

THE GEORGE WASHINGTON UNIVERSITY

Banks Are Not Mere Bystanders

Why compliance officers should have security clearances

Brett Wallace

Spring 2009

Introduction

Despite the economic troubles during the financial crisis of Fall 2007, the prospects for bank nationalization look dim.¹ The federal government has however, continued to assume an increasingly large role in some of the nation's predominant financial institutions.² Freddie Mac and Fannie May have been placed under federal conservatorship. The government is the majority shareholder of AIG and owns almost \$100 billion of preferred shares in brand-name banks like Bank of America and CitiGroup. The end goal isn't nationalization, but to decrease bank's self sufficiency, facilitating their ability to effectively run their business on their own in the future.³

This model doesn't only apply to the bank's balance sheet, but can apply to its compliance officers' efforts to counter-illicit finance as well. Banks were already drowning in their regulatory requirements under the Patriot Act and the Bank Secrecy Act.⁴ Now due to the recent financial calamity, the banking industry has been forced to slash the budgets and staffs of their compliance offices, further compounding the problem.⁵ In order to patch a potentially gaping compliance hole, the federal government should use law enforcement to enhance bank's ability to effectively exercise due diligence. The best mechanism the government can use is to formally grant security clearances to select bank employees so that classified information can be shared with compliance offices. Increasing public-private cooperation in this manner would be a boon to anti-money laundering and counterterrorism finance efforts. A robust public-private framework for cooperation is the critical missing link in one of the most effective counterterrorism instruments the U.S. has at its disposal: the financial war on terror.

¹ Colin Barr, "What is Nationalization?," *Fortune*, February 20, 2009, <http://money.cnn.com/2009/02/20/news/nationalization.what.is.it.fortune/index.htm>.

² David Ellis, "Don't Bet on Bank Nationalization," *CNN Money*, January 22, 2009, http://money.cnn.com/2009/01/22/news/companies/banks_nationalization/.

³ Ibid.

⁴ Courtney J. Linn, "How Terrorists Exploit Gaps in U.S. Anti-Money Laundering Laws to Secrete Plunder," *Journal of Money Laundering Control*, Volume 8, Issue 3 (2005) pp. 200-214.

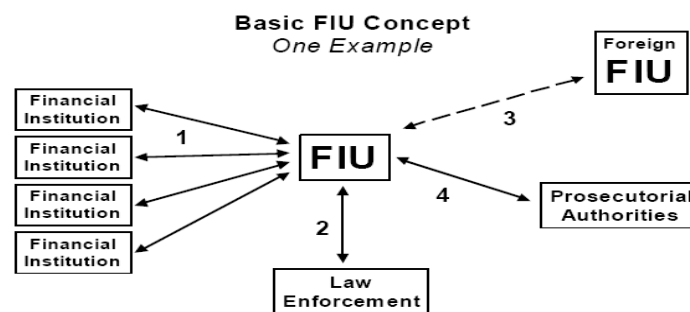
⁵ Dennis Lormel, "Dangerous Riptide Threatens Financial Institutions," *Counterterrorism Blog*, February 26, 2009, http://counterterrorismblog.org/2009/02/dangerous_riptide_threatens_fi.php.

Section One: The Compliance Office

"Banks are...not conscripted neutrals in transactions."⁶ "Banks are 'intelligence collectors'... People who do not like this need to get over it"⁷

Banks are the first line of defense against illicit finance. They alone are able to accept deposits and provide direct access to deposits through payment systems.⁸ If an individual wants to store, transfer, or accept funds that have an illicit origin it is very difficult to do without use of a bank. In recognition of banks' role as the most easily identifiable party to a financial crime, the U.S. has implemented three operational tools to combat money laundering; the Bank Secrecy Act, the USA PATRIOT Act and the International Emergency Economic Powers Act (IEEPA).

Passed in 1970, the Bank Secrecy Act has evolved into an extremely powerful law that does precisely the opposite as its name suggests. Instead of keeping banking information secret it obliges banks to snitch on their customers if they observe a crime.⁹ Bank customers do not have a privileged, confidential relationship with their banks.¹⁰ When a bank clears a financial transaction of 10,000 or more, it must send a Currency Transaction Report (CTR) to the Financial Crimes Enforcement Network (FinCEN), the United States' Financial Intelligence Unit (FIU). When a bank observes suspicious activity, it



1. Disclosures transmitted to FIU.
2. FIU receives additional information from law enforcement.
3. Possible exchange with foreign counterpart FIU.
4. After analysis, FIU provides case to prosecutor for action.

⁶ California Bankers Assn. v. Shultz, 416 U.S. 21 (1974).

⁷ Jeffery Breinholt, "The Holy Grail of Public-Private Counterterrorism Cooperation," *Counterterrorism Blog*, May 23, 2007, http://counterterrorismblog.org/2007/05/the_holy_grail_of_publicprivat.php.

⁸ Department of Treasury and Department of Justice, "2007 National Money Laundering Strategy," 2007, <http://www.treas.gov/press/releases/docs/nmls.pdf>.

⁹ Jeffery Breinholt, "The Bank Secrecy Act for Beginners," *Counterterrorism Blog*, February 14, 2008, http://counterterrorismblog.org/2008/02/the_bank_secrecy_act_for_begin.php.

¹⁰ Ibid.

is obliged to send a Suspicious Activity Report (SAR) to FinCEN. These mandatory reports form the raw data and investigatory evidence that FinCEN uses to fight financial crime.

Title III of the Patriot Act amended the Bank Secrecy Act in 2002. The revision requires all financial institutions to create their own anti-money laundering program with the following mandatory minimums: (1) the development of internal policies, procedures and controls, (2) the designation of a compliance officer (3) an ongoing employee training program, (4) an independent audit function to test these programs.¹¹ In short, banks are required to “know their customer” which gives them the ability to know when it is appropriate to report suspicious activity to FinCEN.

The Patriot Act also proscribes standards to combat international money laundering. Title III requires due diligence standards for U.S. financial institutions that have correspondent accounts.¹² Additionally, Title III includes extraterritorial jurisdiction over foreign financial institutions that have a relationship with the United States, meaning the U.S. has subpoena and seizure power if the *foreign* institution fails to meet *U.S.* anti-money laundering standards.¹³ Lastly, the regulations also prohibit conducting business with foreign shell banks.¹⁴

The third crucial piece of legislation in U.S. anti-money laundering efforts is IEEPA. It essentially allows the president to sever the United States’ economic relationship with any individual, company, or country deemed a threat to the country’s national security or economy.¹⁵ The Department of Treasury’s

¹¹ “Bank Secrecy Act/Anti-Money Laundering Program Policies and Procedures,” Wells Capital Management, April 2007, [https://www.wellscap.com/docs/WellsCap%20BSA%20Policies%20%20Procedures%20\(4-26-07\)%20\(2\).pdf](https://www.wellscap.com/docs/WellsCap%20BSA%20Policies%20%20Procedures%20(4-26-07)%20(2).pdf).

