Medea Group
Innovative Security and Development

Dynamic Threats of Jihadist Money Laundering

Implications in Commercial Banking

June 2007

Introduction

This is the second in a series of six papers discussing the money laundering practices of Islamic terrorist groups and the implications therein. The focus of this paper on the commercial implications of money laundering will pay particular attention to Western Banks, Islamic Financial Institutions and Offshore Banking. Discussion will pivot on legal dynamics intended to dissuade exploitation and corruption within the financial system including the USA PATRIOT Act, the Financial Action Task Force (FATF) and Islamic legal rulings, in addition to collaborative banking relationships and private banking. The analysis will attempt to answer the fundamental question of why expanded legal models have been unable to stem the tide of terrorist money laundering practices and the commercial implications of those policies and their failures.

Attention will also be placed upon the differences between money laundering and terrorist financing and the elements which make it exceedingly difficult to prevent a terrorist attack by 'following the money.'

Accurately discussing terrorist money laundering practices necessitates a dissection and clarification of two often grouped but diametrically opposed activities: terrorist financing and money laundering. Money laundering by definition begins with dirty money, whether from criminal proceeds, extortion, narcotics, etc., that needs to be 'washed' in order to be reintroduced elsewhere as clean. Under normal circumstances this includes the breaking up and moving around of large amounts of money, as criminal proceeds often number in the millions.

Terrorist financing contrasts drastically with this model, however before engaging in the differences, the term must be spliced. Terrorist financing refers to two different aspects of the terrorist monetary spectrum: fundraising and operations. The first distinction from money laundering is terrorist fundraising and financing often begin as clean money and becomes dirtied as a product of their application. In this vein, it is far more difficult to track until after the event, at which point the damage has been done. Secondly, the operational funding of terrorist events often involves the movement of small amounts of funds at irregular intervals to a number of different accounts.

While there is obviously an interrelationship between terrorist fundraising and money laundering it remains critical to understand the fundamental differences between the two.

In order to better frame the discussion, the scope of the problem will now be presented.

Scope

While expert estimates set the value of laundered currency flow as high as US$2.85 trillion annually,[1] most agree at least $1-2 trillion is moving through legal financial networks, about half of which is via the United States.[2] To put these numbers in more

identifiable terms, the amount of money laundered annually lies somewhere between the GDPs of Germany and Spain.[a]

While there are clearly other methods of moving illicit currency quietly across borders, this paper focuses on legal financial channels. This is the method with the most oversight and therefore should show the most successful implementation of anti-money laundering (AML) tactics. This paper demonstrates while sufficient legislation is in place to slow or even shut down illicit financial flows via legal pipelines, banking entities do not want to reduce their access to such large volumes of funds. Illicit finances present an excellent value to the financial marketplace as: "Money launderers, including both transnational corporations and the public officials who are bribed by them in their own countries or overseas are not normally a credit risk, so there is no normal prudential risk in accepting them as clients or in accepting their funds."[3]

To accurately portray the problems inherent in legal AML and anti-terrorist financing mechanisms and their commercial implications, a detailed account of such legislation is now presented.

Legal Mechanisms to Prevent Money Laundering and Terrorist Financing

The commercial world understands its susceptibility to exploitation by the darker forces of the market. It has endeavored to either take advantage of opportunities presented by those elements or protect their networks from illicit uses. To the second end, a number of processes have been developed, whether political, legal or religious, to deter negative manipulation of market forces. The next section outlines three very different attempts to regulate financial marketplaces in an effort to prevent money laundering, and the commercial implications of each: the Patriot Act, Sharia law and the FATF.

Patriot Act

On October 26, 2001, the United States upped the ante in the war on terrorist financing by passing into law the comprehensive anti-terror legislative package known as the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism). Among the gifts it bestowed upon law enforcement were stringent regulations on currency flow and greater oversight of U.S. and non-U.S. financial institutions doing business in America or with U.S. companies abroad. It requires all U.S. financial entities transferring funds and engaging in large cash transactions to exercise due diligence before granting a non-U.S. institution access to the American financial system via a correspondent account or relationship.[4] Correspondent relationships will be discussed in a later section. Additionally, all U.S. financial entities are now required to have AML programs, such as know your customer (KYC) protocols and other methods meant to identify customers or, minimally, the source of deposits.[5]

[a] 2006 estimated Gross Domestic Product of Germany – $2,585,000,000,000; Spain – $1,070,000,000,000 Source – CIA World Factbook, Rank Order – GDP; available at https://www.cia.gov/library/publications/the-world-factbook/rankorder/2001rank.html

