accounts in New Jersey and outside the United States, although the owner/controller of those bank accounts was not revealed. Also, an unknown person's account at the Union Bank of Switzerland wire transferred $1,414,406 to BIF's checking account in the United States. Those funds were commingled in BIF's checking account with donations that BIF received from other sources and disbursed in large part to the BIF offices overseas.

On December 14, 2001 U.S. Treasury blocked all BIF assets. FBI searched the Chicago offices of BIF and Arnaout's home, seizing from both places items such as financial records, office equipment, and personal property. Charges included conspiracy to engage in financial transactions involving proceeds of unlawful activities, namely mail fraud and wire fraud, with the intent to promote those crimes, as well as to provide material support to organizations

[35] Because NGOs can be used to obtain funds for charitable organizations, the flow of funds both into and out of the NGO can be complex, making them susceptible to abuse by money launderers and terrorists. BSA/AML MANUAL, *supra* note 1 at 320.
[36] *See supra* text accompanying note 7.

involved in violent activities; and to transfer funds from within the United States to outside the United States with intent to give material support to organizations engaged in violent activities.[3738] In 2003 Enaam Arnaout pled guilty to racketeering only. Evidence concerning transactions was not introduced.

Data: Court documents provide only general description of payment transactions. Proceeds of Crime?

Type of Transaction(s): Wire or check transactions from one charity to numerous accounts of unknown control, receipt of a very large amount from a foreign account of unknown control to a charity.[39]

Suspicious Transaction(s)? Type: Yes. Possible placement, layering.

Proceeds of Crime? Diversion of charitable donations.

9. BMI/Mostan, Soliman Bihieri, Mousa Mohammad Abu Marzook, Ghaleb Himmat and Youssef Nada

In 1985, BMI was incorporated in New Jersey. The articles of incorporation of BMI listed Soliman S. Biheiri ("Biheiri"), an Egyptian convicted of immigration violations, as an incorporator and as BMI's President. In 1988, Mostan International Corporation ("Mostan") was incorporated in New Jersey. Bihieri was an incorporator and Vice President and was Mostan's registered agent and Director. Mousa Mohammad Abu Marzook ("Marzook"), the self-proclaimed political leader of Hamas and an SDGT in Novermber 1, 2001, was its president. Mostan was established to generate funds for Marzook/Hamas. Marzook was its sole shareholder.

Mostan had an account at the Bank of New York. The bank records for Mostan showed large wire transfers to overseas accounts.[40] Biheiri's computer was searched and found to have contact information for Ghaleb Himmat and Youssef Nada.

BMI reported more than $25,000,000 in projected revenues and leases as early as 1992 in a business that solicited real-estate investments and offered leasing services for Muslims in what was alleged to be a scheme based in Virginia and Maryland to raise cash for terrorists.[41]

---

[37] *See supra* text accompanying note 15.
[38] *See supra* text accompanying note 17.
[39] *Id*.
[40] *See supra* text accompanying note 17.
[41] *See supra* text accompanying note 15.

BMI's investors included Abu Marzook, who was an investor in an Oxon Hill real-estate development known as Barnaby Knolls which was financed through a BMI subsidiary, BMI Real Estate Development Inc., and involved the construction of 57 homes, beginning in January 1991; Yasin Qadi ("Qadi"), a Saudi multimillionaire involved in banking, chemicals, diamonds and real estate, who was designated by the Treasury Department in 2002 as a terrorist and is suspected of diverting millions of dollars to Osama bin Laden's al-Qaeda network. Authorities alleged that Qadi led the Saudi-based Muwafaq (Blessed Relief) Foundation, which the U.S. Treasury Department said was used as a front for al-Qaeda to launder millions of dollars to the terrorist organization. Yousef Nada, an Egyptian national and resident of Switzerland, who was designated a terrorist financier by the U.S. and U.N. in November 2001. U.S. law-enforcement authorities suspected that Nada provided significant funding to al-Qaeda; Nada is a founder of Al-Taqwa Bank, which was alleged to be at the center of a financial network that helped fund global terrorism. The U.S. Treasury Department designated the bank an SDGT shortly after the September 11, 2001, attacks.

Bihieri was found guilty in 2004 of making false statements. Marzook was indicted for various terrorism related crimes and money laundering in absentia in 2003.

In 2006 Nada sued the Swiss government because of financial losses incurred resulting from the three-and-a-half year investigation. "It was all wrong," Nada, the 75-year-old founder and former managing director of Nada Management, formerly known as al-Taqwa, said at his home in Italy near the Swiss border. "Switzerland was mistaken and misled." In 2005 the Swiss authorities dropped their investigation. But Switzerland was forced to drop the case against top officials of the company on July 1, 2005 because they said authorities in the Bahamas had failed to provide essential bank records by a court deadline.

Data: Court documents provide only general information on payment transactions, including the "significant wire transfers overseas" from BMI. Details on transactions are expected from prosecutors.

Type of Transaction(s): Significant cross border wire transaction from company in one jurisdiction with possible ownership/control held by possible terrorists to numerous accounts in other jurisdictions of unknown control.[42][43]

[42] Cross-border transfers need to be accompanied by the name, account number (or unique reference number where there is no account e.g. one-off transactions), and address. An identity number or customer identification number or date and place of birth can be substituted for the address if there are fears about revealing the address of a customer. Providing this information on the wire transfer will enable information about the sender to be obtained much more quickly and easily if there is an international money laundering or terrorist financing investigation than if it has to be the subject of lengthy inquiries. Paul A. Schott. The World Bank. *Reference Guide to Anti-*

Suspicious Transaction(s)? Type: Yes. Possible placement (depending on nature of deposits), layering. Possible terrorism financing due the terrorist-related ownership/control of payor.[44]

Proceeds of Crime? No.