¹² A correspondent account is defined broadly in U.S. code 5318A(f)(1)(B) as “an account established to receive deposits from, make payments on behalf of a foreign financial institution, or handle other financial transactions related to such institution.”

¹³ Robert Graves, “Extraterritorial Application of the Patriot Act,” News/Press, Jones Day, November 2007, <http://www.jonesday.com/files/News/2df0b605-1cc3-4729-ae61-a0305551bbe5/Presentation/NewsAttachment/a90f839d-3ae4-4ee6-bb4a-ad4d36ea6e87/PATRIOT%20Issues%20for%20foreign%20banks%20PPT.pdf>

¹⁴ A shell company has “no physical presence other than a mailing address, employ no one and produce nothing.” Department of Treasury and Department of Justice, “2007 National Money Laundering Strategy,” 2007, <http://www.treas.gov/press/releases/docs/nmls.pdf>.

¹⁵ United States Department of Treasury, “International Emergency Economic Powers Act,” Terrorism and Financial Intelligence Publications and Legislation, *Department of Treasury* February 12, 2006, <http://www.treas.gov/offices/enforcement/publications/ieepa.pdf>.

Office of Foreign Assets Control (OFAC) is responsible for maintaining a list of entities the president has decided to sanction, including terrorism financiers, narcotics traffickers, and weapons proliferators. Banks then have the responsibility of scrubbing their customer lists against OFAC's lists to ensure that they are not interacting with any designated entities.¹⁶

Furthermore, the United States government runs an extensive anti-money laundering/counterterrorism finance operation across the national security apparatus. The CIA operates the Terrorism Finance Tracking Program which conducts daily surveillance of SWIFT data.¹⁷ The FBI formed the Terrorism Financing Operations Section in 2002 in order to direct and coordinate its field offices' terrorism finance investigations.¹⁸ Treasury now has its own in-house intelligence agency, the Office of Intelligence and Analysis, which along with FinCEN and OFAC form the Office of Terrorism and Financial Intelligence (TFI). Even the Pentagon has become involved, establishing the Iraq Threat Finance Cell in Baghdad as a way of coordinating financial intelligence with military operations.¹⁹

Finally, the United States participates in several international bodies to coordinate international AML/CTF cooperation.²⁰ Among the most important are the Financial Action Task Force (FATF), which "examines money laundering techniques and trends, reviews the actions of individual jurisdictions and the international community and sets out measures that still need to be taken to combat money laundering,"²¹ and the Egmont Group, which is a forum for international FIU cooperation.²²

¹⁶ "Bank Secrecy Act/Anti-Money Laundering Program Policies and Procedures," Wells Capital Management, April 2007, [https://www.wellscap.com/docs/WellsCap%20BSA%20Policies%20%20Procedures%20\(4-26-07\)%20\(2\).pdf](https://www.wellscap.com/docs/WellsCap%20BSA%20Policies%20%20Procedures%20(4-26-07)%20(2).pdf).

¹⁷ Eric Lichtblau and James Risen, "Bank Data is Sifted By U.S. in Secret to Block Terror," *New York Times*, June 23, 2006, <http://www.nytimes.com/2006/06/23/washington/23intel.html?ex=1308715200&en=168d69d26685c26c&ei=5088&partner=rssnyt&emc=rss>.

¹⁸ Matthew Levitt and Michael Jacobson, "The Money Trail: Finding, Following, and Freezing Terrorist Finances," Policy Focus #89, *The Washington Institute for Near East Policy*, November 2008. p. 17, <http://www.washingtoninstitute.org/pubPDFs/PolicyFocus89.pdf>.

¹⁹ Ibid.

²⁰ Including the UN, the EU, G7, G8, G20, FATF, the Egmont Group, APEC, ASEAN, OAS, OSCE and Manila Framework Group.

²¹ Department of Treasury Office of Public Affairs, "Testimony of Juan Zarate, Assistant Secretary Terrorist Financing and Financial Crimes, U.S. Department of Treasury, Before the House Financial Services Subcommittees

Section Two: The Value of the Financial War on Terror

“Terrorism is generally perceived as being the pursuit of political ends through violent means and certainly, in the popular perception, involves such things as bank robberies and the kidnapping or killing of innocent civilians. In part, this remains true, but a high degree of sophistication has been added to this so that the terrorist is now more likely to conform to the image of a middle-ranking clerk than to a gun-toting hoodlum.”²³

The notion that terrorism is “cheap” is the most commonly cited objection to investing heavily in a financial war against terror. An indictment of the efficacy of financial counterterrorism measures, the argument is essentially that it takes very little money to “buy some fertilizer, rent a truck, and bring down a building.” Therein lies the cost-effectiveness of terrorism, as the executive dean of Harvard’s Radcliffe Institute for Advanced Study puts it, “one can get so much bang for one’s buck. It is cheap and easy and lends itself to a dramatic impact.”²⁴ Those opposed to financial countermeasures use the approximate operational cost of major terrorist attacks, shown in the table below, to bolster their argument and show that terrorist conspiracies, when analyzed empirically, are relatively inexpensive.

The direct attack costs of a terrorist conspiracy²⁵

Attack	Date	Estimated cost
London transport system	7 July 2005	GBP 8 000
Madrid train bombings,	11 March 2004	USD 10 000
Istanbul truck bomb attacks,	15 & 20 November 2003	USD 40 000
Jakarta JW Marriot Hotel bombing	5 August 2003	USD 30 000
Bali bombings	12 October 2002	USD 50 000
USS Cole attack	12 October 2000	USD 10 000
East Africa embassy bombings,	7 August 1998	USD 50 000

on Domestic and International Monetary Policy, Trade and Technology and Oversight and Investigations” U.S. Department of Treasury Press Room, September 30, 2004 <http://www.ustreas.gov/press/releases/js1971.htm>.

²² The Egmont Group, “Information Paper on Financial Intelligence Units and the Egmont Group,” *Library: Egmont Documents*, September 2004, http://www.egmontgroup.org/info_paper_final_oct_2004.pdf.

²³ James Adams, “The Financing of Terror,” in *Contemporary Research on Terrorism*, ed. Paul Wilkinson and Alasdair Stewart (Aberdeen: Aberdeen University Press, 1987) p. 401.

²⁴ Cited in: Matthew Levitt, *Hamas: Politics, Charity and Terrorism in the Service of Jihad*, (New Haven: Yale University Press, 2006) 53.

