TRYSTS OR TERRORISTS? FINANCIAL INSTITUTIONS AND THE SEARCH FOR BAD GUYS

*Richard K. Gordon**

INTRODUCTION

In early March of 2008, the news broke that Eliot Spitzer, the then-current Governor and former Attorney General of New York, had been involved in purchasing sexual favors from an elite escort service called the Emperors Club.[1] What was unusual about the unfolding story was not just that a sitting governor would patronize such an establishment, but that his involvement had apparently been uncovered in part as a result of reports filed by banks under federal anti–money laundering policies and policies combating the financing of terrorism.[2] Spitzer's secret love life had been exposed by a regime designed primarily to catch serious criminals and terrorist financers and to grab their funds for the public fisc.[3]

Apparently Governor Spitzer had paid for services by having his bank, North Fork, transfer funds from his account to at least two

* Associate Professor of Law, Case Western Reserve University School of Law; Visiting Associate Professor of International Studies, Brown University, Fall 2008. B.A. 1978, Yale; J.D. 1984, Harvard. From 1994 through 2003 the author served as a senior staff member at the International Monetary Fund where he worked on the development and implementation of the international standards for anti-money laundering and, following the terrorist attacks of September 11, 2001 on the United States, combating the financing of terrorism. The views expressed in this paper are the author's alone and should not be attributed to the International Monetary Fund. The author would like to thank Professor Craig Boise and the participants in the Wake Forest Law Review Symposium for their comments and the students who participated in the Spring 2007 Case Western Reserve University School of Law seminar Financial Sector Integrity for their contribution to this article.

1. Danny Hakim & William Rashbaum, *Spitzer, Linked to a Sex Ring as a Client, Gives an Apology*, N.Y. TIMES, Mar. 11, 2008, at A1, *available at* http://www.nytimes.com/2008/03/10/nyregion/10cndspitzer.html?_r=1&hp&oref=slogin.

2. Moisés Naím, *Caught in the Wrong Net; Spitzer and the CEO Were Both Toppled by a Post-9/11 Hardening of Views on Global Money Laundering*, NEWSWEEK (International Edition), Mar. 31, 2008, *available at* http://www.newsweek.com/id/128422.

3. *Id.*

"shell" companies controlled by the Emperors Club.[4] According to an article in *Newsweek* by Moisés Naím (who is also the editor of *Foreign Policy*):

> The inquiry into the Emperors Club . . . began last year, whena bank, HSBC, reported to U.S. Authorities [meaning FinCen,the Financial Crimes Enforcement Network] that the accountsof two companies, QAT and QAT Consulting Group, wereregularly receiving deposits from questionable sources. Severalof the transfers had come from accounts that seemed set up tomask the sender's identity. The investigation ultimatelyrevealed that the person in question wasn't a drug dealer or aterrorist. It was the governor of New York.[5]

Newsday reported that the investigation began with "tips" from banks that noticed unusual wire transfers between Spitzer's account and "shell companies," i.e. QAT International and QAT Consulting Group, set up by the Emperors Club.[6] According to the affidavit filed in support of the sealed complaint, QAT Consulting Group, Inc. and QAT International, Inc. were used to "promote" and "conceal" the prostitution business of the Emperors Club.[7] Again according to news reports, both Spitzer's bank and the bank where QAT and QAT Consulting Group held accounts filed Suspicious Activity Reports ("SARs") (which are called Suspicious Transaction Reports ("STRs") outside of the United States) with the government, which ultimately led to an investigation of Spitzer and the Emperors Club.[8]

While press reports vary, the more specific facts appear to be these. North Fork detected Spitzer engaging in "unusual financial transactions" by making "large cash transfers" that did not fit his "usual pattern for the accounts," which triggered concern in the bank.[9] One source also reported that, after transferring the funds, Spitzer called North Fork and asked that his name "be removed" from one of the wires, which lead the bank to file a SAR.[10] The

4. Keith B. Richburg et al., *FBI Watched Spitzer Before February Incident*, WASH. POST, Mar. 12, 2008, at A1, *available at* http://www.washingtonpost.com/wpdyn/content/story/2008/03/11/ST2008031102183.html.

5. Naím, *supra* note 2.

6. Michael Amon, *Rival Tipped Feds; Controversial GOP Operative's Letter to FBI About Spitzer's Trysts 'Taint's Probe of Former Guv," Prof Says*, NEWSDAY, March 24, 2008, at A7.

7. Sealed Complaint at 33, United States v. Brener, 08 Mag. 0463 [hereinafter Sealed Complaint]. *See also id*. at 31–33.

8. Don Van Natta, Jr. & Jo Becker, *Bank Reports, Then Wiretapping, Led to Unraveling of Ring and Its Client*, N.Y. TIMES, March 13, 2008, at A20, *available at* http://www.nytimes.com/2008/03/13/nyregion/13legal.html?scp=1&sq=Bank+Reports%2C+Then+Wiretapping%2C+Led+to+Unraveling+of+Ring+and+Its+Client+9&st=nyt.

9. Jonathan D. Epstein, *Spitzer Didn't Bank on Money Trail Fiasco*, BUFFALO NEWS, Mar. 16, 2008, at A13.

10. John Sandman, *Spitzer SAR Disclosure an AML Breach*,

affidavit attached to the SAR quoted a telephone call from an Emperors Club employee who said that Spitzer did not "do traditional wire transferring."[11] Another source stated that suspicion was also raised because "Spitzer had tried to break down large wire transfers into amounts smaller than $10,000, seemingly to get around federal reporting rules."[12] Another source suggested that the bank may have filed a SAR as revenge for Spitzer's efforts when he was New York Attorney General to force the bank to refund $20,000 in what Spitzer claimed had been illegal fees.[13] Another possibility was that the bank was especially vigilant because Spitzer was, as Governor, "a politically exposed person" and therefore more likely to be soliciting bribes.[14] Still another source reported that sometime later, HSBC Bank filed one or more SARs when its employees "investigated" QAT International and QAT Consulting Group, both of which had accounts at the bank, and discovered that HSBC's files for the companies "included virtually no information . . . due diligence was not done—there was no Dun & Bradstreet, no documentation, almost nothing in the file . . . "[15] FinCEN then passed on the SARs to the Internal Revenue Service, which began an investigation.[16]

Press reports differed on exactly why the IRS pressed forward with an investigation, which included wiretaps and a criminal complaint. One suggests that it was the combination of SARs from North Fork and HSBC that started the investigation.[17] Another said the investigation may have started much earlier when the lawyers representing Roger J. Stone Jr., a Republican political consultant, "wrote a letter to the F.B.I. stating that Gov. Eliot Spitzer had patronized high-priced prostitutes during trips to Florida."[18] Other sources suggested that when government authorities discovered that the SARs concerned a senior government official, they had to

---

SEC. INDUS. NEWS, Mar. 31, 2008, at 1, *available at* http://www.accessmylibrary.com/coms2/summary_0286-34232673_ITM.

11. Sealed Complaint, *supra* note 8, at 27.

12. Melanie Lefkowitz & Michael Amon, *Wife, Close Aide Urged Spitzer to Stay, Say Sources*, NEWSDAY, Mar. 16, 2008, at A8.

13. Tony Allen Mills, *Toppling of the Luv Guv is 'Wall Street Revenge,'* THE SUNDAY TIMES (London), Mar. 16, 2008, *available at* http://www.timesonline.co.uk/tol/news/world/us_and_americas/us_elections /article3559410.ece.

14. Van Natta & Becker, *supra* note 9.

15. *Id.*

16. *Id.*

17. *Id.*; *New York Governor Spitzer Resigns in Prostitution Scandal; Federal Probe Ensnares High-Priced Ring*, FACTS ON FILE WORLD NEWS DIGEST, Mar. 13, 2008, at A3.

18. Danny Hakim & Fernanda Santos, *G.O.P. Consultant Says His Lawyers Told F.B.I. in '07 of Alleged Spitzer Trysts*, N.Y. TIMES, Mar. 24, 2008, at B5, *available at* http://www.nytimes.com/2008/03/24 /nyregion/24spitzer.html?scp=1&sq=G.O.P.+Consultant+Says+His+Lawyers +Told+F.B.I.+in+%9207+of+Alleged+Spitzer+Trysts&st=nyt.

investigate further.[19] Another quoted a defense lawyer who said, "[i]f the government gets a SAR about a high-ranking public official, they would be negligent not to pursue it, if only to determine whether there was bribery or extortion involved."[20]

A number of commentators noted, however, that while the system was designed to ferret out major criminals and terrorists,[21] instead it snared a man hiring a prostitute, which is not a crime normally on the authorities' radar screen.[22] Another commentator quoted Don Van Natta, Jr., a former director of FinCEN. "What 9/11 taught us is the value of financial information," Van Natta said. "Money doesn't lie. Money leaves a footprint. And that's exactly what happened with Spitzer."[23]

Although not all of the press reports are fully consistent (and many rely on unverifiable sources), there are a number of key issues surrounding how the Spitzer/Emperors Club case *apparently* unfolded. First, Spitzer made payments to the Emperors Club indirectly through QAT International and QAT Consulting Group, companies controlled by the Club.[24] Spitzer ordered his bank either to wire money to the bank accounts of one or more of the companies, which then held the cash until it was withdrawn by the Emperors Club or its owners, or to wire the money on to a bank account held directly by the Emperors Club or its owners.[25] Both Spitzer's bank and the shell companies' bank were monitoring the transactions of their account holders and decided to make a report to FinCEN when they discovered something "suspicious."[26] With respect to Spitzer, reasons for suspicion included that his account activities did not fit his usual pattern of account activity, he had apparently broken down larger transfers into smaller amounts, he had tried to delete his name from one or more transfers, and he was an important politician.[27] With respect to QAT International and QAT Consulting

19. David Johnston & Philip Shenon, *U.S. Defends Tough Tactics on Spitzer*, N.Y. TIMES, Mar. 21, 2008 at A1, *available at* http://www.nytimes.com/2008/03/21/nyregion/21justice.html?scp=1&sq=U.S. +Defends+Tough+Tactics+with+Spitzer&st=nyt.

20. *Id.*

21. *Id.*

22. *Id.*

23. Van Natta & Becker, *supra* note 8.

24. Brian Ross, *It Wasn't the Sex; Suspicious $$ Transfers Led to Spitzer*, ABC NEWS, Mar. 10, 2008, http://abcnews.go.com/Blotter/story?id=4424507.

25. *Money Transfers Spark Spitzer Probe*, UPI.COM, Mar. 12, 2008, http://www.upi.com/Top_News/2008/03/12/Money_transfers_spark_Spitzer _probe/UPI-92401205333210.

26. Van Natta & Becker, *supra* note 8.

27. *See* Mario Bruno-Britz, *Spitzer Exposed by Bank's Anti-Money Laundering Technology*, BANK SYSTEMS & TECH., Mar. 27, 2008, *available at* http://www.banktech.com/aml/showArticle.jhtml?articleID=206904957; Robert Kessler, *Eliot Spitzer's Bank Turned Him In to the IRS*, NEWSDAY, March 11, 2008, *available at* http://www.newsday.com/news/local/state /ny-stspitzerbank0312,0,4637246.story; *Lessons from Spitzer's Fall*,

Group, the main reason for suspicion was that they were shell companies and that the bank had previously failed to conduct "due diligence" by creating a client profile regarding the companies' activities.[28] FinCEN apparently matched the two reports, and reported this information to the IRS, which noted the suspicious nature of the transactions, including Spitzer's position as attorney general, and began the investigation leading to his downfall.[29]

As will be discussed in greater detail infra, each of the details of the transactions would normally raise suspicion under not only U.S. anti-money laundering and financing of terrorism ("AML/CFT") rules, but under the AML/CFT international standard as well.[30] In fact, anyone familiar with these rules can only wonder why someone would so obviously trigger the possibility of an investigation rather than simply pay the Emperors Club directly. One possibility might be that Spitzer was trying to hide his involvement in the event that there was an investigation of the club. However, as the former director of FinCEN noted, such a relatively minor detour would not cover up his involvement in the event of such an investigation since there would still be records of the payments made from Spitzer's account to the accounts of the two shell companies. One report speculated that the reason Spitzer took such minor steps to conceal or obfuscate the transactions was not to hide his payments to the Emperors Club from law enforcement, which rarely prosecutes consensual sex for pay, but instead to keep the facts from his family, especially his wife.[31]

Spitzer's transactions that resulted in the filing of SARs—and that resulted in the commencement of a formal criminal investigation—can be contrasted with a common transaction involving the financing of terrorism. One typical example cited in a recent report on terrorism financing by the Financial Action Task Force ("FATF") involves a legitimate charity that quickly raised large amounts of funds from the local community.[32] A controller of the charity diverted a portion of these donations to terrorist training camps in Pakistan. The transactions consisted of domestic transfers to the charity and international transfers to an individual, who then turned the money over to the terrorists. There were no circuitous payments as in the Spitzer case—the transactions were actually quite simple and direct. The only indication that terrorism financing might be involved was that law enforcement had reason to

CHRISTIAN SCI. MONITOR, Mar. 13, 2008, at 8, *available at* http://www.csmonitor.com/2008/0313/p08s01-comv.html; *see also supra* note 20.