10. The Detroit Sleeper Cell Case, Karim Koubriti, Ahmed Hannan, Farouk Ali-Hammoud and Abdel-Ilah Elmardoudi

This is a troublesome case, with allegations of material support and fraud followed by allegations of prosecutorial misconduct. Karim Koubriti ("Koubriti") was found guilty of providing material support to a terrorist group and Ahmed Hannan ("Hannan") had been found guilty of identification forgery, but these convictions were overturned in 2004 when the lead prosecutor and star witness were accused of mishandling evidence and providing false testimony, respectively. Koubriti and Hannqn were found guilty of mail fraud, insurance fraud and material support of terrorism in connection with his 'economic jihad' scheme to defraud an insurance firm.

Exactly how these funds were used to support terrorism, and through what financing means, is not clear from available court documents. Abdel-Ilah Elmardoudi was convicted for operating a phone card "shoulder surfing" scheme in which he stole hundreds of telephone calling-card numbers from unsuspecting travelers at the Minneapolis-St. Paul International Airport and then "supplied them to overseas callers who used them" to make a total of $745,000 in international calls from Egypt, Kuwait, East Africa, the Philippines, the Middle East, and the Balkans.

The lead prosecutor was dismissed from this case for prosecutorial misconduct and later prosecuted. After speaking with his attorney and attempting to negotiate a discussion he decided not to discuss the case. So far, we have been unable to locate anyone at Department of Justice who is willing to discuss the case.

Data: Court documents provide no description.

Type of Transaction(s): Unknown.

Money Laundering and Combating Terrorist Financing, 2006, at 175 *available at* http://www.Reference_Guide_AMLCFT_2ndSupplement.pdf.

[43] *See supra* text accompanying note 11.

[44] *See supra* text accompanying note 17.

Suspicious Transaction(s)? Type: Unknown.

Proceeds of Crime? Yes.

11. Hossein Esfahani.

According to allegations Hossein Esfahani ("Esfahani") was a hawaladar who transmitted funds to and from Iran by means of wire transfers through intermediary money exchanges in Dubai via Harris Bank to Dubai from October 31, 2001 through February 14, 2005, in breach of financial sanctions against Iran.[45] Using the false name "Ahmad Khalij," Esfahani set up various shell bank accounts in the U.S.[46] Deposits ranged from just $200 to $150,000, much of which was proceeds of drug crime.[47] The majority of the nearly $4,000,000 sent to Iran was wired to three Dubai money transfer companies, and, from there to Shiraz, Iran.[48] In the remaining cases he "used hawala to send cash to Iran." While terrorism financing is not directly alleged it seems clear that Esfahani was trying to evade detection, so similar issues arise.

In 2006 Esfahani pled guilty to operating an unlicensed MSB and to breaching sanctions against Iran. We have contacted prosecutors to see what if any evidence on transactions was admitted to trial but they have not responded to repeated requests.

Data: Court documents provide only general descriptions of payment types. Because Esfahani pled guilty it may be that no details were admitted into evidence.

Type of Transaction(s): Cash deposits, large international wire transfers from personal bank accounts under false name to money transfer companies with unknown account names/owner or controller.

Suspicious Transaction(s)? Type: Yes. Placement, layering, and/or unlicensed MSB.

Proceeds of Crime? Yes.

12. Abad Elfgeeh.

Abad Elfgeeh ("Elfgeeh") was a hawaladar who maintained an account for Carnival French Ice Cream ("Carnival") at J.P. Morgan Chase, as well 12 feeder

---

[45] *See supra* text accompanying note 17.
[46] *See supra* text accompanying note 11.
[47] Placement; Possible smurfing; See supra text accompanying note 19.
[48] Layering.

accounts at Chase and other banks in the names of various physical persons and businesses.[49] Large totals of money was deposited into the Carnival account in small amounts as transfers from the feeder accounts and large sums of money was wired out of the Carnival account to accounts in 25 foreign countries, although the names of the receiving accounts are not noted.[50] For example, in a one-month period during the fall of 2000, more than $245,000 was deposited into the Carnival account and more than $268,000 was wired out. Between 1996 and 2003, the total amount deposited into the Carnival account was $22,190,642.21, and the total amount withdrawn was $ 21,995,556.54. Another Chase bank account in the name of the Prospect Deli that was opened by Aref and listed the home address and telephone number of Elfgeeh, which was the same account-opening information used for another feeder account at Astoria Federal Bank. The Prospect Deli was a business a few blocks away from the Carnival French Ice Cream shop; the Prospect Deli was in operation only from 1996 to 1998, but activity in the Prospect Deli bank account continued until 2002.[51] For example, bank records showed that in 2001 approximately $850,000 was deposited into the Prospect Deli account and about $ 823,000 was transferred out to the Carnival account.

Evidence showed Elfgeeh's money transfers were tied to Sheikh Mohammed Ali Hassan al-Moayad, who was sentenced to 75 years in a U.S. prison and fined $1,250,000 for conspiring to support and fund al-Qaeda and Hamas. Elfgeeh was convicted in 2006 of running an unlicensed MSB. Repeated requests for assistance from prosecutors to help identify if any payments records were admitted as evidence have been unsuccessful.