²⁵ Chart originally appeared in “Terrorism Financing,” *Financial Action Task Force*, February 29, 2008, <http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf>.

Unfortunately for the terrorism is “cheap” point of view, it has problems. The central flaw of the anti-financial warfare camp is that it solely focuses on the operational costs for terrorist attacks, while ignoring the broad infrastructural costs that a terrorist organization requires. The “costs” side of a terrorist organization’s balance sheet can thus be divided into two sections, direct operational support and broad organizational requirements.²⁶

Included under direct support are the costs required for an isolated terrorist conspiracy. Among them are the direct expenses of the attack itself, such as weapons and ammunition, vehicles, explosive precursors, vehicles, maps, and communication or surveillance technology. Additionally, members of terrorist organizations often receive salaries for basic sustenance, living expenses, and taking care of family members. Lastly, there are investments made early on in the operational planning stage including forging documents, bribes, travel to different locations, and any necessary training (flight school classes, for example).

In turn, a look at the broad organizational requirements reveals the enormous hidden costs that come with maintaining a successful terrorism outfit that can sustain a focused counterterrorism assault. Infrastructure for strategic communications, promotion of ideology, recruitment, indoctrination, political and social works projects, safe houses and various administrative costs are all vital to the day-to-day operations that keep terrorists in business. Although there is no one universal cost-sheet checklist that could reflect all terrorist organizations’ infrastructural expenses, they all require a certain degree of institutional expenditures to stay in business. A brief look at the finances of Al Qaeda, Hamas and Hezbollah illustrate this point.

Al Qaeda’s awareness of their own financial infrastructure’s importance is plainly obvious after examining its sheer effort and dedication to fiduciary security. In terms of quantity, Al Qaeda has

²⁶ These distinctions and their explanations are borrowed from “Terrorism Financing,” *Financial Action Task Force*, February 29, 2008, <http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf>.

accounts or financial connections in roughly 100 countries²⁷ and its budget is estimated to be \$36 million a year.²⁸ As for the quality of its money management, Rohan Gunaratna's seminal book Inside Al Qaeda offers an apt description. "Intelligence and security services worldwide, including the CIA and MI6, have never before encountered a global terrorist financial network as sophisticated as Al Qaeda's. Comparisons with other such networks reveal that Al Qaeda has built the most complex, robust and resilient money generating and money moving network yet seen."²⁹ In fact, building this intricate web of financial transactions can be seen as Bin Laden's foremost accomplishment, as it facilitates two of Al Qaeda's most advantageous characteristics; its resiliency and its transnational nature.

Estimates of Hamas' budget range from \$30 million to \$90 million annually.³⁰ It uses charity-based funding and social work to recruit new members, spread bribes, gain favors from the local population, and facilitate militant and terrorist activities. (Hamas's political and social infrastructure is closely tied to its terrorist cells; so close, in fact, that its entire network can be seen as one large terror apparatus.)

Hezbollah's budget is said to add-up to anywhere from 100-200 million dollars to over 1 billion dollars after you add contributions from Shia expatriate communities and proceeds from criminal

²⁷ Josh Meyer, "Cutting Money Flow to Terrorists Proves Difficult," *Los Angeles Times*, September 28, 2003, A1.

²⁸ Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror*, (New York: Colombia University Press, 2002), 61. Note that this figure is from a 2002 study, based on pre September 11th estimates. Attempts to decipher what Al Qaeda's budget is today would be nearly impossible. For example, former UN Monitor of Terrorism Financing Victor Comras admits that "We haven't the faintest notion now of what al Qaeda and other salafist terrorist groups need or spend today." See Victor Comras, "Talking Paper: War on Terrorism Financing, Counterterrorism Blog Conference, Four Years Later: Are We Safer?," *The Intelligence Summit*, September 8, 2005, <http://www.intelligencesummit.org/news/AndrewCochran/VC090805.php>. This is especially problematic considering the lack of consensus within the terrorism analyst community over the relevance of Al Qaeda's central leadership, exemplified by the disagreement between Bruce Hoffman and Marc Sagemen. See Elaine Sciolino and Eric Schmitt, "A Not Very Private Feud Over Terrorism," *The New York Times*, June 8, 2008, http://www.nytimes.com/2008/06/08/weekinreview/08sciolino.html?_r=2&oref=slogin&oref=slogin.

²⁹ Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror*, (New York: Colombia University Press, 2002), 61.

³⁰ Matthew Levitt, *Hamas: Politics, Charity and Terrorism in the Service of Jihad* (New Haven: Yale University Press, 2006) p. 54.

enterprise activities to the exorbitant largesse it receives from Iran.³¹ Hezbollah is thus effectively able to operate without financial constraints. Its extra cash often ends up in the hands of Palestinian terrorist groups for the purposes of fomenting instability with Israel. Additionally, Hezbollah has an overhead cost which many terrorist organizations lack. It spends millions on its personal television station, al-Manar, which it uses to disseminate propaganda throughout the Middle East.³² Lastly, intelligence officials have testified that potentially thousands of members of the Mahdi Army in Iraq have been trained by financially draining Hezbollah camps in Lebanon.³³ A substantial portion of the threat that Hezbollah poses to the world today stems from these activities, all of which are all made possible by its brimming budget.

Terrorism will always exist; only a utopian society could eradicate all of the factors that spur it on. The goal should thus be to constrict terrorists' operating environment to the maximum extent possible. Each dollar available to a terrorist is like oil, lubricating the machinery of terror and ensuring it runs more frequently, more reliably, and with greater sophistication.³⁴ Or to borrow Secretary Colin Powell's words, "money is the oxygen of terrorism. Without the means to raise and move money around the world, terrorists cannot function."³⁵ While trying to prevent terrorists from functioning is a bit lofty, a financial smother campaign is a more concrete and attainable goal. Such a campaign may not always work to stop isolated incidents or low-level attacks, but is most likely to stop a spectacular event that

³¹ Andrew Cochran, "Millions in Criminal Proceeds + Iran's Oil Millions = Hearts, Minds, Votes for Hezbollah," *Counterterrorism Blog*, May 22, 2008, http://counterterrorismblog.org/2008/05/millions_in_criminal_proceeds.php.

³² Matthew Levitt, "Hizballah Finances: Funding the Party of God, PolicyWatch #965," *The Washington Institute for Near East Policy*, March 1, 2005, <http://www.thewashingtoninstitute.org/templateC05.php?CID=2266>.

³³ Michael Gordon and Dexter Filkins, "Hezbollah Said to Help Shiite Army in Iraq," *The New York Times*, November 27, 2006, <http://www.nytimes.com/2006/11/28/world/middleeast/28military.html>.