28. Van Natta & Becker, *supra* note 8.

29. *Id.*

30. *See infra* note 38 and accompanying text.

31. Stevenson Swanson, *Spitzer Quits in Remarkable Fall from Grace,* CHI. TRIB., Mar. 13, 2008, at 1.

32. FINANCIAL ACTION TASK FORCE, TERRORIST FINANCING 12 (2008), http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf.

believe that the charity's controller had some connection with people suspected of being involved in terrorist activities, including the individual who received the payments from the charity. The report notes that "[l]aw enforcement assessed that the charity was being exploited both as a 'front' to raise funds and as a 'means of transmission' to divert a portion of them to known terrorist associates of A."[33] However, the transactions themselves were not suspicious.[34]

In a typical transaction, a legitimate (or sometimes illegitimate) charity collects cash and other donations and deposits those to a bank account in a western country, then makes a payment directly to the bank account of another charitable organization or business location in another country, often a jurisdiction with serious internal conflict, including terrorism.[35] Often, some or all of that money is then diverted to finance terrorism while some is used for legitimate charitable activity.[36] If terrorists are smarter (or at least more knowledgeable) than Eliot Spitzer, one would expect that they would not arrange their financial affairs in such a way that would trigger the filing of SARs resulting in subsequent investigations. There may be other reasons that a bank may discover and report that a client may be financing terrorism (for example, they know that the client associates with known terrorists). However, one can assume that the terrorists would try to not follow former Governor Spitzer's lead by adding circuitous transactions that might result in the filing of a SAR.

Having demonstrating a few of the key features of some factors that may trigger a bank to alert law enforcement as to possible illegal activity and for the government to conduct a follow-up investigation, and having suggested that terrorist financing may not often follow such detectable patterns, this Article will turn to a fundamental problem that goes to the heart of AML/CFT policies, or at least those that focus on banks and other financial institutions. There is a constant and unresolved tension between how much financial institutions should be expected to do and how much the government should be expected to do to uncover criminals,

33. *Id.*

34. *Id.*

35. *See, e.g.*, MATTHEW LEVITT, HAMAS: POLITICS, CHARITY, AND TERRORISM IN THE SERVICE OF JIHAD 62–69, 72 (2006) (discussing Hamas fundraising and money laundering). The author is currently engaged in a project to examine terrorism financing techniques, sponsored by the United Nations Counter-Terrorism Implementation Task Force. Although there have been a few exceptions, the examples of terrorism financing examined so far generally fit into the pattern described above.

36. Pierre-Emmanuel Ly, *The Charitable Activities of Terrorist Organizations*, 131 PUB. CHOICE 177, 178–79 (2007), *available at* http://papers.ssrn.com/abstract=951003 (noting that terrorist groups support both legitimate charitable activity and terrorism, in part to generate political support from their legitimate activity).

especially terrorists and their financiers.[37] According to the internationally accepted AML/CFT regime,[38] financial institutions[39]

37. *See, e.g.*, CONSULTATIVE GROUP TO ASSIST THE POOR (CGAP), AML/CFT REGULATION: COULD INCREASING ACCESS IMPROVE SECURITY? (2008), http://64.127.136.149/portal/site/portfolio/Feb2008FAI/.

38. FINANCIAL ACTION TASK FORCE, THE 40 RECOMMENDATIONS (2004), *available at* http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html [hereinafter FATF 40]; THE FINANCIAL ACTION TASK FORCE, 9 SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING, *available at* http://www.oecd.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html [hereinafter FATF SPECIAL IX]; FINANCIAL ACTION TASK FORCE, METHODOLOGY FOR ASSESSING COMPLIANCE WITH THE FATF 40 RECOMMENDATIONS AND THE FATF 9 SPECIAL RECOMMENDATIONS (2007), *available at* http://www.fatf-gafi.org/dataoecd/16/54/40339628.pdf [hereinafter FATF METHODOLOGY]. Each has been adapted as part of a "global standard" for AML/CFT by vote of the International Monetary Fund ("IMF") Executive Board; *see also IMF Advances Efforts to Combat Money Laundering and Terrorist Finance*, Public Information Notice No. 02/87, August 8, 2002, *available at* http://www.imf.org/external/np/sec/pn/2002/pn0287.htm; INTERNATIONAL MONETARY FUND, REPORT ON THE OUTCOME OF THE FATF PLENARY MEETING AND PROPOSAL FOR THE ENDORSEMENT OF THE METHODOLOGY FOR ASSESSING COMPLIANCE WITH ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) STANDARD 1 (2002), *available at* http://www.imf.org/external/np/mae/aml/2002/eng/110802.pdf [hereinafter IMF METHODOLOGY]. The author, who was a senior staff member at the IMF from 1994 to 2004, was a principle author of IMF documents relating to AML/CFT during those years. Also, each member of the FATF and each of the seven FATF-style regional bodies has accepted the FATF 40 + 9 as the global standard. *See* FINANCIAL ACTION TASK FORCE, FATF MEMBERS AND OBSERVERS, *available at* http://www.fatf-gafi.org/document/52/0,3343,en_32250379_32237295_34027188_1_1_1_1,00.html (providing web links to each FATF-style regional body); s*ee also* PAUL ALLEN SCHOTT, REFERENCE GUIDE TO ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM III-5 to -8 (2d ed. 2006), *available at* http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf. There are also a number of UN-sponsored conventions and Security Council Resolutions dealing with AML/CFT. *Id.* at III-2 to -5. But, these are incorporated into the FATF standard through the Methodology Document Recommendation 1 and Special Recommendations I, II, and III. IMF METHODOLOGY, *supra* note 38, at 12, 62–66.

39. Financial institutions include any person who engages in the following activities: 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; and underwriting and placement of life insurance and other investment related insurance, money, and currency

(and a few others),[40] are required to implement a series of AML/CFT "preventive measures." These are rules that require financial institutions to identify and monitor their clients activities to see if they might be laundering criminal proceeds or financing terrorists. If the financial institution suspects they are, it must describe the cause for suspicion and make a report to the government for further investigation.[41] At least for regulated financial institutions (the most important of which in most developed countries are deposit-taking institutions, securities firms, broker-dealers, insurance firms, and money transfer agents),[42] it is the financial institution's supervisors, regulators, and examiners who are tasked with ensuring that these "preventive measures" are effectively implemented.[43] The United States largely follows the rules prescribed by the international AML/CFT standard.[44]

These rules are fundamentally different in type and kind from the prudential rules that are also imposed on regulated financial institutions and whose implementation is a primary function of the financial institution's supervisors, regulators, and examiners. These rules are designed primarily to protect the safety and soundness of individual financial institutions and the financial system as whole, including, in particular, the customers of those financial institutions. These rules are about not putting all investment (typically lending) eggs in one financial basket, or making sure that investors judge risk appropriately, or that banks have enough capital to pay depositors in the event of significant loan defaults:[45] in

changing. FINANCIAL ACTION TASK FORCE, 40 RECOMMENDATIONS GLOSSARY, http://www.fatf-gafi.org/glossary/0,3414,en_32250379_32236889_35433764_1_1_1_1,00.html#34289432 (last visited Sept. 1, 2008).

40. This refers to 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. *See* FATF 40, *supra* note 38, at 12.

41. *Id.* at 2–3. *See also infra* notes 42–48 and accompanying text (discussing these rules in greater detail).

42. FATF, SUMMARIES, REPORTS AND ANNEXES, http://www.fatf-gafi.org/document/32/0,3343,en_32250379_32236982_35128416_1_1_1_1,00.html.

43. FATF 40, *supra* note 38, at 7–8 (describing Recommendations 23–25).

44. *See* FINANCIAL ACTION TASK FORCE, THIRD MUTUAL EVALUATION REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM, UNITED STATES OF AMERICA 299–303 (2006), *available at* http://www.fatf-gafi.org/dataoecd/44/9/37101772.pdf [hereinafter MUTUAL EVALUATION REPORT]. U.S. rules are discussed in greater detail infra. *See infra* notes 45–48 and accompanying text.

45. *See generally* BASEL COMMITTEE ON BANKING SUPERVISION: THE BASEL CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION (1997), *available at* http://www.bis.org/publ/bcbs30a.htm (explaining that the Core Principles cover seven principal areas: preconditions for effective banking supervision, licensing and structure, prudential regulations and requirements, methods of banking supervision, information and record-keeping requirements, formal powers of supervisors, and cross-border banking).

other words, the kind of prudential rules that have not always been carefully observed in the past year. But in general, the supervisors and the supervised, the Office of the Comptroller of the Currency and the Federal Reserve Board and U.S. banks, for example,[46] have similar goals with respect to prudential rules. No one wants a bank or other financial institution to become illiquid or insolvent—not the bank's owners, not the bank's managers, and not the bank's supervisors or examiners. Each group tends to have similar interests, if not identical ones.

Before AML rules were established, banks and other financial institutions did not consider themselves in the business of catching criminals, especially not terrorists. Now, however, as a result of the creation and implementation of the global AML/CFT standard, they are.[47] Much (though certainly not all) of the difficulty that financial institutions have in identifying and reporting suspected terrorist transactions lies in the difficulty they have in identifying suspected money laundering or the proceeds of crime.[48] This is not a surprise given that the CFT rules relating to a financial institution's responsibility to detect terrorism-financing transactions are based on the earlier, pre-existing AML rules. For this reason it is necessary first to turn to the latter.

I. INTRODUCTION TO MONEY LAUNDERING AND AML RULES

This Article will discuss in detail key AML principles infra, but because it helps first to have a plain-language understanding and more common sense introduction to the issue, this Article briefly will review the key issues and apply them to the Spitzer and terrorism-financing cases.

Sustained global interest in anti-money laundering policies began in the 1980s, primarily in the context of concern over international drug trafficking. Because the drug trade (and other illegal activity) generated huge profits, criminals found it necessary to find a way to introduce the cash they made into the formal financial system so that it could be spent or invested without drawing the attention of law enforcement. However, simply depositing huge amounts of cash at a single bank could also draw the attention of bank officials and, eventually, law enforcement.

46. COMPTROLLER OF THE CURRENCY ADMINISTRATOR OF NATIONAL BANKS, ABOUT THE OCC, *available at* http://www.occ.treas.gov/aboutocc.htm; THE FEDERAL RESERVE SYSTEM: PURPOSES AND FUNCTIONS, SUPERVISION AND REGULATION, *available at* http://www.federalreserve.gov/pf/pdf/pf_5.pdf.

47. *See, e.g.*, THE WOLFSBERG GROUP, WOLFSBERG AML PRINCIPLES, http://wolfsberg-principles.com (last visited Sept. 1, 2008); s*ee also* MARK PIETH & GEMMA AIOLFI, THE PRIVATE SECTOR BECOMES ACTIVE: THE WOLFSBERG PROCESS, *available at* http://www.wolfsberg-principles.com/pdf/Wolfsberg -Process.pdf (discussing the origins of the Wolfsberg principles).