Data: Court documents provide only general descriptions of payment types. Because Esfahani pled guilty it may be that no details were admitted into evidence.

Type of Transaction(s): Large number of cash deposits under different business names at various banks to a single account at one business with no obvious business connection, large wire transfers from that business to different bank accounts in other jurisdictions.

Suspicious Transaction(s)? Type: Yes. Placement, layering, and/or unlicensed MSB.

Proceeds of Crime? No.

---

[49] *See supra* text accompanying note 11.
[50] Placement; Layering; Smurfing; See supra text accompanying note 17.
[51] Shell company, *see supra* text accompanying note 11.

13. Help the Needy, Rafil Dhafir, Maher Zagha, Ayman Jarwan, and Osameh Al-Wahaidy

Rafil Dhafir ("Dhafir"), Maher Zagha ("Zagha"), Ayman Jarwan ("Jarwan"), and Osameh Al-Wahaidy ("Al-Wahaidy") and the two unregistered charities, Help the Needy and Help the Needy Endowment, Inc., allegedly solicited contributions from people in the United States, deposited these funds in accounts in their own names at Oneida Savings Bank and Key Bank in New York in accounts opened and controlled by Dhafir, Jarwan, and Al-Wahaidy.[52] Payments were then made to accounts in the name of Zagha held at Fleet Bank, then paid to another account in Zagha's name at the Jordan Islamic Bank in Amman.[53] One or more banks filed a suspicious activity report although the details of the report were not identified. From there, checks as large as $ 100,000 were paid to individuals Iraq in breach of sanctions.[54] After Zagha's Key Bank account was closed, transfers were made directly from HTN's accounts to Zagha's account in Jordan.[55] Over $2.7 million was moved through accounts at the Jordan Islamic Bank.

Dhafir was convicted in 2005 of various charges. The others pled guilty in 2003. Researchers have contacted prosecutors to see if documents regarding payments were admitted as evidence but they have yet to respond.

Data: Court documents provide only general descriptions of payment types.

Type of Transaction(s): Numerous deposits made to various individual accounts, then transferred to single accounts in different jurisdiction, then checks paid to individuals in a third jurisdiction.

Suspicious Transaction(s)? Type: Yes. Placement, layering, possible integration.

Proceeds of Crime? Diversion of charitable contributions.

14. Rahmat Abd Hir, Zulkifli Abd Hir Zulkifli

Rahmat Abd Hir's ("Abd Hir") brother is Zulkifli Abd Hir Zulkifli ("Zulkifli"), an acknowledged member of the Moro Islamic Liberation Front and an alleged high-ranking member of Jemaah Islamiyah in the Philippines. Abd Hir consistently responded to Zulkifli's requests for money and supplies by wiring

[52] Placement; Charities, see *supra* text accompanying note 7.
[53] Layering.
[54] Possible integration.
[55] Layering.

over $10,000 to his brother using various bank accounts in the Philippines. Prosecutors provided detailed information on the wire transfers.

Data: Detailed information on wire transfers.

Type of Transaction(s): Small amounts sent via wire transfers from a bank account in one jurisdiction to various individual bank accounts in another jurisdiction.[56]

Suspicious Transaction(s)? Type: No. Recipient was a suspected terrorist making the case obvious.

Proceeds of Crime? No.

15. Holy Land Foundation, KindHearts, Khaled Smaili, Abu Marzook

See also discussion above at Alamoudi regarding HLF. The Global Relief Foundation ("GRF"), a U.S. charity, was affiliated with HLF and also designated an SGTD.[57] After these designations a former GRF official Khaled Smaili established KindHearts, a U.S. charity, in January 2002 to continue the missions of both HLF and GRF without a designation.[58]

Mousa Mohammed Abu Marzook ("Marzook"), a senior member of Hamas since 1997, served as the Deputy Chairman of Hamas Political Bureau. Marzook provided substantial funds to the HLF in the early 1990s. Between 1992 and1993 Marzook wire transferred from various accounts of the charities and some personal accounts nearly $1,000,000 to Salah's personal bank accounts at LaSalle Bank of Chicago.[5960] After Salah arrived in Israel he arranged to have approximately $230,000 from his personal bank accounts in Chicago transferred to his personal bank accounts in an Israeli bank for distribution to Hamas members. He was then taken into custody there. In April 1993, when Salah remained in custody in Israel, his wife withdrew approximately $536,000 from their joint personal LaSalle Bank account and deposited the amount into another account at Standard Bank and Trust for personal use in paying off a loan.

In 2007 there was a mistrial, but in 2008 HLF and five of its leaders on charges of providing material support to Hamas.

---

[56] Possible smurfing, if the amounts were small to avoid detection.
[57] *See supra* text accompanying note 7.
[58] *Id*.
[59] *See supra* text accompanying note 7.
[60] *See supra* text accompanying note 17.

Data: Court documents provide detailed information on wire and check transactions among these organizations and persons. Many actual payment records (check and wire transactions) are also available.

Type of Transaction(s): Large international wire transfers from various charitable and personal accounts in one jurisdiction to personal accounts in another jurisdiction (some in the name of the same individual) in another jurisdiction.[6162]

Suspicious Transaction(s)? Type: Yes. Layering, possible integration.

Proceeds of Crime? Diversion of charitable donations.