³⁴ Matthew Levitt, *Hamas: Politics, Charity and Terrorism in the Service of Jihad*, (New Haven: Yale University Press, 2006), 55.

³⁵ Colin Powell, "Remarks on Financial Aspects of Terrorism at Office of Financial Crimes Enforcement Network," *US Department of State*, November 7, 2001, <http://www.state.gov/secretary/rm/2001/5979.htm>.

involves a great deal of planning and dedicated resources.³⁶ For example, when Ramzi Yousef bombed the World Trade Center in 1993 he was so strapped for cash that he was unable to build a large enough bomb to create his desired “domino effect” with the towers.³⁷ (He intended to explode one tower and then have it topple into the other).³⁸

Even if cutting off terrorist organization’s sources of funding is unable to directly thwart operations and attacks, using financial information as counterterrorism intelligence has proven to be an invaluable tool.³⁹ In fact, financial investigations can be more important than any tactical battlefield victory.⁴⁰ The information gleaned from following the money trail allows for counterterrorism officials to go on the offensive, thereby disrupting current and future operations and rolling-up terrorist cells. It further permits financial information to be used directly alongside other forms of information in an integrated and coordinated manner, thus enhancing long-term intelligence analysis.⁴¹ As money works its way through a given financial network, it carries with it certifiable information that can be traced. People’s names, locations, purchases, occupations, and travel history can be discovered, illicit activity can be uncovered and investigators can then follow a verifiable trove of information. Even if the trail only leads to financiers, facilitators, or couriers, capturing these individuals can then lead to a windfall of additional intelligence. Dennis Lormel, the former head of the FBI Terrorist Financing Operations

³⁶ Todd Sandler, Daniel D. Arce and Walter Enders, “Copenhagen Consensus 2008 Challenge Paper: Terrorism,” *Copenhagen Consensus Center*, February 2008, http://www.copenhagenconsensus.com/Admin/Public/DWSDownload.aspx?File=%2FFiles%2FFiler%2FCC08%2FPapers%2F0+Challenge+Papers%2FCP_Terrorism_-_Sandler.pdf.

³⁷ Matthew Levitt, Hearing on “The Role of Charities and NGOs in the Financing of Terrorist Activities,” U.S. Senate Committee on Banking, Housing and Urban Affairs, Subcommittee on International Trade and Finance, August 1, 2002, http://banking.senate.gov/02_08hrg/080102/levitt.htm.

³⁸ Steve Coll, *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, From the Soviet Invasion to September 10, 2001* (New York: The Penguin Group, 2004) p. 249-250.

³⁹ “Terrorism Financing,” *Financial Action Task Force*, February 29, 2008, <http://www.fatfgafi.org/dataoecd/28/43/40285899.pdf>.

⁴⁰ John A. Cassara, *Hide and Seek, Intelligence, Law Enforcement and the Stalled War on Terrorist Finance* (Dulles, Virginia: Potomac Books, 2006) xiii.

⁴¹ John Roth, Douglas Greenburg, and Serena Wille, “Monograph on Terrorist Financing,” *National Commission on Terrorist Attacks Upon the United States*, 2004, http://www.911commission.gov/staff_statements/911_TerrFin_Monograph.pdf.

Section, has championed the successes of this strategy. He has gone on the record stating that during his FBI tenure, American financial investigations thwarted six separate terrorist plots.⁴² More recently, British authorities were able to prevent the 2006 liquid explosives airliner plot largely because of critical financial intelligence.⁴³

Data from the FBI indicates that in 42% of cases, the investigative file includes a SAR or a CTR.⁴⁴ Therein lies the crucial role of banks. The moment that a terrorist or terrorist supporter deposits money in a bank and comes in contact with the highly regulated financial world is the moment that it is easiest to identify and disrupt.⁴⁵ As terrorist organizations are forced to rely more and more on illicit sources of funds and common criminal acts, their infrastructure and operations become more vulnerable to financial counterterrorism tools because prosecutors don't even need to win a conviction based on the intention to commit an act of terrorism, merely on the crime of money laundering or financial fraud.

Additionally, the 9-11 investigation is exemplary of how financial information from banks can yield critical 'after the fact' information to discover the perpetrators of an attack. The United States was able to identify connections between all of the hijackers by using financial leads.⁴⁶ Then, the trails lead to Al Qaeda operatives in Hamburg, Germany who provided the hijackers with financial and logistical support. A wire transfer of \$14,000 from the Hamburg Cell enabled investigators to link Zacarias Moussaoui to the plot and to subsequently indict and convict him for his role in the September 11th

⁴² Jeffery Breinholt, "Be Careful What You Wish For: A Review of Ibrahim Warde's 'The Price of Fear'," *Counterterrorism Blog*, April 7, 2008, http://counterterrorismblog.org/2008/04/be_careful_what_you_wish_for_a.php.

⁴³ Matthew Levitt, "Are We Winning the Financial War on Terror?," *Middle East Strategy at Harvard*, January 25, 2008, http://blogs.law.harvard.edu/mesh/2008/01/financial_war_on_terrorism/.

⁴⁴ Matthew Levitt and Michael Jacobson, "The Money Trail: Finding, Following, and Freezing Terrorist Finances," Policy Focus #89, The Washington Institute for Near East Policy, November 2008. p. 17. <http://www.washingtoninstitute.org/pubPDFs/PolicyFocus89.pdf>.

⁴⁵ Courtney J. Linn, "How Terrorists Exploit Gaps in U.S. Anti-Money Laundering Laws to Secrete Plunder," *Journal of Money Laundering Control*, Volume 8, Issue 3 (2005) pp. 200-214.

⁴⁶ Matthew Levitt, Hearing on "The Role of Charities and NGOs in the Financing of Terrorist Activities," U.S. Senate Committee on Banking, Housing and Urban Affairs, Subcommittee on International Trade and Finance, August 1, 2002, http://banking.senate.gov/02_08hrg/080102/levitt.htm.

attacks.⁴⁷ After getting Moussaoui, the discovery of his receipt of \$35,000 from the terrorist group Jemaah Islamiah enabled the United States to establish links to Al Qaeda associated operatives in Malaysia. Ultimately, financial links to key Al Qaeda money-men were some of the first pieces of information that confirmed many terrorism experts' suspicion that 9-11 was in fact an Al Qaeda operation.⁴⁸

Lastly, critics of the financial war on terror forget that the precise effects of economic tools like sanctions, SAR's, and material support/money laundering prosecutions aren't always that easy to measure.⁴⁹ Not only is it difficult to counterfactually determine if an attack could have been possible with less cash or what the strength of a given terrorist organization would be without imposing financial pressure on it but the deterrent aspect is often difficult to measure precisely as well. Sanctions and strict 'know your customer' regulations don't merely punish and preclude individuals that are currently engaged in terrorism financing, but also deter other parties who might otherwise be willing to bankroll terrorist activity and organizations.⁵⁰ The instances where individuals have hesitated to provide logistical, financial or political support to terrorism because of the potential financial penalties they would incur will remain unknown. Even when deterring perpetrators forces them to merely use alternative, less regulated means of remittance, that is a victory for law enforcement because it complicates terrorist operations, forcing them to use less reliable and less efficient methods. This positive externality of deterrence is often overlooked.