48. Eugene Yoo, *The Institutional AML Challenge*, SEC. INDUSTRY NEWS, Sept. 18, 2006, *available at* http://actimize.com/index.aspx?page=news21.

In the paradigm case, drug traffickers receive large sums of money in cash because those who purchase illegal drugs do not pay by check or credit card, which can be traced. Because it looks rather odd, especially to the police, to carry around a trunk full of often filthy low-denomination currency to buy big ticket items and to make legitimate investments, the criminal needs to enter the cash into the formal financial system via a financial institution. Doing so is referred to as the "placement stage."[49]

One of the first AML principles was to require financial institutions (especially banks, which are usually the point of entry in the financial system for cash) to identify exactly who their customers were and to report to the authorities whenever a customer deposited a substantial amount of cash.[50] One benefit of knowing the identity of a customer is that the bank or law enforcement agency can identify the accounts of known criminals. Of course, some customers often legitimately receive or deposit huge amounts of cash, such as those running a 7-11 or some other cash-intensive business. In order to prevent constant reporting of unhelpful information, the bank, or at least the authorities, needs to be able to exclude these customers. In order to determine if patterns of cash deposits do not suggest that the customer was receiving criminal proceeds, it is necessary for the bank to determine the customer's legitimate activities and whether they could be expected to generate such cash. Once a customer profile has been established, deposit patterns that do not fit that profile would legitimately generate some suspicion. The bank could then investigate and see if the customer's profile had changed such that the unusual transactions could be explained by some legitimate activity. If not, the bank could report such suspicions without fear of generating too many false positives. Such information might be enable law enforcement authorities to catch drug traffickers.

Under the AML principles, once a bank was required to establish a customer profile, it would also be possible to determine when non-cash payments looked atypical (i.e. possibly the proceeds of crime).[51] In other words, it would be able to detect whether the proceeds might be from crimes other than those that generated significant cash. This would allow AML rules to include other types of crimes, meaning those that did not generate cash proceeds, as "predicate offenses" to suspected money laundering.[52] In addition,

49. The background to the development of AML rules is described in many places, but for one of the best brief introductions, see SCHOTT, *supra* note 38, at I-7 to I-9.

50. *See, e.g.*, THE WOLFSBERG GROUP, WOLFSBERG AML PRINCIPLES ON PRIVATE BANKING (2002), http://www.wolfsberg-principles.com/privat-banking.html.

51. *Id.*

52. *See* PETER REUTER & EDWIN M. TRUMAN, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 105 (2004).

patterns of payments from an account, as well as deposits into an account, could be monitored for transactions that did not fit the expected patterns of a customer.

While this was the beginning, the AML system needed to become more complex and extensive in order to overcome evasive countermeasures taken by criminals to avoid being caught under anti-money laundering rules. Criminals would avoid the cash transaction reporting requirements by "smurfing" or breaking up large cash deposits into smaller ones in many accounts opened by confederates or their lawyers, or by legal persons, like companies.[53] Money from these accounts would then be deposited to a single account held by the criminal. In order to distance themselves further from the illegal origins of profits, criminals would then often make payments to others, including corporations or other legal persons. This activity is typically called the "layering stage."[54] In order to aggregate such payments and to trace them through the payment chain, financial institutions need to be able to identify who the real owner of the account is (i.e. the beneficial owner or controller), and not just the legal titleholder to the account (i.e. the name on the account). Because this can be difficult to ascertain, the financial institution would also want to know the customer profile of each person holding an account to see if it were normal for the customer to receive and make payments in a particular way.[55]
Because banking is international, every intervening bank would need to follow the same procedures and make the information available to law enforcement from other countries, which would then require cross-border cooperation. For example:

> Assume a law professor has, in addition to her employment income, significant criminal proceeds from both narcotics sales and from defrauding her employer. Every month she receives $10,000 in cash from selling illegal stimulants to her first-year contracts students and $5,000 in reimbursements for fictional travel to law review symposia. Her legitimate bank deposits would include such items as law professor wages, plus perhaps other miscellaneous small amounts (e.g. interest on savings accounts and the occasional holiday gift). Her bank transactions would also include regular, often recurring payments (e.g. rent, utilities, and payments for credit card debt).

53. INSTITUTE FOR INTERNATIONAL RESEARCH, ANTI-MONEY LAUNDERING AUDIT & COMPLIANCE FORUM: GLOSSARY, http://www.iirusa.com/AMLAC2006/2688.xml (last visited Sept. 1, 2008).

54. Eduardo Aninat et al., *Combating Money Laundering and the Financing of Terrorism*, 39 FIN. & DEV. 3, *available at* http://www.imf.org/external/pubs/ft/fandd/2002/09/aninat.htm.

55. *See* WOLFSBERG AML PRINCIPLES, *supra* note 47.

Under a client identification and cash reporting regime, any cash deposits into her bank account above a certain amount would trigger the filing of a report. The professor might seek to avoid such a filing by opening a number of accounts at different banks and depositing only small amounts of cash into each account. However, if the bank is required to inquire as to the client's profile of legitimate deposits and monitor actual deposits to see if they conform with that profile, the bank would inquire as to why a professor's account involves only deposits of small amounts of cash rather than other transactions such as wage deposits, etc. Absent a suitable explanation, a SAR would be filed, in this case from each of the banks where the professor held a small cash account. This would permit the financial intelligence unit to aggregate cash amounts from each, allowing the unit to pursue further investigation.

In order to avoid such detection, the professor could enlist confederates, such as (other) lawyers, to open accounts on her behalf. However, if the bank is also required, as part of the client identification requirement, to determine the beneficial owner of the account, the bank could trace the account back to the professor. While the confederates could lie, this would, among other things, expose the confederate to criminal charges and make it more likely that the professor's criminal activities would be discovered.

An alternative would be for the professor to set up accounts in the names of companies and disguise the fact that she controlled the companies. However, if the bank were required to seek identification of the beneficial owner and controller of the company, the bank could, again, trace the account back to the professor. The professor could attempt to disguise this ownership though layers of companies, false shareholder or director names, etc., or even make identification harder by setting up the company in a foreign jurisdiction. In these instances where identification of the beneficial owner would be difficult, the bank could be required to see if the company had a legitimate purpose, and, if it did not, to file a SAR.

Eventually the professor would want to be able to use the money in the bank accounts without having to withdraw cash. This would mean that the professor would have to make relatively small payments from the account either to another single account (known as aggregation) to be used to make a purchase, such as an investment, or to make many payments directly for a purchase or an investment. In addition, if the bank is required to include as part of its client profile payments as well as deposits, these payments could also arouse suspicion. The bank would be required to inquire as to

> why the client was making such payments if they did not correspond to some obvious legitimate aspect of the client's daily life.
>
> In order to disguise aggregation or final payment, the professor might make payments to accounts held by a company set up for this purpose. Again, the bank's identification of beneficial owners or bona fides of the company could result in suspicion.
>
> Finally, once a bank is required to create a client profile and monitor transactions against that profile, non-cash deposits potentially representing proceeds of crime could also arouse suspicion.

In a nutshell, the requirements that banks and other financial institutions identify customers, establish client profiles, monitor for unusual transactions, and report to the authorities if they detect something that looks as if it involved the proceeds of crime is the foundation of the AML "preventive measures" standard. Once it is known to authorities that an account may contain the proceeds of crime, it would be possible to require the bank to freeze the account until its final province was adjudicated; if the contents turned out to be criminal proceeds, the money could be seized by the state.[56]

Of course, it would be necessary to sanction a financial institution that failed to follow these rules.[57] Sanctions could include criminal charges if the financial institution, or its employees, knew (or should have known) that it was assisting criminals in laundering proceeds of a predicate offense, which would require making money laundering a crime.[58] It could also include making AML rules part of the general set of prudential rules that the supervisors of financial institutions must implement,[59] even though, as noted above, they are not actually prudential in nature

56. Bruce Zagaris, *The Emergence of an International Anti-Money Laundering Regime: Implications for Counselling Businesses*, *in* THE ALLEGED TRANSNATIONAL CRIMINAL: THE SECOND BIENNIAL INTERNATIONAL CRIMINAL LAW SEMINAR 127, 204 (Richard D. Atkins ed. 1995).

57. *See, e.g.*, Economic Sanctions Enforcement Procedures for Banking Institutions, 71 Fed. Reg. 1971 (Jan. 12, 2006), *available at* http://www.treas.gov/offices/enforcement/ofac/legal/regs/fr71_1971.pdf.

58. *See, e.g.*, *The Bank Secrecy and the USA Patriot Act: Hearing Before the H. Committee on International Relations,* 108th Cong. (2004) (testimony of Herbert A. Biern, Senior Associate Director, Division of Banking Supervision and Regulation), *available at* http://www.federalreserve.gov/boarddocs /testimony/2004/20041117/default.htm (describing the United States' implementation of sanctions for violation of the Bank Secrecy Act, 31 U.S.C. 5311 et seq., and quoting the statement of Herbert A. Biern, Senior Associate Director, Division of Banking Supervision and Regulation).

59. *See* SCHOTT, *supra* note 38, at V-23 to -25.

(nor similar with respect to the overlapping interests of both regulator/supervisor and regulated).

It is easy to see why application of these principles would result in financial institutions and investigative authorities becoming interested in the Spitzer case, at least if key facts happened as they were presented in news reports. First, there were payments that were unusual in that they did not fit the client's profile. Secondly, there were payments that could indicate smurfing as well as attempts by an account holder to hide his identity and companies whose client profiles could not be identified. Finally, while identification of Spitzer's original account did not turn up a known criminal, it did turn up an important politician.

With respect to the charity-financing-of-terrorism example, there were none of these traits, except possibly one: if any of the account holders appeared to be known or suspected terrorists, then it would be a relatively simple task for the bank to report and for the authorities to investigate and act.

What should be clear from even a layman's perspective is that the transactions, when looked at together, do not really suggest laundering or corruption. In question were payments Governor Spitzer was making, not payments he was receiving; even a cursory investigation would show that he neither owned nor controlled the Emperors Club or its shell companies. If anything, he was making payments for something. It turned out to be sex. But why not terrorism?

II. ORIGINS OF GLOBAL AML EFFORTS

In order to counter money laundering, a number of countries, most notably the United States and France, took the lead in pressing for an international anti-money laundering effort. The first major international agreement to enact uniform anti-money laundering laws was the UN Convention Against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances (also called the Vienna Convention).[60] The convention required all parties to enact legislation providing for the identification and confiscation of laundered drug money and to set out procedures of mutual legal assistance in countering money laundering. In 1990, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime (Strasbourg Convention) was convened,[61] and the following year the first European Directive

60. *See generally* United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 20, 1988, I.L.M. 493, *available at* http://www.unodc.org/pdf/convention_1988_en.pdf. The original Treaty was adopted in 1988.

61. *See generally* Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Nov. 8, 1990, E.T.S. 141, *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/141.htm.

on the prevention of the use of the financial system for the purpose of money laundering was adopted.[62]

The next major international step to enhance global anti-money laundering efforts came with the creation of the Financial Action Task Force in 1989, following the G-7 Summit in Paris.[63] The original task force consisted of sixteen member countries of the Organization for Economic Co-operation and Development ("OECD"), with the United States and France taking leadership roles.[64] The task force was inter-governmental in nature, with members represented by financial supervisors, criminal investigators, and prosecutors.[65] While it had a small secretariat, the work of the FATF was originally carried on almost entirely by its members. Less than a year later the FATF published its first set of 40 Recommendations, which were designed to provide a comprehensive plan of action for fighting money laundering and which looked somewhat like an AML standard. Drafted primarily by the United States, the Recommendations covered the criminalization of money laundering, the freezing and seizing of criminal proceeds, and the key preventive measures for financial institutions, such as customer identification and record keeping, transaction monitoring, and the filing of SARs when a financial institution suspected money laundering. They also required cross-border cooperation in investigating and prosecuting money laundering.