16. Richard David Hupper.

On several occasions during an almost two year period of time, Richard David Hupper ("Hupper") provided money to Hassam Jamjoun ("Jamjoun"), a Hamas figure, in Israel. This money was transferred by cash in person by Hupper and also by way of a Western Union cash wire transfer to Jamjoun in Israel.[6364] Jamjoun was to transfer these funds to Hamas for a variety of things, including assisting the families of Israeli-imprisoned Hamas members. In May of 2008 Hupper pled guilty to one count of providing material support to Hamas. Because of the guilty plea no evidence on the transfers was submitted. However, researchers contacted Hupper's attorney in the hope of persuading Hupper to provide the information himself. While he has so far not agreed to cooperate we hope that he will eventually change his mind.

Data: Court documents provide no information on the transactions. It is hoped that Hupper may provide these documents voluntarily.

Type of Transaction(s): Small MSB wire transfers by a person in one jurisdiction to a person in another jurisdiction.

Suspicious Transaction(s)? Type: No. Recipient of Western Union transfer was a known Hamas figure making the case obvious.

Proceeds of Crime? No.

---

[61] *See supra* text accompanying note 7.
[62] *See supra* text accompanying note 17.
[63] *See supra* text accompanying note 15.
[64] *See supra* text accompanying note 17.

17. Islamic Assembly of North America, Omar Al Hussayen.

According to the indictment, between November 16, 1999 and February 26, 2003, Omar Al Hussayen ("Al Hussayen") was an employee, official, and registered agent of the Islamic Assembly of North America ("IANA"). IANA was a U.S. registered non-profit charitable organization with offices in Ann Arbor, Michigan.[65] As such, he engaged in significant decision-making and business transactions related to the IANA's business, particularly with respect to the creation, maintenance and content of websites and other internet media. He also set up a number of web sites for various jihadi organizations, including Hamas.

Al Hussayen came to the United States from Saudi Arabia to study at the University of Idaho. While there he received a stipend for living expenses from Saudi Arabia. During that same time he maintained at least six United States bank accounts in Indiana, Texas, Idaho and Michigan. From at least January 23, 1997, until February 26, 2003, he received into and disbursed out of these accounts around $300,000 dollars in excess of the stipend he received during the same period.[66] Beginning November 16, 1999 he disbursed funds to and on behalf of IANA and its officers, including its president, to pay various operating expenses, including employee salaries and foreign and domestic IANA-related travel expenses for himself and others. He also disbursed money directly to the president of the IANA via wire transfers and personal checks and maintained a checking account in Michigan in his name alone, but with the president's home address. About $100,000 of the money allegedly came in two installments from the student's uncle, Saleh Abdel Rahman Al-Hussayen.

According to the Justice Department in the spring of 2002, Al-Hussayen became a target of a Foreign FISA surveillance based on suspicious activity reports, which were based on the amount and source of funds received from overseas sources and of donations he made to IANA. Al Hussayen was eventually acquitted of all material support charges, although he was deported for breaching his immigration status. We have made repeated requests of the prosecutors to provide us the evidence, or reference to the evidence, but so far have not succeeded.

Data: Court documents available provide no detailed information on the transactions.

Type of Transaction(s): Large bank transfers from accounts in one jurisdiction to multiple accounts held by one person at multiple banks in another jurisdiction.[67]

---

[65] *See supra* text accompanying note 7.
[66] *See supra* text accompanying note 26.
[67] Layering.

Large numbers of transfers from one personal bank account in that jurisdiction to many different recipient accounts in the same jurisdiction.[68]

Suspicious Transaction(s)? Type: Yes. Layering, possible integration.

Proceeds of Crime? Unclear.

18. Islamic American Relief Agency, Mubarak Hamed, Ali Mohamed Bagegni, Abdel Azim El-Siddig, Ahmad Sultan Mustafa and Khalid Al-Sudanee

In 1985, a Sudanese immigrant founded the Islamic African Relief Agency. It engaged in humanitarian activities around the world, often in partnership with similar organizations. In 2000, Islamic African Relief Agency changed its name to the Islamic American Relief Agency ("IARA"). Meanwhile, the entity in Sudan calling itself the Islamic African Relief Agency continued to exist under that name. On October 13, 2004 the U.S. Office of Foreign Asset Control ("OFAC") designated the Islamic African Relief Agency an SDGT. Although IARA was not independently designated, OFAC considered it to be the United States branch of the Sudanese organization, the decision was unsuccessfully challenged. In 2007 IARA and its employees: Mubarak Hamed, the organization's executive director; Ali Mohamed Bagegni; Abdel Azim El-Siddig; Ahmad Sultan Mustafa and Khalid Al-Sudanee were charged with transferring funds from IARA's bank accounts in the Western District of Missouri, to ISRA's bank accounts in Amman, Jordan. There were a total of 18 transactions ranging from $4,000 to $50,000 made in this manner.[69] In 2008, they were charged with transferring $130,000 in 8 transactions, ranging from $7,000 to $28,000, from March 2003 to August 2004 to the Islamic Relief Agency ("ISRA") bank accounts in Peshawar, Pakistan, purportedly for an orphanage housed in buildings owned and controlled by Specially Designated Global Terrorist Gulbuddin Hekmatyar.[70] In the latter indictment Mark Siljander ("Siljander"), a former U.S. Congressman from Michigan (1981-87) and owner/director of Global Strategies, Inc., was charged with with money laundering, conspiracy and obstruction of justice in the case. To compensate Siljander for his lobbying services to get IARA de-designated, IARA transferred roughly $50,000 in funds to accounts that were controlled by Siljander at the National Heritage Foundation and the International Foundation.