⁴⁷ John Rosenthal, "Doing Justice to Zacarias Moussaoui," *Policy Review*, Hoover Institution, December 2007-January 2008, <http://www.hoover.org/publications/policyreview/11886641.html>.

⁴⁸ Matthew Levitt, Hearing on "The Role of Charities and NGOs in the Financing of Terrorist Activities," U.S. Senate Committee on Banking, Housing and Urban Affairs, Subcommittee on International Trade and Finance, August 1, 2002, http://banking.senate.gov/02_08hrg/080102/levitt.htm.

⁴⁹ Michael Kraft, "Iran: Cutting Airlinks – Another sanctions tool," *Counterterrorism Blog*, October 11, 2007, http://counterterrorismblog.org/2007/10/iran_cutting_air_links_another.php.

⁵⁰ Patrick Obrien, "U.S. Financial Pressure on Terrorists and Rogue Regimes, Speech Prepared for Delivery at the Washington Institute for Near East Policy, Special Events" *The Washington Institute for Near East Policy*, March 3, 2008, <http://www.washingtoninstitute.org/templateC07.php?CID=390>.

Section Three: The Holy Grail of Public-Private Counterterrorism Cooperation

"The next wall to tear down is between government agents and American bankers. When this occurs, the fields of counterterrorism and money laundering will be finally wedded, to the benefit of all Americans."⁵¹

According to the 9-11 Commission's Monograph on terrorism financing, "the United States' method to prevent criminals from taking advantage of the financial system relies on the basic premise that financial institutions—not the government—are in the best position to detect money laundering and related illicit transactions."⁵² But using banks to detect terrorism financing isn't always so simple. Terrorist organizations' funds often have a 'clean' origin, either from a charity or a legitimately owned business.⁵³ It's only once the money is put in the hands of a known terrorist that the money becomes 'dirty.'⁵⁴ Furthermore, bank's reliance on computerized systems to detect terrorism financing is problematic, as there is no pre-defined pattern of activity, resulting in an unwieldy amount of false-positives.⁵⁵ Detecting terrorism financing without additional intelligence collection and analysis is about as difficult as finding an needle in a haystack.⁵⁶

Law enforcement has access to government databases, 'national technical means' of intelligence collection, and mandatory institutional filings through the Bank Secrecy Act, but not to the actual financial institution records themselves. Moreover, BSA data is only useful to FinCEN if banks are

⁵¹ Jeffery Breinholt, "The Holy Grail of Public-Private Counterterrorism Cooperation," *Counterterrorism Blog*, May 23, 2007, http://counterterrorismblog.org/2007/05/the_holy_grail_of_publicprivat.php.

⁵² John Roth, Douglas Greenburg, and Serena Wille, "Monograph on Terrorist Financing," *National Commission on Terrorist Attacks Upon the United States*, 2004, http://www.911commission.gov/staff_statements/911_TerrFin_Monograph.pdf.

⁵³ Jonathan Winer, "Money Laundering: Through the Wringer," *The Economist*, April 14, 2001, pp. 64-66.

⁵⁴ Stefan D. Cassella, "Reverse Money Laundering," *Journal of Money Laundering Control* Volume 7, Issue 1 (2003) pp. 92-94.

⁵⁵ Tom Lasich, "The Complex Issue of Blending the Capacities of Law Enforcement and Financial Institutions for the Purpose of Countering Terrorism Financing," *International Seminar on Combating the Financing of Terrorism*, Davos, Switzerland, 1-3 October 2008, http://www.baselgovernance.org/fileadmin/docs/Giessbach_II/11_Workshop_III_-_TL.pdf.

⁵⁶ Anne Clunan, "U.S. and International Responses to Terrorism Financing," *Strategic Insights*, Volume IV, Issue 1 (January 2005) <http://www.ccc.nps.navy.mil/si/2005/Jan/clunanJan05.asp>.

doing an adequate job with their reporting requirements. Since 2002 the number of SAR filings has exploded, law enforcement is practically drowning in them because of ‘defensive’ filings.⁵⁷ In other words, banks don’t always have the resources or the political will to engage in thorough due diligence, in which case they over-report suspicious activity to reduce the risk of being held liable. Although the number of SARs for terrorism financing has decreased slightly every year since 9-11, indicating that banks have become more circumspect in their filing, the goal should be to reduce the burden on compliance offices to obviate the need for defensive filings all together.⁵⁸ Achieving that goal without easing up on reporting requirements is the tricky part.

Clearly both sides - law enforcement and banks - are missing crucial parts of the counterterror finance equation. When the assets of both are combined, it engenders actionable intelligence. The ultimate question is, how can the vast amounts of information available at banks be combined with sensitive law enforcement data in a way that both protects privacy rights and doesn’t compromise classified information?⁵⁹

The best way to improve public-private cooperation between banks and law enforcement is to grant top-secret level clearances to a certain number of bank compliance officers in the United States. This would effectively set up a “secure channel” of information sharing between banks and law enforcement. According to the Undersecretary for Terrorism and Financial Intelligence, Stuart Levy,

⁵⁷ According to the Financial Intelligence Unit head at the U.S. Branch of a European Bank, post 9-11 banks filed SARs like mad, thinking everything that transpired in the Middle East was somehow related to terrorism financing. Interview by author, April 22, 2009.

⁵⁸ Data on SAR filings can be found here, “SAR Activity Review, By the Numbers,” Financial Crimes Enforcement Network, U.S. Department of Treasury, http://www.fincen.gov/news_room/rp/sar_by_number.html. Compliance offices have become more circumspect in SAR filing according to the Financial Intelligence Unit head at the U.S. Branch of a European Bank, interview by author, April 22, 2009.