In 1991, the FATF began its program of annual compliance self-evaluations, requiring the completion of a questionnaire and participation in its mutual evaluation program.[66] The mutual evaluations involved on-site assessments of compliance with the Recommendations, undertaken by experts drawn from other member nations. The following year, FATF helped set up the Caribbean Financial Action Task Force ("CFATF"), the first FATF-style regional body designed to advance adoption of the FATF 40.[67] While membership in regional bodies required a political commitment to implement the FATF 40 and to undergo mutual evaluations, no treaty obligation was involved and no timetable was

62. Council Directive 91/308/EEC of 10 July 1991, OJ L 166 (July 28, 1991).

63. FINANCIAL ACTION TASK FORCE, ABOUT THE FATF, http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html, (last visited Sept. 1, 2008) [hereinafter *About the FATF*].

64. *Id.*

65. FINANCIAL ACTION TASK FORCE, WHAT IS THE FATF?, http://www.fatf-gafi.org/document/57/0,3343,en_32250379_32235720_34432121_1_1_1_1,00.html (last visited July 28, 2008) [hereinafter *What is the FATF*].

66. *See* FINANCIAL ACTION TASK FORCE, FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING ANNUAL REPORT 1991–1992 (1992), *available at* http://www.oecd.org/dataoecd/63/39/35752730.pdf.

67. *See* FINANCIAL ACTION TASK FORCE, FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING ANNUAL REPORT 1992–1993 5, 4 (1992), *available at* http://www.oecd.org/dataoecd/13/61/34325384.pdf.

set for implementation.[68]

The FATF also worked on developing appropriate "countermeasures" to those jurisdictions that failed adequately to implement anti-money laundering policies.[69] Additionally, the FATF expanded its membership to include twenty-four members of the OECD, plus Hong Kong, Singapore, and representatives of the European Commission and the Gulf Co-operation Council.[70]

In 1996, a revised version of the 40 Recommendations was completed which extended AML preventive measures to non-bank financial institutions.[71] In addition, the Asia-Pacific Group on Money Laundering, a FATF-style regional body, was formed, and the mutual evaluation procedures of the CFATF and the Offshore Group of Banking Supervisors were assessed as being in conformity with the FATF's principles.[72] It also agreed to apply "preliminary *sanctions* against certain [FATF] members" that did not comply with the 40 Recommendations. (Note that the word "countermeasures" was not used.).[73] In 1997, with the creation of the Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (then known as the PC-R-EV), the European Council's FATF-style regional body,[74] such anti-money laundering regional organizations existed for nearly every significant financial center.[75]

During the early 1990s, FATF members expressed concern about jurisdictions they believed were key weak links in enforcing anti-money laundering rules.[76] At that time many onshore

68. *See generally* CARIBBEAN FINANCIAL TASK FORCE, CFATF: AN OVERVIEW, *available at* http://www.cfatf.org. The "uncommitted" commitment to implement the FATF 40 was discussed at a number of CFTAT meetings and later at APF and PC-R-EV meetings, which were the former acronyms to describe a committee of experts on anti-money laundering. *Id.*

69. BAHAMAS FINANCIAL SERVICES BOARD, FATF COUNTER MEASURES FOR NON-COOPERATIVE COUNTRIES AND TERRITORIES, Mar. 11, 2003, http://www.bfsb-bahamas.com/news_detail.lasso?id=33782.

70. *See* ABOUT THE FATF, *supra* note 63.

71. FATF 40, *supra* note 38, at 3.

72. FINANCIAL ACTION TASK FORCE, FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING ANNUAL REPORT 1996–1997, *available at* http://www.jya.com/fatf96-97.htm.

73. *Id*.

74. COUNCIL OF EUROPE, MONEYVAL, WHAT ARE MONEYVAL'S OBJECTIVES?, http://www.coe.int/t/dghl/monitoring/moneyval/About/MONEYVAL_in_brief_en.asp (last visited Sept. 1, 2008).

75. This committee (now Moneyval) includes the vast majority of Eastern European states, in addition to the Asia/Pacific Groups on Money Laundering, the Caribbean Financial Action Task Force, the Eastern and Southern Africa Anti-Money Laundering Group, the Eurasian Group, Middle East and North African FATF, the West African Group, and the Financial Action Task Force on Money Laundering in South America. The Wolfsberg Group of Banks, Commonwealth Secretariat, and Organization of American States (CICAD) further buttressed the regional anti-money laundering organizations. *Id.*

76. J.C. SHARMAN, THE GLOBAL ANTI-MONEY LAUNDERING REGIME AND DEVELOPING COUNTRIES: DAMNED IF THEY DO, DAMNED IF THEY

jurisdictions, including almost all poorer or developing countries, had little or no enforcement of AML rules.[77] However, it was the role played by some key offshore jurisdictions that was frequently mentioned as the most troublesome.[78] The 1996 FATF 40 included FATF 21, which stated that financial institutions should give heightened due diligence to business relations and transactions with persons from jurisdictions that "do not or insufficiently apply [the] Recommendations."[79] Such heightened due diligence could result in a financial institution refusing to undertake transactions with a person from a non-complying jurisdiction, but the Recommendation was vague on this issue.[80]

III. THE ADDITION OF CFT

Following the attacks of September 11, 2001, the U.S. Treasury Department began immediately to push other members of the FATF to include terrorism financing as a central part of the organization's mandate.[81] On October 29th and 30th, the FATF, meeting in an extraordinary plenary session in Washington, adopted eight new recommendations on terrorist financing.[82] However, that the financing of terrorism should be tied to anti-money laundering was, by no means, obvious. While terrorism had existed before 9/11, the original FATF 40 made no reference to it.[83] As discussed, AMLs 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, which could be as simple as charitable donations, but rather a criminal destination: terrorism.

Of course, there were some connections. As noted, identifying exactly who the financial institution's clients were was a key aspect

DON'T? 14 (working paper presented at the International Studies Association Annual Conference Mar. 22–25, 2006), *available at* http://www.allacademic.com//meta/p_mla_apa_research_citation/1/0/0/7/5/pages100752/p100752-1.php.

77. *Id*.

78. *Id.*

79. FATF 40, *supra* note 38, at 5.

80. For further discussion of this issue, see Benjamin R. Hartman, *Coercing Cooperation from Offshore Financial Centers: Identity and Coincidence of International Obligations Against Money Laundering and Harmful Tax Competition*, B.C. INT'L & COMP. L. REV. 255, 273–278 (2001), *available at* http://www.bc.edu/schools/law/lawreviews/meta-elements/journals/bciclr/24_2/02_FMS.htm.

81. *See* SHARMAN, *supra* note 79, at 4.

82. *HM Treasury Welcomes Tough New Measures to Tackle Terrorist Financing*, HM TREASURY, Oct. 31, 2001, http://www.hm-treasury.gov.uk/newsroom_and_speeches/press/2001/press_118_01.cfm.

83. FATF 40, *supra* note 38.

of AML preventive measures.[84] These measures could also be used to identify whether the client was a terrorist, providing of course that the financial institution or the authorities knew who the terrorists were. This proved to be a valuable avenue for CFT measures.

Even before the September 11th attacks, the United Nations 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.[85] The committee created a consolidated list of entities and officials associated with these organizations as submitted by members. Subsequent resolutions strengthened this original commitment.[86] Resolution 1373, passed as a result of the September 11th attacks, extended the requirement of states to freeze accounts to terrorists other than al-Qaeda and the Taliban.[87] The UN General Assembly had also adopted a UN Convention on suppression of terrorism financing, although it did not go into force until April of 2002.[88] 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."[89] Assuming that someone could

84. *See* WOLFSBERG AML PRINCIPLES, *supra* note 46.

85. S.C. Res. 1267, para. 4, U.N. Doc. S/RES/1267 (Oct. 15, 1999), *available at* http://www.un.org/sc/committees/1267/.

86. *Id.* (including links to the relevant Security Council Resolutions).

87. S.C. Res. 1373, para. 1, U.N. Doc. S/RES/1373 (Sept. 28, 2001), *available at* http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement.

88. Ctr. for Nonproliferation Studies, International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, *available at* http://www.nti.org/e_research/official_docs/inventory/pdfs/finterr.pdf.

89. G.A. Res. 109, art. 8, U.N. Doc. A.54/49 (Dec. 9, 1999), *available at* http://www1.umn.edu/humanrts/instree/financingterrorism.html. The Treaty defined terrorism as acts described in any treaty in the Annex, and "[a]ny 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.* at 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.* at Annex; *see also* G.A. Res. 164, art. 2(1), U.N. GAOR, 52nd Sess. (May 23, 2001) (defining terrorist bombings as the bombings of state or government facilities, forms of public transportation, or other aspects of the public infrastructure). With certain limited exceptions in each convention, the terrorists must be

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.

The first Special Recommendation of the convention requires each jurisdiction to take immediate steps to ratify and to implement fully the 1999 UN Convention for the Suppression of the Financing of Terrorism and to implement the Security Council resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly UN Security Council Resolution 1373.[90] Special Recommendation III specifically requires that each jurisdiction freeze funds or other assets of terrorists, those who finance terrorism, and terrorist organizations, according to UN resolutions and generally.[91] Special Recommendation II requires each jurisdiction to criminalize the financing of terrorism, terrorist acts, and terrorist organizations, and to ensure that such offenses are designated as money-laundering predicate offenses.[92] In other words, knowingly laundering any proceeds from terrorism would constitute the crime of money laundering, although one would normally expect that the vast majority of jurisdictions would view terrorism as a serious crime and therefore already a predicate offense to money laundering.[93]

The proposed regime certainly could generate problems with respect to implementation. First, maintaining an up-to-date list of known terrorists could be difficult, even if the final list applicable to domestic financial institutions was to be undertaken by a domestic governmental authority. Certainly errors can arise in putting together the list at both an international and a local level, and even a brief freezing of a person's bank account can cause serious damage.[94] Next, there may be many people or organizations with the same name; it may be hard for financial institutions to ensure that their procedures identify the correct persons, legal or physical. Other problems could arise for financial institutions depending on how the general recommendations were to be translated into rules

nationals of a different state than the state in which the terrorist act took place.

90. FATF SPECIAL IX, *supra* note 38, at 1.

91. *Id.*

92. *Id.*

93. It was discussed at the time that some countries, for example, the United States, that use a specific list of offenses as predicates for the crime of money laundering (rather than something more general like "all serious crimes") might not have thought to include terrorism. CHARLES DOYLE, CRIMINAL MONEY LAUNDERING LEGISLATION IN THE 109TH CONGRESS (2006), *available at* http://www.house.gov/gallegly/issues/crime/crimedocs/RS22400.pdf.

94. Also, procedures for removal from the U.S. Sanction's Monitoring Committee list can be problematic. *See* Nicole Nice-Petersen, *Justice for the "Designated": The Process That is Due to Alleged U.S. Financiers of Terrorism*, 93 GEO. L.J. 1387, 1406–09 (2005); Jennifer R. White, *IEEPA's Override Authority: Potential for a Violation of the Geneva Convention's Right to Access for Humanitarian Organizations?*, 104 MICH. L. REV. 2019, 2024–26 (2006).

in domestic legislation, rules that will be discussed infra. However, in general at least, these rules, which one attendee at the Special Meeting referred to as the "Christmas Rules" ("He's making a list/ Checking it twice/ Gonna find out/ Who's naughty and nice"),[95] were relatively straightforward.[96]

However, the proposed new CFT regime required more. Financial institutions were already required to profile clients and monitor their transactions to see if the proceeds of crime or money laundering were involved and, if appropriate, to report a suspicious transaction to the government. Then, perhaps, the financial institution could also profile clients and monitor transactions to see if they might have some involvement in the financing of terrorism and report those cases as well. This is exactly what new Special Recommendation IV did when it required that financial institutions extend suspicious transaction/activity-reporting requirements to terrorism financing.[97]

Interestingly, a question arose at the FATF Special Meeting as to why only the financing of *terrorism* should be included, rather than the financing of other serious crimes. One participant in the FATF meeting noted that "under the proposed rule, if I plan to use my bank account to buy bullets to kill my wife the bank need not care, but if I plan to use the account to buy bullets to threaten a local politician they need to report me."[98]

The FATF Special meeting added three other specific Special Recommendations of interest to financial institutions. They were: Special Recommendation VI, which required alternative remittance systems (i.e. those that are not part of the regulated financial system) to be brought into the regulatory system;[99] Special Recommendation VII,[100] which provided new rules on information transmitted with funds transfers; and Special Recommendation

95. J. FRED COOTS & HENRY GILLESPIE, SANTA CLAUS IS COMING TO TOWN (1934), *available at* http://www.the-north-pole.com/carols/santacome.html.