We discussed the cased with prosecutors, but a court protective order prohibits them from providing any substantive information.

---

[68] Layering; possible integration.
[69] Possible smurfing.
[70] Possible smurfing; *see supra* text accompanying note 7.

Data: Court documents available provide no detailed information on the transactions.

Type of Transaction(s): Direct bank transfers from a charity in one jurisdiction to two charities in another jurisdiction.[71]

Suspicious Transaction(s)? Type: No.

Proceeds of Crime? Diversion of charitable donations.

19. Monzer Al Kassar, a/k/a Abu Munawar, a/k/a El Taous, Tareq Mousa Al Ghazi and Luis Felipe Moreno Godoy.

Monzer Al Kassar ("Al-Kassar") became an arms dealer in the early 1970s when the government of Yemen asked him to buy rifles and pistols from Poland for them (it is alleged that those arms were then sent to various terror groups).[72] In the 1970s he was arrested in both Denmark and the UK for selling hashish.[73] In 1984 he was expelled from the UK for drug and arms trafficking; he then moved to Spain.[74] In 1987 investigations into the Iran-Contra scandal found that he had been involved in selling arms to the Contras. In 1992 he made arms sales valued in the millions of dollars to Croatia, Bosnia and Somalia, violating United Nations arms embargoes to all three countries. Up to 2002 he collaborated with Polish Military Information Services in illegal arms trading. 2006, Iraq called him one of the main sources of financial and logistics support for the Iraqi insurgency. In 2007 he was approached by DEA undercover agents posing as operatives of the Revolutionary Armed Forces of Colombia ("FARC") wishing to use drug proceeds to purchase weapons.[75] Al-Kassar provided them with bank accounts of individuals in Spain and Lebanon, which were ultimately were used to receive more than $400,000 in payments through bank transfers from bank accounts of other individuals.[76]

On November 20, 2008, he was convicted of money laundering and conspiring to sell arms to suppliers for FARC. Prosecutors recently have provided researchers with detailed bank records on these transactions.

Data: Court documents provide detailed information on the transactions.

---

[71] *See supra* text accompanying note 7.
[72] *See supra* text accompanying note 19.
[73] *Id.*
[74] *Id.*
[75] *See supra* text accompanying note 19.
[76] Placement and layering.

Type of Transaction(s): Large transfers from a number of individual bank accounts in one country to a number of individual bank accounts in other countries.

Suspicious Transaction(s)? Type: Yes. Placement, layering.

Proceeds of Crime? Yes.

20. Hemant Lakhani.

Hemant Lakhani ("Lakhani") claimed to be able to buy a Stinger missile to be used to shoot down an American plane. An FBI informant named Rehman gave purchase money to Lakhani, told him how to send it along so that it would look "clean" once it got to London. There were two such transfers: Rehman was to give the money to Yehuda Abraham ("Abraham"), a jeweler in Manhattan who also owned a money transfer business.[77] Lakhani told Rehman that he would recognize Abraham upon the presentation of a bill with a specific serial number. Abraham then wire transferred the money from his personal account in the U.S. to his personal bank accounts in Hong Kong and Switzerland. Lakhani then engaged in an effort to purchase a stinger from Ukraine; a U.S./Russian sting operation was put into motion to sell Lakhani a fake missile. At Lakhani's request Matheena Raja, an Indian national and businessman, made wire transfers of a total of $86,000 in two transactions from his personal account in the U.S. to Lakhani's personal account in London to purchase the missile.[78]

Researchers discussed the case with one of the prosecutors who could not recall any financial records being introduced as evidence.

Data: Court documents provide no detailed information.

Type of Transaction(s): Wire transfers from personal accounts in one jurisdiction to the personal accounts of the same individual in other jurisdictions. Large wire transfers from one personal account in the U.S. to the personal account of an unconnected individual in another jurisdiction.

Suspicious Transaction(s)? Type: Possible. Large transfers to unrelated person may not fit client profile.

Proceeds of Crime? No.

---

[77] *See supra* text accompanying note 25.
[78] *See supra* text accompanying note 17.

21. LTTE Procurement Plot, Murugesu Vinayagamoorthy, Nachimuthu Socrates, Thirukumaran Sinnathamby, Thirukumaran Sivasubramaniam, Vijayshanthar Patpanathan, Suresh Sriskandarajah, Ramanan Mylvaganam.

On August 19, 2006 defendants were arrested on Long Island after three of them engaged in negotiations with an undercover FBI agent to purchase and export anti-aircraft missiles and launchers and other military equipment for the Liberation Tigers of Tamil Eelam ("LTTE"). The defendants were allegedly acting at the direction of senior LTTE leadership in Sri Lanka, including Pottu Amman, the LTTE's chief of intelligence and procurement and the right-hand man to LTTE leader Velupillai Prabakharan. The defendants discussed using bank accounts in Switzerland, St. Croix, or other offshore locations to finance the purchase. The parties also discussed a total price of between $900,000 and $937,500 for the equipment and the training. The complaints also allege that the defendants' conspiracy to provide material support to LTTE included fund raising in the United States and Canada, relying on "front" charitable organizations including the Tamil Relief Organization and the World Tamil Coordinating Committee to give the fund raising the appearance of legitimacy. These organizations were also used to send goods and material to LTTE in Sri Lanka.