⁵⁹ Tom Lasich, “The Complex Issue of Blending the Capacities of Law Enforcement and Financial Institutions for the Purpose of Countering Terrorism Financing,” *International Seminar on Combating the Financing of Terrorism*, Davos, Switzerland, 1-3 October 2008, http://www.baselgovernance.org/fileadmin/docs/Giessbach_II/11_Workshop_III_-_TL.pdf.

much of the information held by law enforcement about whom and what to look for is classified.⁶⁰ Intelligence agencies have an obligation to protect their sources and methods, making secrecy an imperative.⁶¹ Furthermore, law enforcement is often reticent about declassifying, or 'downgrading' intelligence in order to protect ongoing investigations.⁶² In addition to intelligence and investigatory concerns, individuals or companies will occasionally remain off OFAC's list of designated entities due to policy considerations or diplomatic sensitivities.⁶³

As discussed already, detecting terrorism financing is possible, but very difficult. Experienced industry experts frequently opine that law enforcement doesn't provide adequate intelligence to effectively focus their monitoring capabilities.⁶⁴ They contend that without specific actionable information, detecting terrorism financing is virtually impossible.⁶⁵ Clearing select bank employees is thus crucial so that the government can provide as much detailed evidence as possible.⁶⁶ Every action taken to increase the possibility of detection increases the probability.⁶⁷ With a secure framework for information sharing, several new avenues to combat terrorism financing become possible.

⁶⁰ Department of Treasury Office of Public Affairs, "Testimony of Stuart Levey, Undersecretary of Terrorism and Financial Intelligence, Department of Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations," U.S. Treasury Department, July 11, 2006, <http://www.house.gov/financialservices/media/pdf/071106sl.pdf>.

⁶¹ Robert Werner, "U.S. Efforts Against Terrorism Financing: A View from the Private Sector," Policy Watch #1251: Special Forum Report, The Washington Institute for Near East Policy, June 26, 2007, <http://www.washingtoninstitute.org/templateC05.php?CID=2627>.

⁶² Department of Treasury Office of Public Affairs, "Testimony of Stuart Levey, Undersecretary of Terrorism and Financial Intelligence, Department of Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations," U.S. Treasury Department, July 11, 2006, <http://www.house.gov/financialservices/media/pdf/071106sl.pdf>.

⁶³ Matthew Levitt and Michael Jacobson, "The Money Trail: Finding, Following, and Freezing Terrorist Finances," Policy Focus #89, The Washington Institute for Near East Policy, November 2008. p. 3. <http://www.washingtoninstitute.org/pubPDFs/PolicyFocus89.pdf>.

⁶⁴ Dennis Lormel, Former Chief of Terrorism Financing Operations Section, Counterterrorism Division, FBI, interview by author, April 13, 2008.

⁶⁵ Ibid.

⁶⁶ Department of Treasury Office of Public Affairs, "Testimony of Stuart Levey, Undersecretary of Terrorism and Financial Intelligence, Department of Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations," U.S. Treasury Department, July 11, 2006, <http://www.house.gov/financialservices/media/pdf/071106sl.pdf>.

⁶⁷ Dennis Lormel, Former Chief of Terrorism Financing Operations Section, Counterterrorism Division, FBI, interview by author, April 13, 2008.

First, FBI intelligence could be scrubbed against bank monitoring systems, enabling them to recognize “hits” on individuals or transactions which pose a money laundering or terrorism finance risk.⁶⁸ For example, if the government was monitoring individuals they thought were planning an attack, the agency involved could pass that information onto banks in the hope that a bank account could be identified. Using account analysis, individuals or companies the suspect has had financial interactions with could be identified for the purposes of creating leads, identifying accomplices, or determining a target.⁶⁹ Linking individuals, accounts, and money changers together in this manner is crucial because it leads authorities to conduits between terrorist organizations and individual cells.⁷⁰ A simple investigative identification through this process could result in the dismantling of an entire criminal organization or the prevention of a terrorist attack.⁷¹

The complexities of international financial flows give criminal groups and terrorist organizations ample opportunities to ‘mask’ their transactions, making it difficult for U.S. banks to know the origin or ultimate destination of funds.⁷² This is especially true since U.S. banks are often only implicated in overseas financing through a tangential transaction which merely involved the U.S. for the purposes of using dollar-denominated assets.⁷³ If banks had access to classified information about potential terrorism fundraisers or cells abroad, it would improve their ability to ‘red-flag’ international

⁶⁸ Jonathan Weiner, former U.S. Deputy Assistant Secretary of State for International Law Enforcement, interview by author, April 5, 2008.

⁶⁹ Dennis Lormel, Former Chief of Terrorism Financing Operations Section, Counterterrorism Division, FBI, interview by author, April 13, 2008.

⁷⁰ Matthew Levitt and Michael Jacobson, “The Money Trail: Finding, Following, and Freezing Terrorist Finances,” Policy Focus #89, *The Washington Institute for Near East Policy*, November 2008. p. 5, <http://www.washingtoninstitute.org/pubPDFs/PolicyFocus89.pdf>.

⁷¹ Marcy M. Forman, “Combating terror financing and other financial crimes through private sector partnerships,” *Journal of Money Laundering Control*, Vol. 9, Issue 1, 2006. p. 114.

⁷² Victor Comras, “Let’s Make Fighting Terrorism Financing An International Battle,” *Counterterrorism Blog*, February 15, 2008, http://counterterrorismblog.org/2008/02/lets_make_fighting_terrorism_f.php.

⁷³ Clearing transactions in dollars in London or Hong Kong raises suspicions, see Review and Outlook, “Morgenthau vs. Tehran,” *The Wall Street Journal*, April 9, 2009, <http://online.wsj.com/article/SB123923602366403369.html>.

transactions that they normally only find out about after the fact since they lack any information that could have forewarned them.⁷⁴

Second, real-time intelligence would facilitate compliance offices' ability to run their own models and better develop due diligence algorithms or identify case typologies to indentify patterns of activity.⁷⁵ This could be done by allowing financial institutions access to certain Federal Bureau of Investigation, Department of Treasury, Central Intelligence Agency and even Immigration and Customs Enforcement databases. The FBI's Investigative Data Warehouse, which is a centralized database containing criminal records from law enforcement, FinCEN data, and public records data, would be a particularly useful tool.⁷⁶ The federal government, in cooperation with financial institutions, could even create a specific database to pool information relating to terrorism financing for the exclusive use of financial institutions. Banks already use a "fraudnet" database that a terrorism financing database could be modeled after.⁷⁷

Third, the government could develop working groups composed of law enforcement and intelligence officials and cleared financial institution officials. Former FinCEN and OFAC director Robert Werner has proposed this approach, advocating granting security clearances to the private-sector members to allow them to constructively participate in formalized discussions.⁷⁸ A formal working group could operate under the auspices of the Bank Secrecy Act Advisory Group. Created in 1994, the BSSAG's membership is comprised of individuals from law enforcement, regulatory authorities, and financial

⁷⁴ Victor Comras, "Let's Make Fighting Terrorism Financing An International Battle," *Counterterrorism Blog*, February 15, 2008, http://counterterrorismblog.org/2008/02/lets_make_fighting_terrorism_f.php.