96. For an overview of the work and procedure of the 1267 Committee, see Eric Rosand, *The Security Council's Efforts to Monitor the Implementation of Al Qaeda/Taliban Sanctions*, 98 AM. J. INT'L. L. 745, 747–753 (2004). The author rightly emphasized the "delicate balance that needs to be struck between having an expedited listing process to ensure that legitimate targets do not escape sanctions, and putting minimum evidentiary standards and a transparent listing process into place to ensure that due process and other human rights standards are respected." *Id.* at 750; *see also* BARDO FASSBENDER, TARGETED SANCTIONS AND DUE PROCESS, STUDY COMMISSIONED BY THE UNITED NATIONS OFFICE OF LEGAL AFFAIRS (2006), *available at* http://www.un.org/law/counsel/Fassbender_study.pdf (discussing concerns over due process rights over specific targeted sanctions).

97. *See* FATF SPECIAL IX, *supra* note 38.

98. *See* G.A. Res. 109, *supra* note 89.

99. *See* FATF SPECIAL IX, *supra* note 38, at 2.

100. *Id.*

VIII,[101] which noted that charities can be particularly vulnerable to terrorism financing and required countries to ensure that charities are not so misused, an observation based primarily on a number of prosecutions brought by law enforcement where primarily Islamic charities had appeared to finance terrorists.

Special Recommendation VIII was not specifically directed to financial institutions. Rather, it required that governments review rules to ensure that nonprofits were not being "misused" by terrorist organizations posing as legitimate entities and that they "ensure" that nonprofits were not being used for clandestine diversion of funds.[102] In other words, Special Recommendation VIII had nothing specifically to do with the financial system: It looked as if it had primarily to do with the regulation of charities, similar to the example discussed earlier in this Article. But Special Recommendation VIII did suggest that charities may be among the more likely terrorism-financing culprits.[103] For this reason, it could be that financial institutions should focus at least some of their suspicious-activity monitoring on this type of client, as they already did for politicians. However, if in fact most charities made payments directly to other charities without following particular patterns that suggested a heightened risk of terrorism financing, then it would be difficult for financial institutions to determine when a transaction was actually suspicious and when to file a SAR with a government agency.

IV. DETAILS ON THE GLOBAL AML/CFT STANDARD

In order to understand the magnitude of the task devolved by the FATF Special Meeting on financial institutions,[104] it is necessary to take a more detailed look at the preventive measures briefly outlined above and how they are implemented in practice.

As noted earlier, before the adoption of the Special Recommendations in 2001, the FATF 40 established a process or strategy through which financial institutions and government authorities would play a role in identifying proceeds of crime.[105] In essence, financial institutions are required to identify clients, create client profiles, monitor transactions, and report suspicious activity to government authorities, who then identify cases from those reports for further investigation, and, if necessary, issue orders for

101. *Id.*

102. *Id.*

103. FINANCIAL ACTION TASK FORCE, INTERPRETATIVE NOTE TO SPECIAL RECOMMENDATION VIII: NON-PROFIT ORGANISATIONS, *available at* http://www.oecd.org/dataoecd/43/5/38816530.pdf.

104. *See supra* note 38 and accompanying text. Following adoption of Special Recommendation VIII by the FATF, the recommendations became part of the international standard. *Id.*

105. *Id.*

freezing the suspected proceeds of crime. Within this overall strategy, financial institutions are tasked specifically with *implementing* systems to detect suspicious or unusual transactions or funds, examining them, and reporting those they suspect are results of the proceeds of crime.[106] This Article refers to this requirement as the "detection, examination, and reporting system."

Key to this overall strategy are the Financial Intelligence Units ("FIUs"), a role played in the United States by FinCEN, noted earlier in the discussion of the Spitzer case. FinCEN serves as a national center for receiving, analyzing, and disseminating SARs, along with other information regarding potential money laundering (and now terrorism financing).[107] The FIU should also have access to other financial, administrative, and law enforcement information so that it can analyze SARs.[108] Actually, FinCEN operates slightly differently than the FIUs of most other countries in that it disseminates essentially all SARs to law enforcement authorities, who then conduct investigations with the assistance of FinCEN.[109]

The FIU and other authorities that investigate possible crimes are tasked with identifying what they believe *actually are* criminal proceeds, that is, with the level of certainty required by the domestic justice systems for asset seizure/confiscation/criminal prosecution, along with supporting evidence.[110] This second, or criminal investigation system, may build on information provided by the detection, examination, and reporting systems, but extends far beyond it.

In effect, the combined strategy outsources some aspects of law enforcement from the criminal investigation system to financial institutions,[111] turning financial institutions into (unpaid) agents of the criminal justice system.

106. FATF 40, *supra* note 38, at 6, 27.

107. FINCEN, WHAT WE DO, http://www.fincen.gov/about_fincen/wwd/index.html (last visited Sept. 7, 2008) [hereinafter WHAT WE DO].

108. *See* FATF 40, *supra* note 38, at 8.

109. MUTUAL EVALUATION REPORT, *supra* note 44, at 60; s*ee also* WHAT WE DO, *supra* note 107.

110. Depending on the jurisdiction, different levels of proof may be required for confiscation of criminal proceeds and for conviction of persons for the crime of money laundering. Temporary or provisional measures such as freezing or seizing assets typically do not require full judicial process. INTERNATIONAL MONETARY FUND, MEXICO: REPORT ON THE OBSERVANCE OF STANDARDS AND CODES—FATF RECOMMENDATIONS FOR ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (2005), *available at* http://www.imf.org/external/pubs/ft/scr/2005/cr05436.pdf.

111. Such outsourcing is described by some authors as "horizontal subsidiarity." *See, e.g.*, WOLFGANG H. REINICKE, GLOBAL PUBLIC POLICY: GOVERNING WITHOUT GOVERNMENT 89–90 (1998) (discussing issues related to assigning public-sector tasks to private-sector actors).

V. DETECTION, EXAMINATION, AND REPORTING SYSTEM

FATF Recommendations 5, 11, and 13 (and the accompanying relevant materials in the accompanying "Methodology" for assessment of compliance) set out the detection, examination, and reporting systems for financial institutions.[112] These consist of requirements for customer due diligence, including customer identification (FATF 5), customer transaction monitoring (first part of FATF 11), transaction examination (second part of FATF 11), and suspicious transaction reporting (FATF 13).[113]

FATF 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 customer.[114] The methodology allows an exception from this latter requirement in the event the legal person is a public company.[115] Financial institutions must also understand the purpose, intended relationship, and conduct with the customer, and undergo ongoing customer due diligence (as HSBC failed to do with respect to QAT International and QAT Consulting Group) in the business relationship, and "scrutiny of transactions undertaken through the course of the 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."[116] In the event the financial institution cannot comply, it should terminate business relations or not undertake a transaction and should "consider" filing a SAR.[117]

The United States complies with these requirements through statutory and regulatory measures,[118] as well as through guidance

112. *See* FATF 40, *supra* note 38, at 2–3, 5.
113. *Id.*
114. *Id.* at 2–3.
115. FATF METHODOLOGY, *supra* note 38, at 13.
116. FATF 40, *supra* note 38, at 3.
117. *Id.* at 3.
118. There have been customer identification rules in effect for banks and similar financial institutions in the U.S. since 1983. *See* MUTUAL EVALUATION REPORT, *supra* note 44, at 95–96; M. MAUREEN MURPHY, CRS REPORT FOR CONGRESS: INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001, TITLE III OF PUB. L. NO. 107-56, 2–4 (2001), *available at* http://epic.org/privacy/financial/RL31208.pdf. Title III of the Patriot Act of 2001, entitled "International Money Laundering Abatement and Anti-terrorist Financing Act of 2001," updated and enhanced these measures by adding several new provisions to the Bank Secrecy Act ("BSA"). 31 U.S.C. § 5311 (2001). Section 326 of the Act provides for the Secretary of the Treasury to promulgate regulations on customer identification, and requires financial institutions to implement reasonable procedures for (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the

outlined in materials used by supervisors in their examinations of financial institutions and compliance with statutory and regulatory provisions. The most recent of these is the Bank Secrecy Act/Anti-Money Laundering Examination Manual,[119] which applies to financial institutions that are banks or bank-like institutions,[120] and where guidance on customer identification[121] and on transaction monitoring are spelled out in greater detail.[122]

FATF 5 also allows financial institutions to determine the "extent of such measures on a risk-sensitive basis, depending on the type of customer, business relationship or transaction," with higher risk categories requiring enhanced due diligence.[123] The methodology goes on to provide certain examples of higher risk categories,[124] which include non-resident customers, private banking, and legal persons or arrangements that are personal-asset holding vehicles, such as QAT International and QAT Consulting Group.[125] FATF 6 goes further and requires that financial institutions have risk management systems to determine if customers are politically-exposed persons, defined as individuals who are or have been entrusted with prominent public functions in a foreign country

person's identity, including name, address, and other identifying information; and (3) determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency. The final regulations on customer identification are found in 31 C.F.R. § 103.121 (2007). 31 U.S.C. § 5314(h) authorizes the Secretary of the Treasury to require financial institutions to report suspicious transactions. It is implemented at 21 C.F.R. § 21.11. There are similar customer identification rules for securities broker-dealers, mutual funds, and futures commission merchants and introducing brokers in commodities. 31 CFR § 103.122 (2007); 31 CFR § 103.131 (2007); s*ee also* ASD Notice to Members 02-21, pages 5–7 (2002); NASD Notice to Members 03-34 (2003). Under 31 CFR § 103.137(c) (2007), 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."

119. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL (2006), *available at* http://www.ffiec.gov/pdf/bsa_aml_examination_manual2006.pdf [hereinafter FFIEC MANUAL].

120. This refers to those financial institutions supervised and examined by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. The Manual also used by the Conference of State Bank Supervisors, the American Council of State Savings Supervisors, and the National Association of State Credit Union Supervisors. *See* FFIEC, ABOUT THE FFIEC, http://www.ffiec.gov/about.htm (last visited Sept. 7, 2008).

121. *See* FFIEC MANUAL, *supra* note 119, at 18–34, 45–59, 120–25, 265–68.

122. *Id.* at 60–76, 149–60, F1–F9, L1–L2.

123. FATF 40, *supra* note 38, at 2.

124. These are derived from the BASEL COMMITTEE ON BANKING SUPERVISION, CUSTOMER DUE DILIGENCE FOR BANKS 6 (2001), *available at* http://www.bis.org/publ/bcbs85.pdf.

125. FATF METHODOLOGY, *supra* note 38, at 14.

(although countries are encouraged to extend this to domestic officials), as well as (in effect) family members or "close associates" of politically-exposed persons.[126] The recommendation further requires that financial institutions take reasonable measures to establish the "source of wealth and source of funds" and conduct enhanced ongoing monitoring of the business relationship.[127] The United States has put in place similar rules.[128] In particular, while United States guidance documents require financial institutions to undertake heightened due diligence when clients are politically exposed persons, this group only includes "foreign" persons.[129] Eliot Spitzer would not be a politically exposed person under this standard.