The defendants all pled guilty in 2009. Researchers spoke to the prosecutors who said that because the defendants had pled guilty no transaction records had been entered into evidence and therefore they remained confidential.

Data: Court documents provide no detailed information.

Type of Transaction(s): Unknown

Suspicious Transaction(s)? Type: Unknown.

Proceeds of Crime? No.

22. LTTE Procurement Plot, Haji Subandi Thirunavukarasu Varatharasa, Haniffa Osman and Erick Wotulo.

From April to September 29, 2006, Haji Subandi Thirunavukarasu Varatharasa ("Varatharasa"), Haniffa Osman and Erick Wotulo, a retired Indonesian General, were involved in a plot to export military weapons to the LTTE. The case involved a sting operation. Central to the plan were two wire transfers, one of $250,000 and one of $452,000 from a company controlled by LTTE supporters with an account at the Eon Bank Berhad in Kuala Lumpur, Malaysia to an account maintained by the undercover agents in Maryland,

supposedly to buy missiles. Varatharasa also purchased food and provisions for his trip from Guam to deliver the weaponry to the LTTE.

All eventually pled guilty. Because of the guilty pleas no evidence was submitted on the banking transactions. However, prosecutors provided some detailed information on those transactions, which appeared to be simple wire transactions from one business to another.

Data: Court documents provide some detailed information on the transactions.

Type of Transaction(s): Large wire transfers from company account in one jurisdiction to account in another. Because a sting operation, unknown if recipient account was profiled by bank.

Suspicious Transaction(s)? Type: Unknown.

Proceeds of Crime? Presumed No.

23. Mahmoud Maawad.

Mahmoud Maawad ("Maawad"), an Egyptian, entered the U.S. in 1999 under a tourist visa and remained after the expiration of his visa. In September, 2005, Sporty's, Inc, a company that sells pilot training materials, reported that they had been defrauded by Maawad. Maawad had placed internet orders for numerous books, DVD's, and pilot training software. Maawad had used an ATM debit card to pay for the orders, but there were no funds in the account. He had also been using a false social security number to work and attend college. When FBI agents raided Maawad's campus apartment and found documents of Western Union transfers to and from Maawad.

Because Maawad pled guilty no details of the Western Union transfers were entered into evidence and none is available.

Data: Court documents provide only general description.

Type of Transaction(s): Size and origin of MSB wire transfers unknown.

Suspicious Transaction(s)? Type: Unknown.

Proceeds of Crime? Yes.

24. MEK Case, Roya Rahmani, Hossein Afshari, Mohammad Omidvar, Hassan Rezaie, Navid Taj, Najaf Eshkoftegi, Mustafa Ahmady, and Alireza Mohamad Moradi.

Each was charged in Los Angeles with soliciting charitable contributions at the Los Angeles International Airport for the "Committee for Human Rights" ("CHR").[79] This money was deposited in a CHR account in at a Bank of America branch in Los Angeles.[80] From there amounts were wired to various individuals with bank accounts at a Turkish bank.[81] From there, money was wired to the accounts of other individuals in Turkey, then wired to the bank accounts of other individuals in Belgium, France, the UAE, and Jordan, which was then diverted to the People's Mujahedin of Iran ("MEK").[82] This was done after participating in a conference call with an MEK leader, in which they learned that the State Department had designated the MEK as a foreign terrorist organization. The MEK leader told them to continue to provide material support despite the designation. The money sent to the MEK through these various transactions amounted to at least several hundred thousand dollars.

Prosecutors provided us with details of all transactions involving the US, Belgium, and France, numbering in the tens of thousands, as well as all records of Rahmani's personal bank account at Washington Mutual Bank, all of which had been admitted into evidence. They also provided us with transcripts of conversations relating to such payments.

Data: Court documents provide detailed information on wire and check transactions including payment records.

Type of Transaction(s): Small deposits to charity bank account in one jurisdiction, wire transfers to large number of unrelated individual bank accounts in another jurisdiction, then wire transfers to large number of unrelated individual bank accounts in various additional jurisdictions, then cash withdrawn.

Suspicious Transaction(s)? Type: Yes. Layering, possible integration.

Proceeds of Crime? Diversion of charitable donations.

---

[79] *See supra* text accompanying note 7.
[80] Placement.
[81] Layering.
[82] Layering and possible integration.

25. Uzair Paracha.

Uzair Paracha ("Paracha") was accused of conducting financial transactions involving that al-Qaeda associate's bank account and of planning to accepting up to $200,000 of al-Qaeda funds to be held as an investment in a business where Paracha was employed until the funds were needed by al-Qaeda. In 2003, an al-Qaeda associate ("AQA") told Paracha to deposit money into his bank account, to use his credit cards, and to close his post office box in Maryland. He told Paracha that the reason for these tasks was to make it appear that the AQA was still in the United States. The post office box that Paracha was to close was held jointly by the AQA and a woman. He said that the woman was a "good sister" who was helping them out. Paracha was to impersonate the AQA and close the post office box, using the story that he and this woman, with whom the AQA had rented the box, were no longer seeing each other. Paracha had possession of the AQA's Maryland driver's license, Social Security card, school identification, credit cards, as well as a key to the post office box.

While Paracha was found guilty of material support this did not include receipt of the $200,000, which was planned only. As a result there was no evidence submitted concerning actual financial transactions other than the use of another's credit card in the U.S. to give the impression that that person was physically present in the U.S. when in fact he was in Pakistan.