Furthermore, "U.S. banks and security firms are barred from opening accounts for non-U.S. shell banks with no physical presence anywhere and no affiliation with another bank".[6] Significantly the Act extends U.S. jurisdiction, enabling the seizure of U.S. accounts held by non-Americans.[7] With regard to the private accounts of foreign elite, in excess of US$1million, section 312 mandates the financial institution take reasonable steps "to ascertain the identity of the nominal and beneficial owners of, and the source of funds deposited into, such account as needed to guard against money laundering and report any suspicious transactions."[8]

The Patriot Act met with some initial success and has had its share of achievements. FinCEN (U.S. Department of Treasury - Financial Crimes Enforcement Network), with support from Patriot Act legislation, has successfully prosecuted some of the largest financial institutions with record fines for lack of compliance with U.S. AML requirements. Dutch major ABN AMRO was fined US$80 million for operating unsupervised correspondent relationships with small Russian financial institutions, posing a "substantial risk of money laundering" in which roughly half of the accounts were missing the required AML documentation.[9]

Florida based Bank Atlantic suffered a US$10 million penalty for running a fund transfer center in which they failed to report "a substantial number" of suspicious transactions.[10]

These cases, among others, serve to create an illusion whereby the Patriot Act successfully deters money laundering activities. While recent legislation has provided substantially more bite than previous policies, punishments remain far too weak to serve as actual deterrents for financial institutions to take notice and amend fraudulent activities.

Money Laundering through U.S. Banks since the Patriot Act
The following is a short list of major money laundering operations conducted via American financial networks *since* the passage of the Patriot Act. These were revealed by an intensive New York District Attorney's investigation concluded in December 2005.

a. From May 2002 to April 2004, over US$3 billion flowed through a Uruguayan remitter's account at Bank of America, most of which "originated from offshore shell companies chartered in Panama and the British Virgin Islands and controlled by illegal Brazilian money service operations."[11] Bank of America was fined US$7.5 million and was required to assist the District Attorney in other investigations.[12]

b. In December 2005, a settlement agreement was reached between the District Attorney's Office and Israel Discount Bank of New York (IDBNY), after the investigation revealed $2.2 billion was moved by illegal Brazilian money transmitters through IDBNY's New York office over a five-year period.[13] Their penalty was to enhance their internal AML controls and a pay a fine of US$8.5 million, with a possibility of additional damages not to exceed US$16.5 million.[14] It was recently reported IDBNY "managed Iranian accounts and transferred funds to citizens of the Islamic Republic,"[15] calling into question the severity of this particular exploitation.

c. Beacon Hill Services Corporation of Midtown Manhattan was convicted in February, 2004 of operating as an unlicensed money transmitter. Over its last six years of operation, more than $6.5 billion was moved through accounts it maintained at JP Morgan Chase.[16] Due to Beacon Hill's shoddy record-keeping, it has been nearly impossible to back-trace financial movement and identifies parties behind transactions or even identifies all the money which passed through the company's accounts. However, "Records were recovered showing that Beacon Hill transmitted $31.5 million to accounts in Pakistan, Lebanon, Jordan, Dubai, Saudi Arabia, and elsewhere in the Middle East."[17] Beacon Hill was shut down and forced to forfeit US$15 million.[18]

Despite Beacon Hill's closure these three cases represent a maximum total of $39 million in fines versus $11.7 billion in illegal transfers. This disparity presents the obvious reality that profit available to banks by currency transfer alone outweighs the penalties incurred by exposure and by extension the ineffectiveness of the American AML policies.

In order to approximate the amount of profit earned from $11.7 billion, the pricing tool at westernunion.com was employed. According to their price lists, Western Union receives anywhere from 2.5% on large economy transactions to as high as over 8% on quick, low currency transfers to or from remote locations. Additional transfers carry a charge of $10.99 on transfers below $100.[19] Even if the abovementioned banks received a meager 1% profit per transaction, the profit equaled $117 million or nearly three times the total fees imposed. The standard 2.5% profit brings the figure to nearly $293 million and at 8% the profit soars to $936 million.[20] While the profit is likely much closer to the initial figure cited, they clearly demonstrate a lack of deterrent power in the legislation.

While participation in terrorist money laundering by western banks will be discussed in a later section, the discussion now turns to Islam, where a stringent moral and legal code stands between Islamic banks and terrorist groups, well out of the sight and understanding of western investigators.