FATF 11 requires that financial institutions pay "special" attention to complex and unusually large or unusual patterns of transactions with no "apparent" economic or visible lawful purpose, examine "as far as possible" the background and purpose of such transactions, and establish "the findings" in writing.[130] Interestingly, this requirement is separate from Recommendation 5(c)'s requirement for ongoing customer due diligence with respect to "scrutiny of transactions."[131] FATF 13 requires that a financial institution report promptly to the financial intelligence unit if it suspects, or has reasonable grounds to suspect, that funds are the proceeds of a criminal activity, which the methodology further defines as filing a SAR.[132] Again, U.S. rules comply with these requirements.[133]

With the exception of the addition of the reference to risk-based systems (including politically exposed persons), the customer due diligence and transaction monitoring and suspicious transaction reporting requirements in the FATF Preventive Measures differ little from those in the previous version adopted in 1996. Although the three recommendations (and their counterparts in U.S. rules) do not say so explicitly or in so many words, they form a system[134]

126. *Id.* at 81.

127. FATF 40, *supra* note 38, at 3–4.

128. The United States has adopted a risk-based system. *See, e.g.*, FFIEC MANUAL, *supra* note 119, at 11–27, I-1, K-1, M-1 to -2.

129. *Id.* at 21, 118–22, 261–64. Section 312 of the U.S. Patriot Act requires institutions to establish special due-diligence procedures with respect to private banking accounts held by, or on behalf of, a non-U.S. person. *Id.*

130. FATF 40, *supra* note 38, at 5.

131. *Id.* at 3.

132. *I*d. at 5.

133. 31 CFR § 103.18 to .19 (2007) (setting forth U.S. rules on investigation and reporting).

134. A working group consisting of the Commonwealth Secretariat, the UNODCP, the World Bank, and the IMF has been engaged in drafting a model regulation for the prevention of money laundering and the financing of terrorism ("Model Regulation"). The most recent draft of the Model Regulation implements, *inter alia*, FATF 4 through 2, and is based on the regulatory

whereby financial institutions must (1) identify customers (and the beneficial owner if different); (2) establish and maintain an up-to-date customer profile;[135] (3) monitor transactions to see if they fit with the customer profile; (4) if not, examine the transaction to see if it might represent the proceeds of crime, including by examining the source of funds; and (5) if so, report the transaction to the financial intelligence unit (along with a description of why the financial institution believes that the transaction is suspicious).

In implementing these five steps, financial institutions may use a risk-based system (in the United States they *must* use such a system) applying enhanced customer due diligence to higher risk customers and reduced customer due diligence to lower risk customers.[136]

However, the recommendations do not give guidance as to exactly how far, and with what criteria, financial institutions should go in implementing Steps 1 through 4 above, and when they should file a SAR under Step 5. And, although there are many places within the Federal Financial Institutions Examination Council ("FFIEC") Manual where helpful "flags" are given as to what would constitute a possible need for heightened scrutiny,[137] there is no guidance there either as to exactly how far, and using what criteria, financial institutions should go.

As one can readily imagine, this creates a serious problem for implementation. Suspicious transactions will nearly always have relatively different risk rankings (i.e. the degrees of likelihood that criminal proceeds are involved), and suspicious transactions will tend to differ with respect to the total amount of criminal proceeds involved. In short, the FATF Preventive Measures do not describe with any precision at what point on the risk continuum financial institutions should identify suspicious transactions (i.e., the continuum stretching from all transactions about which a financial

frameworks in the UK, Canada, Australia, Hong Kong SAR, and a number of other Commonwealth countries. 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 Financial Market Integrity, the World Bank). 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.*

135. Presumably, if the customer profile suggests that proceeds of crime are involved, the financial institution should go directly to Step 4.

136. FINANCIAL ACTION TASK FORCE, GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING 2, *available at* http://www.oecd.org/dataoecd/43/46/38960576.pdf [hereinafter FATF GUIDANCE].

137. *See, e.g.*, FFIEC MANUAL, *supra* note 119, at 61.

institution may have any suspicion at all to those for which financial institutions have a very strong suspicion).

Also, the FATF Preventive Measures do not provide guidance as to whether financial institutions should consider all transactions equally, regardless of the size of the suspected criminal proceeds, or whether they should focus on transactions with relatively larger amounts of suspected criminal proceeds. The wording of the recommendations themselves includes a number of terms that are not easily defined in practice and therefore add significantly to the problem. For example, what are "reasonable measures" when it comes to identifying a beneficial owner/controller? How detailed must a "risk profile" be, and when will it be "necessary" to identify the source of funds? With respect to politically exposed persons, what are "reasonable measures" to establish the source of wealth and source of funds, and what constitutes "enhanced" monitoring? What does it mean to examine "as far as possible" the "background" and "purpose" of unusual transactions? Again, there is little help in the FFIEC Manual.

VI. CRIMINAL INVESTIGATION SYSTEM

Even with its shortcomings, the discussion in the FATF 40 of the detection, examination, and reporting system is considerably more developed than that of the criminal investigations system. While many of the Recommendations discuss the tools that should be available for investigations, there is very little discussion of exactly what the FIUs or investigating authorities should do. The FATF 26 states only that an FIU should be a "national centre for receiving (and as permitted, requesting), analysis, and dissemination of a suspicious activity/transaction report and other information regarding money laundering or terrorist financing."[138] FinCEN appears to have insufficient direction as to its exact role in the detection, examination, and reporting system, much like the insufficient direction as to where the role of financial institutions should end and FinCEN and government investigators should begin.[139]

A. Development and Implementation of Preventive Measures

Under the FATF Preventive Measures, financial institutions must develop (and implement) their own systems to carry out their detection, examination, and reporting requirements.[140] As part of

138. The methodology goes on to reference the Egmont Group Statement of Purpose, which adds little to what is found in Recommendation 26 and does not discuss what "analysis" means or how the financial institution's detection and reporting of a suspicious transaction differ from a FIU's "analysis" of the transaction. FATF 40, *supra* note 38, at 8.

139. *See* MUTUAL EVALUATION REPORT, *supra* note 44, at 60–67.

140. *See, e.g.*, FATF 40, *supra* note 38, at 8.

the five basic steps of the detection, examination, and reporting system, financial institutions need to develop ways of identifying types of customers and types of transactions that, in addition to being "unusual," indicate a higher risk for the generation of criminal proceeds.[141] Financial institutions must develop systems that they believe will bear fruit in identifying transactions that are more likely to suggest criminal proceeds than others. However, the principle business of financial institutions is not criminal law enforcement. There are a number of ways that financial institutions try to fulfill their obligations in this regard.

B. Methods, Trends, and Typologies

Money laundering methods, trends, and typologies have emerged as key tools for financial institutions to implement their AML duties under the FATF Recommendations. At least in theory, typologies describe typical tactics used by launderers or patterns that indicate a higher risk of laundering. Special typologies are often described for different categories of criminals or types of criminal proceeds. Typologies (and other guidance with respect to identifying laundering) are produced and published by the FATF, FATF-Style Regional Bodies ("FSRBs")[142] and national competent authorities, especially FIUs. While these typologies and other information provide some guidance, according to surveys of financial institutions, they believe the information provided to be extremely general and therefore of little use in identifying transactions that are of a *materially higher risk* than other transactions. Therefore, the recommendations do not provide sufficient assistance to financial institutions designing and implementing their risk-based preventive measures requirements.[143] As the European Commission noted, the AML and CFT systems can only work if (among other

141. FATF GUIDANCE, *supra* note 136, at 3.

142. *See, e.g.*, FINANCIAL ACTION TASK FORCE, FATF METHODS & TRENDS, *available at* http://www.oecd.org/pages/0,3417,en_32250379_32237277_1_1_1_1_1,00.html; FINANCIAL ACTION TASK FORCE, REPORT ON MONEY LAUNDERING TYPOLOGIES 2003-2004, 19–23, *available at* http://www.fatf-gafi.org/dataoecd/19/11/33624379.pdf (discussing Politically Exposes Persons ("PEPs")); FINANCIAL ACTION TASK FORCE, REPORT ON MONEY LAUNDERING TYPOLOGIES 2001-2002, 12–14, *available at* http://www.fatf-gafi.org/dataoecd/29/35/34038006.pdf (discussing corruption and private banking).

143. MATTHEW H. FLEMING, UK LAW ENFORCEMENT AGENCY USE AND MANAGEMENT OF SARS: TOWARDS DETERMINING THE VALUE OF THE REGIME 55, 59–60 (2005), *available at* http://www.jdi.ucl.ac.uk/downloads/publications/research_reports/Fleming_LEA_Use_and_Mgmt_of_SARs_June2005.pdf (noting that there is a perception among financial institutions in Australia, the U.S., the U.K., France, and other OECD countries that there is little useful information provided by domestic financial intelligence units to financial institutions, especially with respect to identifying typologies, including new money laundering techniques, trends within existing techniques, and the relative identification of more prominent typologies).

things) financial institutions have expertise to carry out the first risk analysis.[144]

C. Feedback from Financial Intelligence Units and Other Government Agencies

These problems are seriously compounded because of the critical lack of feedback from FIUs (or other parts of the criminal investigations system) to financial institutions as to any aspect of the SAR systems. As discussed above, financial institutions rely on money laundering typologies to help design their AML systems. However, except in very rare cases, financial institutions report that they are not told if a SAR has resulted in a real positive, let alone what aspects of the report were useful to the FIU (or other part of the criminal investigations system) in identifying criminals or criminal proceeds.[145] Without such information, financial institutions can only guess to what degree they are successful in identifying suspicious transactions.

D. Costs

While public sector investigative duties are normally financed through general revenues, financial institutions' detection, examination, and reporting duties must normally be financed by increasing prices the institutions charge clients, reducing net profits, or (most probably) a mix of the two. Higher financial institution prices can have significant and adverse public policy effects, such as decreasing access to financial services by low income clients.[146] Reports suggest that financial institution costs in implementing preventive measures have been increasing significantly.[147]

Also, assuming that increasingly onerous detection, examination, and reporting duties are likely to increase financial institutions' marginal costs, a conflict of interest arises between the

144. EUROPEAN COMMISSION, DIRECTORATE-GENERAL JUSTICE FREEDOM AND SECURITY, FINAL REPORT 30 (2007), *available at* http://ec.europa.eu/justice_home/doc_centre/terrorism/docs/report_01_02_07_with_appendix_en.pdf.

145. *See, e.g.*, *id.* at 53 (indicating that financial institutions want to know which suspicious activity/transaction reports were helpful and why).

146. *See generally* JENNIFER ISERN & DAVID PORTEOUS, AML/CFT REGULATION: IMPLICATIONS FOR FINANCIAL SERVICE PROVIDERS THAT SERVE LOW-INCOME PEOPLE (2005) (discussing, *inter alia*, how increased costs due to implementation of AML/CFT regulations may reduce the supply of affordable financial services to low-income persons).