Data: Court documents provide only a general description.

Type of Transaction(s): Deposits.

Suspicious Transaction(s)? Type: No.

Proceeds of Crime? No.

26. Christopher Paul

Christopher Paul ("Paul"), a 44-year-old Muslim convert and native of Columbus, Ohio, allegedly agreed to involvement in a conspiracy to attack European resorts where U.S. citizens are known to vacation and U.S. properties, such as embassies and military installations. In the early 1990s, Paul traveled to Pakistan and Afghanistan. At an al-Qaeda training camp in Afghanistan, he received initial training in, among other things, the use of assault rifles, rocket-propelled grenades, and small unit tactics. After successfully completing this training, he joined al-Qaeda and stayed at the Beit ur Salam guesthouse. After fighting in Afghanistan, Paul returned to Ohio, where he began instructing individuals in martial arts at a mosque in Columbus. He also began recruiting local individuals with extremist intentions in order to establish a jihadist group in

Ohio. Over time and through his association with al-Qaeda, Paul became dedicated to committing jihad and furthering the objectives of al-Qaeda and other radical Islamic fundamentalists.

From 1993 through 1995, Paul, using various passports and names, traveled to the Balkans and fought in conflict zones such as Bosnia, establishing further contact with radical Islamic fundamentalists, and creating a master list of al-Qaeda leaders and other Islamic radicals worldwide. Paul returned to Columbus after fighting in the Balkans, and, in 1997, received a fax from two al-Qaeda co-conspirators in Europe asking, on behalf of "the brothers," for Paul to find them a "true group and place to make jihad." While in Columbus, Paul conducted training operations in Burr Oak State Park in Ohio with several members of his local group, replicating terrorist training he had received in Afghanistan and Bosnia.

On April 16, 1999, Paul traveled to meet with members of an Islamic terror cell in Germany. Paul provided explosives training. Upon his return to Ohio from Germany, Paul had a member of his group in Columbus purchase a printer/scanner in May 1999. Paul also bought other equipment to be use by extremists, including night vision equipment and a laser range finder. In November 1999, bank records show that Paul wire transferred $1,760 to Mehdi, one of the principal members of the German cell.

Paul was indicted on April 11, 2007, charged with conspiracy to provide material support, namely sending money to a known terrorist figure in Europe. In 2008 Paul pled guilty to conspiracy to use a weapon of mass destruction. As a result, any payments to and from Paul and others in the Ohio, the Bosnia, Afghanistan, or Germany, including Paul's wire transfer, were not introduced as evidence and prosecutors could not disclose this information.

Data: Court documents provide only a general description.

Type of Transaction(s): Cross border payments of unknown type, single small cross border wire transfer.

Suspicious Transaction(s)? Type: Unknown.

Proceeds of Crime? No.

27. The Portland 7. Patrice Lumumba Ford, Martinique Lewis , Al Saoub, Maher "Mike" Hawash, Jeffrey Battle, Muhammad Bilal, and Ahmed Bilal.

Shortly after 9/11, a group of Muslim-Americans in Oregon sought to join Taliban forces fighting American troops in defense of al-Qaida. They tried to enter Afghanistan through China, but were unsuccessful and came home. The group was led by Jeffrey Battle ("Battle") and Patrice Lumumba Ford ("Ford")

and included Mike Hawash. Martinique Lewis ("Lewis"), the ex-wife of co-defendant Battle, was allegedly involved in money laundering. She admitted that she transferred or transmitted money or funds from the United States to a place outside the country for the purpose of assisting Battle in willfully supplying services to the Taliban. When told about the money in October Lewis allegedly wired to Battle, who federal officials said was headed to Afghanistan, the money. Lewis did not travel with the group; she was charged with supporting the effort by sending money to Battle in Hong Kong and Bangladesh.

All seven eventually pled guilty. In his plea agreement Ford admitted that he had wired $500 through Western Union to Al Saoub in Guangzhou, China, and $200 to Ahmed Bilal in Indonesia.[83] He also admitted that he had wired an additional $483 through Western Union to defendant Al Saoub in Guangzhou, China.[84] In her guilty plea Lewis also admitted that on a number of occasions she wired money to Battle via Western Union to various locations in Hong Kong, China and Bangladesh in amounts ranging from $100 to $400 dollars.[85] They were aware that on each occasion the money wired was to be used to support Battle's continuing attempts to enter Afghanistan to fight in jihad for the Taliban against the United States and its allies.

Because of the guilty pleas details of the payments were not admitted as evidence.

Data: Court documents provide only a general description.

Type of Transaction(s): Small number of small MSB wire transfers from one jurisdiction to several individuals in multiple jurisdictions.

Suspicious Transaction(s)? Type: No.

Proceeds of Crime? No.

28. The LAX Millenium Plot, Mokhtar Haouari, Abdelghani Meskini and Ahmed Ressam. In 1994, Haouari met Ressam.

The so-called "Millennium Plot" to bomb Los Angeles International Airport ("LAX") in late December 1999 involved Mokhtar Haouari ("Haouari"), Abdelghani Meskini ("Meskini") and Ahmed Ressam ("Ressam"). In 1994, Haouari met Ressam, a fellow Algerian, in Montréal. Between 1996 and 1997, Ressam sold Haouari stolen identification documents, charge cards and a fake Canadian passport. In 1998, Ressam left for Afghanistan to attend terrorist training camps. Months before Ressam's departure, Haouari had met up with

[83] *See supra* text accompanying note 17.
[84] *Id*.
[85] Possible smurfing, if the small amounts were used to avoid suspicion or detection.