Sharia

The Sharia is the compendium of Islamic jurisprudence and as such only a small portion deals with monetary matters. This discussion focuses on these portions of its codes. Islamic financial institutions are famous for their adherence to the strictest interpretation of banking secrecy and confidentiality. A financial ocean unto themselves, this secrecy is frequently a cause of frustration for western investigators and intelligence operatives searching for hidden financial threads in an effort to prevent an attack or apprehend suspects. While commonly thought to be a breeding ground for the storage and transfer of illicit and hostile finances, in actuality financial institutions governed by Islamic jurisprudence are perhaps less likely to serve the interests of those who wish to do harm.

Despite popular perceptions, in Islam "the right of bank secrecy and confidentiality is not always absolute."[21] There are exceptions to the rule of bank secrecy and under certain, specific circumstances disclosure becomes mandatory. Such instances include:

a. When public interest dictates law and order should be maintained, the preservation of the public good overrides the protection of the right of privacy and secrecy. Situations where disclosure becomes mandatory in criminal cases are numerous, especially in economic crimes such as fraud, drug trafficking and money laundering.[22]

b. When an individual's right has been denied or encroached upon, the right of privacy and secrecy related to bank accounts would not be upheld.[23]

c. Disclosure of bank information to non-official applicants in response to and implementation of contractual provision.[24]

d. When there is a duty to make financial disclosure in accordance with due process of law.[25]

Under Sharia financial code, Islamic banks and institutions are forbidden from participating in financial transactions which lead to, or could be associated with: speculation, the accumulation and charging of interest and activities which could be viewed as unclean. These activities include gambling, prostitution and drug trafficking. [26] They are forbidden from participation in or receiving any illicit profits derived from illegal activities. Noted Islamic financial scholar Dr. Fath El Rahman Abdalla El Sheikh asserts:

> As these illegal activities are the major sources of dirty money to be laundered by many techniques most of which are accomplished by underground operations that may be beyond the reach of the competent authorities, it could be asserted that Islamic law is contributing to a great extent in the control of money laundering by combating its sources.[27]

The implication to the financial sector from a code which marries legal with moral justice poses an immensely powerful deterrent to illicit activities. Much of the Islamic world claims to adhere strictly to the tenets of the Sharia code, and financial networks often advertise product lines and investment opportunities that are not just clean, but pristine. As the Sharia prohibits much of the action being combated by the Patriot Act and similar legislative protocols in the West, its ramifications should be sufficient to prevent many of the illicit funds from flowing through Islamic financial pipes. Unfortunately, the Sharia code falls short of its intended goals, not through a flawed design but by the actions of its supporters.

As Dr. El-Sheikh expounds:

> Despite the Islamic commands given by the divine revelations, which should be followed in letter and spirit and cannot be violated or ignored on the basis of

> rational arguments or inner desires, there have been several violations in the practices of Islamic banks, other financial institutions and individuals who claim to carry out business in accordance with Sharia principles.[28]

Greed and lust for profit know no bounds; political, religious or otherwise. In the 1991 fraud case of BCCI (Bank of Credit and Commerce International), Islamic institutions and investors were encouraged to deposit substantial funds with the bank under the assurance all moneys invested would be in accordance with the Sharia.[29] It was later revealed BCCI had not invested as alleged, but rather in financing the drug trade and many other illegal activities. Proceeds were laundered by the bank in several jurisdictions and investors "lost more than US$800m in that unsuccessful venture."[30]

While most Islamic financial institutions and their employees adhere to this strict code of conduct, others believe laundering money in support of terrorist activities *is* in the letter of the law, and believers are not simply permitted, but encouraged to do so.

Islam is a noble, but complicated religion with a diversity of spiritual leaders, each claiming his voice to be that of Islamic truth. On occasion, the message becomes twisted. Since coming to power in 1989, The National Islamic Front Government (NIF) in Sudan:

> …has imposed a distorted Islamic code on all aspects of life, which unfortunately has provided a shelter for Islamic banks to perpetrate their corrupt practices and be used as conduits for funneling funds to Islamic fundamentalist organizations that took refuge in the Sudan by the collusion of the NIF in the early years of its regime.[31]

Despite the theoretical regulatory controls of banking activities under Islamic law, too many individuals are willing to turn a blind eye, even to their religious virtues, in order to make a profit or financially support a terrorist entity. Movements exist within Islamic circles to curb illicit financial practices but lack of oversight and adherence to confidentiality provide strong resistance to effective reform.