⁷⁵ Jeffery Breinholt, "New Report on Bank Terrorism Liability," *Family Security Matters*, February 8, 2008, <http://www.fsarchives.org/article.php?id=1386560>.

⁷⁶ Michael J. Sniffen, "Obama Keeping FBI Database Details a Secret," *Denver Post*, April 19, 2009. http://www.denverpost.com/cj_12177992?source=rss.

⁷⁷ Matthew Levitt and Michael Jacobson, "The Money Trail: Finding, Following, and Freezing Terrorist Finances," Policy Focus #89, *The Washington Institute for Near East Policy*, November 2008. p. 47, <http://www.washingtoninstitute.org/pubPDFs/PolicyFocus89.pdf>.

⁷⁸ Tom Lasich, "The Complex Issue of Blending the Capacities of Law Enforcement and Financial Institutions for the Purpose of Countering Terrorism Financing," *International Seminar on Combating the Financing of Terrorism*, Davos, Switzerland, 1-3 October 2008, http://www.baselgovernance.org/fileadmin/docs/Giessbach_II/11_Workshop_III_-_TL.pdf.

institutions who are selected in order to solicit advice on the administration of the Bank Secrecy Act.⁷⁹ BSSAG's goal is to improve information flows between the private and public sector and it has adopted information sharing as a priority.⁸⁰ The BSSAG would thus be a natural fit. This working group would be a powerful liaison mechanism, allowing law enforcement to better learn the intricacies of the banks' systems, and allow compliance officers to increase their understanding of the terrorist threat.

Additionally, the working group could be tasked with ensuring the effectiveness of this new anti-terrorism financing asset; having cleared compliance officers. It could conduct training on how to use government databases, how to ensure intelligence remains classified, and address other issues that might stand in the way of information sharing. Based on the 9-11 Commission Report's publicized objections to providing clearances to banks, the issues most likely to come up would be privacy and civil liberty issues.⁸¹

The U.S. could base its model on Britain's "Vetted Group" established by their Serious Organized Crime Agency (SOCA). The Vetted Group is unique in that it is an active producer of intelligence. Members review SOCA intelligence and then produce a declassified document in the form of an Intelligence Alert. SOCA then circulates the Alert to relevant industries, as it is specifically tailored to be as relevant and meaningful to the private sector audience as possible. Private sector members of the group are thus able to add-value to government produced intelligence.⁸²

⁷⁹ Financial Crimes Enforcement Network, U.S. Department of the Treasury, "Unauthorized Disclosure of Suspicious Activity Reports," August 18, 2004, <http://files.ots.treas.gov/480024.pdf>.

⁸⁰ Department of Treasury Office of Public Affairs, "Testimony of Stuart Levey, Undersecretary of Terrorism and Financial Intelligence, Department of Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations," U.S. Treasury Department, July 11, 2006, <http://www.house.gov/financialservices/media/pdf/071106sl.pdf>.

⁸¹ John Roth, Douglas Greenburg, and Serena Wille, "Monograph on Terrorist Financing," *National Commission on Terrorist Attacks Upon the United States*, 2004, http://www.911commission.gov/staff_statements/911_TerrFin_Monograph.pdf.

⁸² HM Treasury, "The financial challenge to crime and terrorism," February 2007, http://www.hm-treasury.gov.uk/d/financialchallenge_crime_280207.pdf.

Critics might contend that the status quo already possesses a mechanism for information sharing between banks and law enforcement under FinCEN's Section 314(a) requirements.⁸³ Law enforcement agencies have the ability request information via FinCEN from 45,000 points of contact throughout U.S. financial institutions.⁸⁴ Every two weeks, FinCEN sends information to a secure server and financial institutions check their records for data matches. Although the program thus far has claimed results, it is only a half-measure. First, agencies must certify that the money laundering activity is 'significant' before submitting a request for information.⁸⁵ This is problematic for terrorism related investigations. First of all, it may not even be a criminal transaction, but merely paying for a mundane "pre-crime" item such as food, lodging or transportation.⁸⁶ Additionally, when using financial intelligence to investigate a terrorism suspect, the financial activity may not be 'significant' but it may be crucial to determine links to a broader terrorist organization, to determine accomplices or to determine a suspect's location. Second, the agency must certify that all other methods of investigation have been exhausted.⁸⁷ This decreases the likelihood that the information gained will be actionable since it delays the request until other methods have been pursued.⁸⁸ Third, banks can only give information for accounts dating back one year and transactions dating the last six months, limiting the scope of information available.⁸⁹ Even worse, law enforcement is often reluctant to use section 314(a) as they

⁸³ Michael Braun, former Chief of Operations for the Drug Enforcement Agency, interview with author, April 6, 2008. Braun indicated that during his time at the DEA, he was not aware of any difficulties sharing information with banks using the Patriot Act.

⁸⁴ Financial Crimes Enforcement Network, Department of Treasury, FinCEN's 314(a) Fact Sheet, April 29, 2009, http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf.

⁸⁵ Ibid.

⁸⁶ Anne Clunan, "U.S. and International Responses to Terrorism Financing," *Strategic Insights*, Volume IV, Issue 1 (January 2005) <http://www.ccc.nps.navy.mil/si/2005/Jan/clunanJan05.asp>.

⁸⁷ Financial Crimes Enforcement Network, Department of Treasury, FinCEN's 314(a) Fact Sheet, April 29, 2009, http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf.

⁸⁸ Quick action is key, see Anne Clunan, "U.S. and International Responses to Terrorism Financing," *Strategic Insights*, Volume IV, Issue 1 (January 2005) <http://www.ccc.nps.navy.mil/si/2005/Jan/clunanJan05.asp>.

⁸⁹ Financial Crimes Enforcement Network, Department of Treasury, FinCEN's 314(a) Fact Sheet, April 29, 2009, http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf.

fear disclosing their sources and methods.⁹⁰ If banks had the necessary clearance and ability to protect classified information, it could alleviate law enforcement's concern. Providing security clearances is thus the best mechanism to generate the most meaningful and most actionable financial intelligence.⁹¹

A potential hurdle would be how to handle correspondent accounts. A cleared employee at a U.S. bank would not be able to share classified information with individuals at the bank's overseas compliance office.⁹² This could potentially disrupt the chain of command at the bank, elevating the U.S. compliance officer's importance. It could also be seen as a security risk, creating a situation where the U.S. employee would be pressured to justify its actions to overseas compliance offices by leaking classified information. However, it seems likely that foreign banks would be willing to accept the responsibility. The Patriot Act's regulations for correspondent accounts mean that all of the foreign bank's transactions involving U.S. financial institutions must meet U.S. anti-money laundering standards.⁹³ Otherwise, their assets in U.S. accounts can be seized.⁹⁴ This makes foreign institutions vulnerable to penalties for allowing their customers to do business with U.S. banks which would be completely legal in their country of origin.⁹⁵ As a foreign banks, have to either pull out of U.S. markets or assume the cost of initiating more stringent AML/CTF standards.⁹⁶ With this dilemma in mind, the privilege of extra intelligence from the U.S. government might tip the decision towards continuing to maintain their American correspondent accounts.