147. Alan E. Sorcher, *Lost in Implementation: Financial Institutions Face Challenges Complying with Anti-Money Laundering Laws*, 18 TRANSNAT'L L. 395, 396 (2005) (noting that banks have significantly increased their spending on AML/CFT procedures); KPMG INTERNATIONAL, GLOBAL ANTI-MONEY LAUNDERING SURVEY 2004: HOW BANKS ARE FACING UP TO THE CHALLENGE 11 (2004), *available at* http://www.us.kpmg.com/microsite/FSLibraryDotCom/docs/AML%20A4_web%2017%20Sept.pdf.

financial institution as the "agent" and the criminal investigations system as the "principal." While FATF 40 does not suggest that financial institutions should be compensated for implementing their agency duties, FATF 23 states that jurisdictions must require financial institutions to implement their detection, examination, and reporting duties through their regular prudential processes with attendant supervisory sanctions applied in the event of a breach.[148]

VII. THE CURRENT SITUATION

Exactly how such a system of incentives is implemented has a significant effect on results. From the perspective of financial institutions, these requirements are very serious, even if they are not well spelled out. FATF 17 requires the imposition of "effective, proportionate and dissuasive sanctions" to deal with natural or legal persons who fail to comply with anti-money laundering or terrorist-financing requirements.[149] FATF 29 specifically states that supervisors of financial institutions "should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing . . ."[150] United States laws comply,[151] and significant fines, as well as other supervisory and regulatory orders against financial institutions, have resulted.[152]

In addition to other possibly adverse effects, if a financial institution is usually sanctioned only for failure to report suspicious transactions (false negatives) and not for reporting too many that do not turn out to be suspicious (false positives), there will be an

148. Under FATF 1 and 2, a financial institution's extensive failure to implement its detection, examination, and reporting duties could result in a charge with the crime of money laundering itself. FATF 40, *supra* note 38, at 1–2. Financial institutions will have a financial incentive to reduce their detection, examination, and reporting costs through a reduction in detection, examination, and reporting duties up to the point of the cost of sanctions (which will include not only monetary sanctions but the cost of any resulting adverse effect on reputation). On the other hand, the criminal investigations system will have an incentive to require their agent financial institutions to carry as great a detection, examination, and reporting burden as is allowed by the enforcement system. *Id.*

149. FATF 40, *supra* note 38, at 6.

150. *Id.* at 9.

151. MUTUAL EVALUATION REPORT, *supra* note 44, at 164–90.

152. *See, e.g.*, U.S. Cease and Desist Order and Order of Assessment of a Civil Money Penalty, In the Matter of American Express Bank International, No. 07-017-B-EC (Bd. of Governors of the Fed. Reserve Syst. Aug. 6, 2007), http://www.federalreserve.gov/newsevents/press/enforcement/enf20070806a1.pdf; U.S. Assessment of Civil Money Penalty, In the Matter of Union Bank of California No. 2007–02 (Dep't of Treasury 2007), *available at* http://www.fincen.gov/news_room/ea/files/ASSESSMENT_In_the_Matter_of_Union_Bank_of_California.pdf; Deferred Prosecution Agreement, U.S.A. Banco Popular de Puerto Rico (D.P.R. 2003), *available at* http://www.fincen.gov/news_room/ea/files/bancopopular.pdf.

incentive for financial institutions to apply too little scrutiny and to over-report.[153] Currently, in many key jurisdictions, there have been considerable increases in SAR reporting, even though costs, as noted above, have also increased.[154] Although detailed information from the criminal investigations system is difficult to find, a review of reports on assessments of compliance with the FATF standards completed by the World Bank, the International Monetary Fund ("IMF"), FATF and FSRBs since the adoption of the Bank/Fund AML/CFT Pilot Assessment Program suggests that, at best, only a very small fraction of SARs filed with financial institutions represent actual positives. The result has been a general flooding of FIUs with essentially "defensive" suspicious activity/transaction reporting, which generates information overload and generally clogs the criminal investigations system with too many false positives.[155] A key improvement to the system as it now operates would be a significant reduction in false positives, though without a corresponding increase in false negatives.[156] The huge increase in suspicious activity/transaction reporting by financial institutions in the United States confirms this larger trend.[157]

In sum, FATF preventive measures do not specify key aspects of financial institutions' responsibilities in identifying and reporting suspicious transactions, including how many resources they should resort to in identifying the bona fides of payment origins or of owners and controllers of accounts, how much scrutiny should be applied to transactions, and how many false positives and false negatives are reasonable. The more effort financial institutions put into such activities, the more costly it is (with serious potential downsides for consumers of financial institution services). And,

153. *See generally* Elod Takats, *A Theory of 'Crying Wolf': The Economics of Money Laundering Enforcement* 4 (International Monetary Fund Working Paper No. 07/81, 2007), *available at http://papers.ssrn.com/abstract=979035* (laying out a theoretical argument for increasing filings of defense suspicious-activity reports by reporting institutions).

154. *See generally* STEPHEN LANDER, SERIOUS ORGANISED CRIMES AGENCY, REVIEW OF THE SARS REGIME 13 (2006), *available at* http://www.soca.gov.uk/downloads/SOCAtheSARsReview_FINAL_Web.pdf (discussing increases in STR reporting); Michael Levi & Peter Reuter, *Money Laundering*, 34 CRIME & JUST. 289 (2006). Of course, if a financial institution is sanctioned for reporting too many false positives, there will be a disincentive to report and a possible increase in false negatives.

155. *See* LANDER, *supra* note 154; Levi & Reuter, *supra* note 162, at 313; FLEMING, *supra* note 143, at 10, 35, 36.

156. *See* REUTER, *supra* note 52, at 94, 101–02 (discussing benefits of reducing false positives).

157. This conclusion is supported by specific studies of the United States and the United Kingdom. *See* Mariano-Florentino Cuellar, *Criminal Law: The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance*, 93 J. CRIM. L. & CRIMINOLOGY 311, 396 (2003) (describing increases in SARing in the United States); LANDER, *supra* note 154, at 25.

while over-reporting creates serious problems for the criminal investigations system, it seems to be the norm.[158] Nevertheless, the criminal investigations system gives little help to financial institutions by failing to proide detailed typologies or feedback as to the usefulness of SARs reported, which could be used by the financial institutions to reduce over-reporting. It would be of considerable help to financial institutions in implementing their detection, examination, and reporting requirements if these issues could be resolved. But apparently they have not been, at least not adequately.

Eliot Spitzer was caught up in the preventive measures net, even though he was not engaged in money laundering. While one must speculate a bit, it seems that his use of what appeared to be basic, run-of-the-mill money laundering techniques such as structuring and trying to hide his identity were enough to bring his transactions to the attention of his bank.[159] The fact that he was a politician (and perhaps one not well-liked by his particular bank) may have been enough for the bank simply to send along a SAR without much additional investigation as to whether money laundering might be involved. The same can be said for the Emperors Club, since the bank sent in a SAR simply because the club was using companies that apparently had no economic purpose other than to disguise their beneficial owner/controller.[160] An attentive IRS agent probably recognized the Governor's name and started an investigation, even though money laundering was not likely.

As noted earlier, even a cursory investigation by the bank would have revealed that Spitzer was making payments and not receiving them and that he was not in control of the ultimate recipients of the payments. But the bank did not need to spend additional resources to conduct an additional investigation as it could simply file a SAR and avoid further sanctions. Apparently this is what it did.

VIII. TERRORISM FINANCING

While the problem that the above system creates for financial institutions (and for government authorities) is clear enough with respect to financial institutions' monitoring of client accounts and reporting when they suspect proceeds of crime or money laundering, it is far more difficult when it comes to suspecting that terrorism financing is involved. When the FATF first published its 40 Recommendations, financial institutions in most FATF member countries were in the process of implementing a detection,

158. Stephen Stead, *AntiMoney Laundering—Compliance vs. Detection*, CREDIT CONTROL J., http://www.creditcontrol.co.uk/features/legalaspects/00002.htm (last visited Sept. 7, 2008).

159. *See* Sandman, *supra* note 10.

160. *See* Van Natta & Becker, *supra* note 14.

examination, and reporting system for criminal proceeds similar to the one required by the FATF 40's preventive measures. But when the detection, examination, and reporting system for terrorism financing was established, 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 at least some guidance from international organizations like the FATF and local law enforcement to help them. While financial institutions appear to over-report transactions and actually find few criminals, at least they had some idea of what they were supposed to do.

Soon after the FATF adopted the Special Recommendation IX (and soon after the United States adopted similar requirements), the FATF Secretariat published a commentary entitled *Guidance for Financial Institutions in Detecting Terrorist Financing*.[161] It was not a promising start. It stated flatly that "[i]t should be acknowledged that financial institutions will probably be unable to detect terrorist financing as such."[162] The paper went on to discuss that the source of terrorism financing is often crime and may therefore be covered already by existing AML detection techniques.[163] Even the report's list of "locations of concern" (i.e. places where transactions should raise heightened scrutiny), were largely the same as those listed in FATF 21: countries that did not comply with FATF 40.[164] While there was mention of charities as being of concern, there was no attempt to tie these concerns to any special type of charity or charity sending payments to locations known to have terrorism concerns.

Of course, if jurisdictions were all following the dictates of Special Recommendation VI and ensuring that nonprofits and charities were not being used by terrorists, financial institutions would not have a problem. It would be the job of governments to identify and shut down charities compromised by terrorists, or at least to place them on a list for financial institutions to check once, if not twice.

Although the United States was the principal country behind the FATF's adoption of the anti-money laundering detection, examination, and reporting system for terrorism financing, the National Commission on Terrorist Attacks Upon the United States' Staff Report on Terrorist Financing, published two years after the adoption of Special Recommendation IV, concluded that:

161. FINANCIAL ACTION TASK FORCE, GUIDANCE FOR FINANCIAL INSTITUTIONS IN DETECTING TERRORIST FINANCING (2002), *available at* http://www.fatf-gafi.org/dataoecd/39/21/34033955.pdf.

162. *Id.* at 3.

163. *Id.* at 7–8.

164. *Id.* at 9–10.

> [F]inancial institutions can be most useful in the fight against terrorist financing by collecting accurate information about their customers and providing this information—pursuant to legal process—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. Financial institutions have the information and expertise to detect the one but not the other.[165]

Subsequent reports on detecting terrorism financing were not much help. The UN Security Council, in its first report on the Al-Qaeda and Taliban Sanctions Monitoring Team, noted that the focus of the international community on countering terrorist financing through the formal banking system had led to the identification of accounts held by al-Qaeda associates. The identification of these accounts would presumably lead terrorists to seek "alternative means to raise and move their assets in ways that are less open to scrutiny," suggesting that terrorists could be moving away from financial institutions entirely,[166] although most likely as a result of the "making a list, checking it twice" system. Subsequent reports reiterated this point.[167] In its sixth report, the monitoring team was not enthusiastic about the effectiveness of preventive measures, in part because of the lack of guidance.[168]

Almost all states have a FIU or equivalent body charged with collecting, analyzing, and disseminating SARs. The volume of SARs has increased tremendously, though the procedure suffers from a lack of guidance as to what to look for, and in many states there is limited capacity to examine these reports, most of which are generated by banks. Only a small proportion of the reports are related to terrorist financing, and hardly any have been associated

165. JOHN ROTH ET AL., NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, MONOGRAPH ON TERRORIST FINANCING: STAFF REPORT TO THE COMMISSION 52 (2004), *available at* http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf.

166. United Nations Security Council, Fifth Report of the Analytical Support and Sanction Monitoring Team Appointed Pursuant to Security Council Resolution 1526, 1617 (2004–2005), para. 49, U.N. Doc. S/2004/679 (Aug. 25, 2004), *available at* http://www.un.org/sc/committees/1267/monitoringteam.shtml (concerning Al-Qaida, the Taliban, and associated individuals and entities) [hereinafter UNSC Fifth Report].

167. UNSC Fifth Report, *supra* note 175, at para. 79 U.N. Doc. S/2006/750 (Sept. 20, 2006), *available at*, http://www.un.org/sc/committees/1267/monitoringteam.shtml.

168. United Nations Security Council, Sixth Report of the Analytical Support and Sanction Monitoring Team Appointed Pursuant to Security Counsil Resolution 1526, 1617 (2004–2005), para. 27, U.N. Doc. S/2007/132 (Mar. 8, 2007), *available at* http://www.un.org/sc/committees/1267/monitoringteam.shtml (concerning Al-Qaida, the Taliban, and associated individuals and entities).

with al-Qaeda.[169]

There was, however, one area that did receive considerable and increasing attention, and that was nonprofits/charities. As noted in the discussion of the example introduced earlier in this Article, and as emphasized by Special Recommendation VIII, charities appeared (though with perhaps insufficient empirical evidence) to be involved fairly regularly in terrorism-financing transactions. This was emphasized repeatedly in reports that could be used as guidance by financial institutions, their supervisors, and law enforcement, including FIUs. For example, the U.S. National Money Laundering Strategy for 2003 stated that the practice of financing terror "through ostensibly charitable institutions is an important element in the global fight against terrorist financing" and committed the U.S. to countering this threat.[170] In its typologies documents during this period, the FATF also stressed that terrorists often abused charities. But even these documents focused on the importance of identifying terrorists and tying them to charities, rather than somehow identifying terrorism financing through "suspicious" patterns of transactions.