The flexibility of Sharia interpretation is a weak deterrent to money laundering and as a result has direct implications commercially. Money in the Islamic world flows through channels beyond normal mechanisms of oversight and a stringent moral code discouraging illicit financial transfer would certainly be a welcome ally in identifying terrorist monetary flows and running commercial businesses. The fruition of the unwinding of Shariatic adherence will be presented in the case study of Al Shamal Islamic Bank, later in this essay. Before our discussion turns in that direction, one additional AML system needs address: an international coalition spearheading the international war on terrorist financing and money laundering. The Financial Action Task Force is a global network of powerful, economic countries operating in collaboration to combat the twin flows of money laundering and terrorist funding.

<u>Financial Action Task Force (FATF)</u>

The global commercial and law enforcement sectors are no strangers to the threat posed by money laundering to the international banking system. The first super-national consortium to combat money laundering (later adapted to counter terrorist financial flows), the Financial Action Task Force was born in 1989 out of a consortium of G-7 member States, the European Commission and eight other countries.[32]

> The Task Force was given the responsibility of examining money laundering techniques and trends, reviewing the action which had already been taken at a national or international level, and setting out the measures that still needed to be taken to combat money laundering. [33]

The task force set international AML standards and revolutionized the industry with the enactment of its 40 recommendations on money laundering and nine special recommendations regarding terrorist financing. These set the guidelines for international AML policy and included many valuable and effective concepts for countering illicit financial flows, including:

5. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names. Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers…[34]

7. Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

    a. Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

    e. With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.[35]

18. Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.[36]

Special Rec. 2

> Each country should criminalize the financing of terrorism, terrorist acts and terrorist organizations. Countries should ensure that such offences are designated as money laundering predicate offences.[37]

Special Rec. 3

> Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.[38]

Special Rec. 7

> Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain. [39]

All member States and those with whom they conduct business are expected to abide by these recommendations. The coalition now boasts 33 members covering most of the industrialized world,[b] in addition to many "observers" and regionalized cooperatives.[40]

The FATF weighted its recommendations in 2000 with the release of the Non-Cooperative Countries and Territories (NCCT) list: a pseudo-blacklist of countries openly violating FATF anti-money laundering policies. In its first review, the FATF singled out 17 countries and territories as non-cooperative,[c] causing embarrassment and setting a serious precedent within the developing world. Although the FATF seemingly got off to a fast start, it had already started unraveling from within.

The operations and initiatives undertaken by the FATF were destined to failure from the start. The Task Force was designed to be a mechanism through which larger, established nation-states could monitor and pressure smaller countries into submission and adoption of internal AML legislation. The organization was not designed to be a governing body that would facilitate inquiry into the ethical business practices of its larger members. Between 2001 and 2002, according to its own assessment, "the US was in full compliance with only 19 of the 28 Task Force recommendations requiring specific action."[41] More importantly, the FATF never provided any effective oversight or

---

[b] Current list of FATF members: Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Co-operation Council, Hong Kong - China, Iceland, Ireland, Italy, Japan, Kingdom of the Netherlands, Luxembourg, Mexico, New Zealand, Norway, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States

[c] First NCCT List – June 22, 2000: Bahamas, Cayman Islands, Cook Islands, Dominica, Israel, Lebanon, Liechtenstein, Marshall Islands, Nauru, Niue, Panama, Philippines, Russia, St. Kitts and Nevis, and St. Vincent and the Grenadines

enforcement mechanism. While member States were required to adapt AML policies and pressure was placed on other, non-members to comply, there were no investigative means to ensure compliance by any member or non-member State. As British money laundering expert Peter Lilley noted, "Although the Financial Action Task Force has promoted best-practice principles to be adopted by all countries the simple truth is that there is no uniformity across the world in relation to anti-money laundering regulations and legislation."[42]

The most striking blow to the FATF's legitimacy as an international anti-money laundering body came when the 2006 annual NCCT report stated, "As of 13 October 2006, there are no Non-Cooperative Countries and Territories."[43] The publication of this statement undermined any legitimacy the organization may have had as an advisory body. This deficiency was highlighted in March of the following year (2007) when the U.S. Department of State released its annual report of Major Money Laundering Countries, identifying 59 countries and jurisdictions as locations of "primary money laundering concern."[44] This represented a substantial increase from 44 the year before.[45] These included notorious offshore locations such as Antigua and Barbuda, Bahamas, Belize, Cayman Islands, Isle of Man, St. Kitts and Nevis. Also included were classic transfer points for illicit finances including Afghanistan, Cambodia, Indonesia, Israel and the United Arab Emirates. More staggering was the branding of FATF member States Australia, Austria, Brazil, Canada, France, Germany, Greece, Hong Kong, Russia, Singapore, Spain, Switzerland, Turkey, the United Kingdom and the United States as locations of primary money laundering concern.