⁹⁰ Robert Werner, "U.S. Efforts Against Terrorism Financing: A View from the Private Sector," Policy Watch #1251: Special Forum Report, The Washington Institute for Near East Policy, June 26, 2007, <http://www.washingtoninstitute.org/templateC05.php?CID=2627>.

⁹¹ Dennis Lormel, Former Chief of Terrorism Financing Operations Section, Counterterrorism Division, FBI, interview by author, April 13, 2008.

⁹² Ibid.

⁹³ Loretta Napoleoni, *Terrorism Incorporated: Tracing the dollars behind the terror networks*, (New York: Seven Stories Press, 2005) p. 214-215.

⁹⁴ Iyandra Smith, "The USA – no longer a haven for the foreign bank," *Journal of Money Laundering Control*, Vol. 11 Issue 3 (2008) pp. 199-209.

⁹⁵ Victor Comras, "Let's Make Fighting Terrorism Financing An International Battle," *Counterterrorism Blog*, February 15, 2008, http://counterterrorismblog.org/2008/02/lets_make_fighting_terrorism_f.php.

⁹⁶ Iyandra Smith, "The USA – no longer a haven for the foreign bank," *Journal of Money Laundering Control*, Vol. 11 Issue 3 (2008) pp. 199-209.

The last advantage relates to banks 'routine transaction' defense. The threat of civil liability under the Anti-Terrorism Act could operate as an incentive for banks to engage in stringent know your customer investigations.⁹⁷ Unfortunately, financial institutions are relying upon a legal defense which eliminates that incentive by shielding them from liability on the basis that they were merely providing a "routine business transaction."⁹⁸ The hope is that if the federal government began to provide banks with real-time intelligence, it would complicate their ability to claim to have been unwitting providers of routine services.⁹⁹ The civil liability could thus incentivize bank's ability to utilize their access to classified information to the maximum extent possible.

Bank regulators already have a duty to protect confidential bank records, making them ideal candidates for being able to secure top-secret level intelligence.¹⁰⁰ Granting clearances in this context is not unprecedented. Scores of defense contractors are given top-secret level clearances in order to do their job, banks should be granted such a privilege as well.¹⁰¹ Considering bank compliance officers are the government's eyes and ears at the gates of the financial system, they are entitled to some benefits.¹⁰²

⁹⁷ Jeffery Breinholt, "The Bank Secrecy Act for Beginners," *Counterterrorism Blog*, February 14, 2008, http://counterterrorismblog.org/2008/02/the_bank_secrecy_act_for_begin.php.

⁹⁸ Steven I. Landman, Bank Liability Under the Anti-Terrorism Act, February 2, 2008, International Assessment and Strategy Center, http://strategycenter.net/docLib/20080202_BankLiability_Landman.pdf.

⁹⁹ Jeffery Breinholt, Deputy Chief of the Counterterrorism Section, Department of Justice, interview by author, April 2009.

¹⁰⁰ Jonathan Weiner, former U.S. Deputy Assistant Secretary of State for International Law Enforcement, interview by author, April 5, 2008.

¹⁰¹ Jeffery Breinholt, "New Report on Bank Terrorism Liability," *Family Security Matters*, February 8, 2008, <http://www.fsarchives.org/article.php?id=1386560>.

¹⁰² Jeffery Breinholt, "The Bank Secrecy Act for Beginners," *Counterterrorism Blog*, February 14, 2008, http://counterterrorismblog.org/2008/02/the_bank_secrecy_act_for_begin.php.

Conclusion

Combating terrorism financing has achieved numerous successes as a counterterrorism tool, but it is important not to become complacent. When one avenue for illicit finance is shut off, organizations devote their efforts to finding another, acting like the “archetypal shark in the water that must keep moving forward—no matter how slowly or incrementally—or die.”¹⁰³ The evidence indicates terrorist organizations study our counterterrorism finance efforts in order to avoid them. When Zacharias Moussoui entered the U.S. with 30,000 dollars on his person, he smartly filed a Currency and Monetary Instrument Report, shielding himself from bulk cash smuggling charges.¹⁰⁴ A recently discovered “jihadi discussion forum” post gives specific instructions on how to safely finance jihadist website activity without being monitored by government intelligence. It states,

*“And I do not exaggerate when I say that most of the monitoring of electronic Jihadi works, identifying the administrators, and tracing their locations are done via tracing the methods of payments that they use starting from the last thread and reaching to main source of payment, which is The Brother, and from there the rest of the contacted brothers get traced.”*¹⁰⁵

Terrorist’s extensive counter-intelligence work make efforts to plug the holes in the U.S. anti-money laundering and counterterrorism finance regime crucial.¹⁰⁶ The first step is to ensure current regulations work effectively via improving the two-way flow of information between the public and private sector. With this new framework for cooperation, efforts can next shift towards regulating check cashers, unlicensed money service businesses, and innovations in electronic payment systems. Law enforcement and banks must work together to innovate their efforts quicker than those engaged in illicit finance in order to maintain decision-cycle dominance.

¹⁰³ Bruce Hoffman, “Countering Terrorists’ Use of the Web as a Weapon,” *CTC Sentinel, Combating Terrorism Center at West Point*, 1 no. 1, (December 2007), <http://ctc.usma.edu/sentinel/CTCSentinel-Vol1Iss1.pdf>.

¹⁰⁴ Jeffery Breinholt, “The Bank Secrecy Act for Beginners,” *Counterterrorism Blog*, February 14, 2008, http://counterterrorismblog.org/2008/02/the_bank_secrecy_act_for_begin.php.

¹⁰⁵ NEFA Foundation TerrorWatch, “Jihadi Discussion Forum Posting on Safely Financing Jihad-Related Websites,” NEFA Foundation, April 7, 2009, <http://www.nefafoundation.org/miscellaneous/FeaturedDocs/nefafinancejihadsites0409.pdf>.

¹⁰⁶ Courtney J. Linn, “How Terrorists Exploit Gaps in U.S. Anti-Money Laundering Laws to Secrete Plunder,” *Journal of Money Laundering Control*, Volume 8, Issue 3 (2005) pp. 200-214.