Meskini, another Algerian, who had arrived in Montréal in October 1997. On various occasions between 1997 and 1999, Haouari provided Meskini with fake Canadian passports and other forms of identification, some of which Meskini used to commit bank and credit card fraud.

By the summer of 1999, Ressam wanted to obtain a credit card. He contacted Haouari and asked if he could "pretend [to be] working" in Haouari's store, Artisanat Nord-Sud, in order to qualify for a credit card. Haouari agreed. He filled out an application for Ressam under the latter's alias, "Benni Noris." Ressam received the Royal Bank Visa card.

Around November 17, 1999, Ressam flew from Montréal to Vancouver. He said that he would call Haouari and let him know when to contact his friend Meskini. Ressam combined the $3,000 in cash he had received from Haouari with money he already had. He bought chemicals, instruments and airline tickets with the money. He also rented a car and paid for a hotel room. For two weeks, Ressam stayed in Vancouver and prepared the chemical materials for the explosives. By the beginning of December 1999, Ressam had returned to Montréal. On his first day back, he met Haouari at the store they were opening. Ressam said that he wanted to meet Haouari's friend in Seattle in one week. Haouari asked Meskini to meet that man in Seattle and to give him $1500 to $2000 in cash. On December 11, Meskini, who had purchased a round trip New York-to-Seattle airline ticket under the alias "Eduardo Rocha," flew to Seattle. On December 14, 1999, Ressam called Meskini and said, "This evening, I will be in Seattle. I'll call you." Ressam then left Vancouver in a rental car with the explosives loaded in the trunk. He took an auto ferry to Victoria and then another ferry to Port Angeles.

Meskini pleaded guilty. Haouari and Ressam were found guilty of providing material support. All transactions other than those undertaken though the visa card was in cash. No bank transactions records were introduced into evidence.

Data: Court documents provide only a general description.

Type of Transaction(s): Fraudulent credit card application, credit card payments.

Suspicious Transaction(s)? Type: No.

Proceeds of Crime? Yes.

29. Aafia Siddiqui, Mohammad Khan

Aafia Siddiqui ("Siddiqui"), a Pakistanti national, came to the U.S. in 1990 and was later married to Mohammad Khan. She attended college and

graduate school and received a PhD in 2001. In 2001, Siddiqui made regular debit-card payments from her account at Fleet National Bank in Boston to Benevolence International ("BI"), designated a SDTO in 2002. From another account they repeated debit-card purchases from stores that specialize in high-tech military equipment and apparel, including Black Hawk Industries in Chesapeake, Virginia and Brigade Quartermasters in Georgia. Black Hawk's website advertises grips, mounts and parts for AK-47s and other military-assault rifles as well as highly specialized combat clothing, including vests designed for bomb disposal. They also made major purchases from U.S. airlines and hotels in Pittsburgh, PA and North Carolina as well as an $8,000 international wire transfer on December 21, 2001 to an individual with an account in Habib Bank in Pakistan.[86] Following BI's designation Fleet National Bank began an investigation and filed a suspicious activity report.

On March 1, 2003 Khalid Shaikh Mohammed, in Pakistani custody, allegedly named Siddiqui as sympathetic. FBI Agents allegedly found evidence that she had rented a post-office box to help a Baltimore, Maryland-based individual alleged to have been an al-Qaeda contact who had been assigned by Khalid Shaikh Mohammed to blow up underground gasoline-storage tanks. Siddiqui was arrested in 2008 on charges related to attempted murder and assault of United States officers and employees in Afghanistan. She was convicted in February 2010 of attempted murder of U.S. soldiers in Afghanistan. Because no other charges were filed no evidence was admitted concerning financial institution transactions.

Data: Court documents provide only a general description.

Type of Transaction(s): Debit card payments to a designated terrorist organization and to high-tech military equipment companies; medium sized cross-border wire transfer to an unknown person.

Suspicious Transaction(s)? Type: Possible. Possible terrorist financing in repeat purchases from military equipment store?

Proceeds of Crime? No.

30. Mohamed Adbullah Warsame.

On January 20, 2004, Mohamed Abdullah Warsame ("Warsame"), a naturalized Canadian citizen was charged with conspiracy to provide material support to a designated FTO. According to the allegations, in March 2000,

[86] *See supra* text accompanying note 17.

Warsame traveled to Afghanistan where he attended a training camp outside Kabul. al-Qaeda funds were used to pay for his airline ticket travel to Afghanistan and to provide him $1,700 traveling money, although it is not known how these payments were made. In the summer of 2000, Warsame attended the al-Faruq training. Warsame subsequently worked at an al-Qaeda guesthouse and clinic. In late March 2001, Warsame traveled from Pakistan, via London, to Canada. After leaving Pakistan, Warsame wired from his individual bank account in the U.S. approximately $2,000 to one of his former camp commanders.[87] Warsame then relocated to Minneapolis, MN. Throughout 2002-2003, Warsame continued to exchange emails with, and provide information to, several individuals associated with al-Qaeda.

Warsame pled guilty to one count of material support. No information regarding financial transfers was admitted as evidence.

Data: Court documents provide only a general description.

Type of Transaction(s): Medium-sized cross border wire transfer.

Suspicious Transaction(s)? Type: No.

Proceeds of Crime? No.

[87] *Id.*