While the FATF continues to exist it has lost its accountability and with no mechanism for enforcing its recommendations it is little more than another bureaucratic layer that costs a lot of money and brings no results to the table.

A strategic design and implementation of the FATF could have directly influenced global commerce and administrative policy. By encouraging and pressuring countries and territories to adopt AML regulations, the organization demonstrated a positive influence. Unfortunately, when the founding members of the organization resist adoption of its core recommendations it is difficult to develop legitimate milestones. Enforced anti-money laundering systems with proper oversight in offshore locations could bring illicit finances into the light.

As shown in the previous sections, despite significant efforts on the part of the legislative community, no true advances have been made in the battle against terrorist financing and money laundering. Furthermore, "As money launderers become cleverer, they are studying the anti-money laundering regulations and devising methods of getting the money through without appearing on official radar screens."[46] This was demonstrated at great length in the first paper of this series, with particular attention placed upon digital currencies and online currency transfer mechanisms.

In all fairness to the financial institutions that genuinely want to crack down and which continue to be exploited:

> It has proved virtually impossible to 'spot' a terrorist prior to an attack – so how can it be logical to expect that those involved in terrorist financing can be identified with apparent ease by businesses (and more particularly employees of these businesses) who come in contact with them?[47]

There is one more important aspect to add to this discussion about AML legislation: the willing breach of the law by financial institutions. It is to this topic the discussion will now turn.

Money Laundering Through Western Banks

Impotence of / Blatant Disregard for AML Protocols

In an effort to curb the extensive use of Western banks by money launderers and terrorist entities:

> …the U.S. Congress has held numerous hearings, provided detailed exposés of the illicit practices of the banks, passed several laws and called for stiffer enforcement by any number of public regulators and private bankers. Yet the biggest banks continue their practices, [and] the sum of dirty money grows. [48]

Two fundamental justifications for this failure will now be presented, and while the first is American specific, it has ramifications for the entire system. There is a gaping loophole in Patriot Act legislation. While the Patriot Act carries a prohibition towards conducting business with shell institutions, there is an exemption "if the non-U.S. bank that has no physical presence is an affiliate of a U.S. *or non-U.S.* financial institution and is subject to supervision by a banking authority in the jurisdiction that regulates its affiliated financial institution." [49]

The clear intent of this exception is to provide financial freedom to U.S. institutions to establish business relationships with shell branches of reputable banks under the assumption there will be adequate supervision provided by the parent institution over its global offices, including shell branches. As thousands of international banks hold correspondence relationships with American banks, this loophole in the Patriot Act allows illicit finances to flow globally through the pipes of any bank that shares wires with U.S. institutions.

Second, and perhaps more importantly, is a fundamental lack of desire among financial institutions to eliminate the lucrative revenue provided by tainted money from their annual budgets. The distressing truth is "the biggest U.S. [and non-U.S.] banks, particularly Citibank, derive a high percentage of their banking profits from serving these criminal and dirty money accounts."[50]

These two flaws represent themselves through two of the biggest markets in the financial world: the private handling of elite client's funds and the interconnected world of

correspondence networks. Exploitation and misuse of these two economic staples will be discussed in the following sections.

Private Banking

There is nothing wrong per se with commercial institutions of any kind wanting to provide their clients with the best service possible, as long as that service falls within the confines of the law.

What has become common practice, according to John Reed, former CEO of Citigroup, is, "Private bankers tend to become advocates for their clients" and by doing so have "lost the detachment needed to monitor their transactions."[51]

Private banking in this analysis refers to any individually owned account with more than US$1 million under management at a particular financial institution. These clients receive personal treatment from account managers endeavoring to keep their customers happy. This aid comes in the form of investment advice but also manifests in the transfer of money to offshore accounts or disguising of a particular money trail's source.

At times private bankers openly defy the law to protect clients and their assets.

Illicit Use of Private Banking

High worth criminals and terrorists use private banking relationships to launder funds. In many cases, it is not so much a case of exploiting the banking networks as facilitating a situation which is mutually beneficial. The terrorist has his money disguised for later use or transfer, and the bank makes a hefty profit.