For example, the 2002–03 Typologies Report discussed a case where a bank filed a SAR for a nonprofit client, but only because someone at the bank had read a newspaper article in which the client was mentioned as being a suspected terrorist organization.[171] However, the following year the FATF Typologies Report appeared to conclude that identification of terrorists is something that lies in the expertise of government authorities and not financial institutions. "[T]he best chance of success for detecting possible terrorist financing links to [nonprofit organizations] *is through intelligence or police work*, which builds on links with other [nonprofits] (operational, financial or through common management and personnel) or though connections to individuals that are already suspected of terrorist or terrorist financing activities."[172]

169. *Id.*

170. U.S. DEP'T OF THE TREASURY AND U.S. DEP'T OF JUSTICE, NATIONAL MONEY LAUNDERING STRATEGY 13 (2003), *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_10.pdf.

171. FINANCIAL ACTION TASK FORCE, REPORT ON MONEY LAUNDERING TYPOLOGIES 2002–2003, 5–6 (2003), http://www.fatf-gafi.org/dataoecd/29/33/34037958.pdf.

172. FINANCIAL ACTION TASK FORCE, REPORT ON MONEY LAUNDERING TYPOLOGIES 2003–2004, 11 (2004) (emphasis added), *available at* http://www.fatf-gafi.org/dataoecd/19/11/33624379.pdf. The report went on to claim,

> The reporting of suspicious unusual transactions by financial institutions and the subsequent analysis by [financial intelligence units] or law enforcement also play an important role in bringing certain cases of suspected terrorist abuse . . . to the surface. In some countries, suspicious transaction reports related to unusual [nonprofit] activity have actually led to the initiation of an

Early in 2008, the FATF released its most comprehensive report to date on terrorist financing.[173] With respect to suspicious activity/transaction reporting by financial institutions, the report again focused on nonprofits/charities. The report stated that "suspicious transaction reporting has a central role in identifying terrorist financing and the movement of terrorist funds through the financial system," and 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."[174] However, the cited cases and examples almost entirely dealt with organizations, including charities, or individuals otherwise identified as having terrorism connections. The only unique terrorism-financing indicators noted in the report were charity/relief organizations linked to transactions, sending or receiving funds from and/or to "locations of specific concern," and "media coverage of account holder's activities,"[175] presumably when the media reveals that an organization or person may be connected to terrorism. The problematic nature of developing a profile of legitimate for-profit and not-for-profit enterprises likely to engage in terrorist activity has not been lost on scholarly commentators.[176]

The focus on charities has been reinforced by local supervisors, including in the United States. For example, the U.S. FFIEC Manual states that financial institutions should engage in customer identification and client profiling, including establishing the purpose and objectives of their stated activities, locations served, organizational structure, donor and volunteer base, funding and disbursement criteria, recordkeeping requirements, affiliation with other NGOs, governments, or groups, and internal controls and audits. And if the financial institution determines that the charity is of "high risk," then additional diligence should be performed, such as evaluating the principals, obtaining and reviewing the financial statements and audits, verifying the source and use of funds, valuating large contributors or grantors of the NGO, and conducting reference checks.[177]

> investigation, while in other cases the reporting system and [financial intelligence unit] analysis have contributed to the development of further leads in ongoing investigations.

Id. However, it did not discuss typologies (other than those indicating money laundering) of use to financial institutions. *Id.*

173. *See* FINANCIAL ACTION TASK FORCE, TERRORIST FINANCING (2008), *available at* http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf.

174. *Id.* at 29.

175. *Id.* at 32.

176. *See, e.g.*, Laura K. Donohue, *Anti-Terrorism Finance in the United Kingdom and the United States*, 27 MICH. J. INT'L L. 303, 394 (2006) ("[I]t is difficult, if not impossible, to discern patterns in financial transactions that would signify terrorist activity.").

177. FFIEC MANUAL, *supra* note 119, at 281–83.

But the customer identification and profiling is really no different than that required for AML purposes, nor is there any indication as to when a financial institution should determine that there is "high risk" and that additional diligence is due. With respect to organizational structure, recordkeeping requirements, and internal controls and audits, it might be possible to examine if charities are implementing best practices as to internal governance. Soon after the adoption of Special Recommendation VIII, the FATF published a paper on such best practices,[178] and there has been a movement in many jurisdictions toward creating best practices for internal governance,[179] including in the United States.[180] However, the fact that there are best practices does not tell financial institutions how closely the charity must follow them before suspicion is raised, or how far the financial institution should go in confirming that the charity is following the practices.

In summary, the guidance provided to financial institutions with respect to CFT suspicious activity/transaction reporting gives very little *actual guidance*. First, there is the general problem that the basic FATF 40 preventive measures—the detection, examination, and reporting system for money laundering upon which the detection, examination, and reporting system for terrorism financing is based—fails to make clear how far a financial institution should go to identify clients, build a client profile, monitor transactions, and determine when a transaction is suspicious. The financial institution should not go so far as to play the role of private detective investigating in detail each client and each transaction, but it needs to do more than make a cursory review if it is to avoid sanctions.

Next, there is little to indicate that a financial institution's client is more likely to be a terrorist or terrorist financier other than that the client, or a person who has some control over it, is a terrorist or is engaging in transactions with someone who is. And, there is little way for a financial institution to know that, other than by learning from someone else who knows, such as a government agency or perhaps the media, or, in other words, by "making a list and checking it" at least once.

178. FINANCIAL ACTION TASK FORCE, COMBATING THE ABUSE OF NON-PROFIT ORGANIZATIONS (2002), *available at* http://www.fatf-gafi.org/dataoecd/39/19/34033761.pdf (discussing international "best practices").

179. *See generally* Emile van der Does de Willebois, *Terrorist Financing Networks and International Non-Profit Organizations*, paper delivered at The University of Pennsylvania (Feb. 6, 2008) (copy on file with the author) (discussing developing international best practice for nonprofit governance and governmental oversight from the perspective of Special Recommendation VIII).

180. U.S. DEPARTMENT OF THE TREASURY, ANTI-TERRORIST FINANCING GUIDELINES: VOLUNTARY BEST PRACTICES FOR U.S.-BASED CHARITIES (2006), *available at* http://www.ustreas.gov/press/releases/reports/0929%20finalrevised.pdf.

However, financial institutions may still see a serious problem. Special Recommendation IV does exist separately from Special Recommendation III. That, plus the relatively undefined nature of the duties imposed on them by FATF preventive measures, plus the threat of serious sanctions, plus the existence of Special Recommendation IV may make financial institutions wary of relying solely on lists, whether government or media-provided. When one factors in the tendency of financial institutions to react to the relatively undefined nature of FATF preventive measures and a cost-benefit analysis by over-reporting, one might expect an increase in SARs related to terrorism financing, and, in particular, many false positives.

This seems to be the case, at least in those jurisdictions reporting suspicious activity/transaction reports filed as indicating terrorism financing.[181] For example, according to FinCEN, since 2003, when records began to be kept of SARs indicating terrorism financing, and up to 2007, numbers have increased five-fold, from 155 to 687.[182] Nevertheless, these numbers are still quite small compared to those for AML/structuring, which went from 155,468 to 347,393.[183] Also, hardly surprisingly, financial institutions tended to focus on charitable organizations and, in particular, nonprofits that involve Islamic organizations and wire activity to or from "suspect" states.[184] If you are a financial institution and you need to report on *someone*, you might as well report on an Islamic charity.

If the existence of Special Recommendation VIII means that there is a largely inaccurate tendency for financial institutions to vastly over-report transactions by certain charities, such over-reporting entails many possible downsides in addition to the waste of resources to financial institutions and to government. If financial institutions seek to reduce costs by discriminating against certain charities, this can have many different social costs. If the charities are more likely to be supporting charitable causes in desperate areas because these causes are more likely to involve terrorist activity, the negative effects could be magnified.[185]

181. *See* REVIEW OF FATF MUTUAL EVALUATIONS FOR TERRORISM FINANCING-RELATED SARS (2008) (copy on file with the author).

182. FINCEN, SAR BY DEPOSITORY INSTITUTIONS, *available at* http://www.fincen.gov/news_room/rp/files/sar_by_numb_09.pdf

183. *Id.*

184. Bank Secrecy Act Advisory Group, *Trends and Analysis*, 10 SAR ACTIVITY REVIEW: TRENDS, TIPS & ISSUES 5, 10–13 (2005), *available at* http://www.fincen.gov/news_room/rp/files/sar_tti_10.pdf.

185. *See, e.g.*, Nina J. Crimm, *High Alert: The Government's War on the Financing of Terrorism and Its Implications for Donors, Domestic Charitable Organizations, and Global Philanthropy*, 45 WM. & MARY L. REV. 1341 (2004) (discussing extensively the liabilities imposed by the U.S. on charitable donations by anti-terrorism financing laws).

CONCLUSION

FATF preventive measures for money laundering are sufficiently vague such that financial institutions rarely know how far to go when implementing them. Financial institutions do, however, at least have some experience, assisted by typologies exercises, in identifying transactions that suggest laundering, but the preventive measures are hardly perfect. Eliot Spitzer was not engaged in laundering the proceeds of crime, yet he was caught up in the preventive measures net. He was making payments to someone for some reason, which might conceivably be the financing of crime. As it turns out, he was financing what was technically a crime (albeit a minor one), but there are no requirements that banks report suspicions of criminal financing, only financing of terrorism. Presumably, because he was not a charity engaging in transactions with other charities in certain suspect jurisdictions, the SAR did not indicate suspected terrorism financing.

In effect, Spitzer used a few techniques identified by anti-money laundering methodologies as of the types used by launderers. Even though a quick analysis by the banks would show that neither laundering nor financing of terrorism was involved, without clear guidance as to how far they needed to investigate, the banks apparently did not undertake any serious analysis at all. Instead, they filed defensive SARs. Apparently, the authorities investigated because Spitzer was *Governor Spitzer*, not because they believed he was laundering the proceeds of crime or financing terrorism.

There appears to be no reason to believe that any genuine terrorist financer would have engaged in similar transactions (or any transactions identified in typologies as indicating suspicion of money laundering). Also, there appear to be no useful typologies indicating terrorism financing other than when known or suspected terrorists are involved or when charities make payments to accounts held by persons in certain geographical areas. And, finally, there is insufficient guidance as to how far financial institutions must go to investigate any of these possible criminal acts to determine if a transaction genuinely raises suspicion, whether it be of money laundering or terrorism financing.

Identifying criminal behavior should always, first and foremost, be the job of governments, not the private sector. AML preventive measures should better recognize this fact and spell out more clearly how far financial institutions should have to go in investigating whether certain transactions may indicate the proceeds of a crime. This can only be accomplished by more clearly defined duties, by providing more information on AML typologies, and by providing extensive feedback to financial institutions on their suspicious activity/transaction reports. In particular, a better system of incentives to reduce false positives while not increasing false negatives should be devised.

Identifying terrorists also should be almost entirely the job of governments and not of financial institutions. Terrorist financing typologies are too focused on certain charities to be of any use in distinguishing false positives and negatives. If a charity or a person who controls a charity that either receives or makes a payment is identified as a possible terrorist, then a financial institution can implement the customer due diligence measures required under regular AML preventive measures to see if the customer is involved with such a person or organization. However, it makes little sense to require the financial institution to decide who is a terrorist and who is not. If there was ever a job for governments, that is one.

Under the current AML/CFT system we are more likely to catch Eliot Spitzer than a real terrorist, and perhaps more likely to catch Mr. Spitzer than a real money launderer—given the huge number of SARs that are false positives and the poor feedback provided, it is impossible to know. This system definitely must be improved if serious criminals, including terrorists, are to be caught.