Private Banking represents big business. Citibank, the world's largest facilitator of private banking services, holds over $100 billion in client assets in private banking offices in 30 countries. [52] Professor James Petras of Binghamton University reports:

> Over the last 20 years, big bank laundering of criminal funds and looted funds has increased geometrically, dwarfing in size and rates of profit the activities in the formal economy. Estimates by experts place the rate of return in the PB [Private Banking] market between 20-25% annually.[53]

Legitimate, private banks provide offshore solutions and conduct business in secret jurisdictions such as Switzerland and Cayman Islands, where criminal charges can be brought on the disclosure of bank information.[54] The commercial implications of Private Banking relationships can best be demonstrated through a case study.

Case Study - Riggs Bank

Riggs Bank, one of the oldest and most prestigious banks in Washington D.C., courted business from former Chilean dictator Augusto Pinochet and helped him hide millions of dollars in assets from international prosecutors while under house arrest in Britain.[55] Despite willful knowledge of Pinochet's links to corruption, illegal arms and drug

trafficking and the disappearance or murder of thousands of political opponents during his reign,[56] Riggs made the corporate decision that risk of political fallout was less important than the financial opportunities presented by managing his accounts. In order to disguise his money, a Bahamas-based Riggs subsidiary established two companies, Ashburton Co. Ltd. and Althorp Investment Co. Ltd., both allegedly owned by trusts registered and managed by Riggs.[57]

According to a *Washington Post* article, "Nowhere on the trust or company documentation does Pinochet's name appear, though he and his family were the ultimate beneficiaries, according to investigators."[58]

In Spring 2002, the story broke when the Office of the Comptroller of the Currency (OCC) unraveled the deception after an OCC examiner started asking questions about Althorp and inquired about its "beneficial owner."[59]

This was only the beginning of the investigations into the management of Riggs' private clients and banking practices. In addition to the Pinochet accounts, an investigation by a Senate subcommittee found other "equally troubling" files on operations in Equatorial Guinea and more than 150 Saudi Arabian accounts.[60] In May 2002, the bank agreed to a civil penalty of $25 million for what federal regulators called "willful, systemic" violation of anti-money laundering laws.[61]

Commercial implications of the illegal manipulation of private banking operations are two sides of the same coin; profitability vs. brand liability and reduced market share. No organization wants to be branded as a facilitator of terrorist operations or international crime. In the case of Riggs Bank, once the Pinochet dealings became public, Congress launched an immediate investigation. The media persecuted the bank's Board. Eventually they were fined by the government and purchased by PNC Bank at a reduced price. Riggs jeopardized its own commercial future, but was well aware of the consequences prior to seeking out Pinochet's funds. This is the proof current AML policies are flaccid. When a financial institution is aware of the consequences of breaking the law but willfully does so in search of profits, the legal impediment to action has vanished. While Riggs, as a smaller financial institution, found itself taken over as a result of this scandal, larger financial institutions like Citibank may prove less susceptible to fluctuations in their market share and more interested in exploring the profits to be made through these types of illicit operations.

Far larger and more complicated than the world of private banking are the interlacing connections between banks known as correspondence relationships. A veritable spider's web of global financial markets, the next section examines the way these financial relationships are used and exploited by terrorist organizations.

Correspondence Banking Relationships

Correspondent banking occurs when banks provide transfer services to one another. For example if a bank in Singapore has a client who wants euros available to him while in

Italy, the Asian bank requires a correspondent relationship with an Italian financial institution willing to make euros available in Italy.

The complexity of tracing cross-border financial flows increases dramatically in consideration of correspondent banking relationships. These arrangements between banks allow a non-citizen/non-resident to effectively hold an account at a foreign bank through a local financial entity that supports a correspondent relationship with the bank abroad.

Many of the largest U.S. and European banks serve as correspondents for thousands of other banks.[62] These institutions, through the accounts they provide to foreign banks, have become conduits for "dirty money" and have, as a result, facilitated illicit enterprises, including drug trafficking and financial frauds.[63]

It should therefore be abundantly clear criminals and terrorists can use a poorly regulated international bank in order to access major, western financial centers by virtue of correspondence relationships.

As a Senate report on money laundering noted, by manipulating these correspondence relationships, "The evidence is clear that terrorists are using our own financial institutions against us, and we need to understand our vulnerabilities and take new measures to protect ourselves from similar abuses down the road."[64]

The report continues:

> We learned in our Subcommittee investigation that bad banks can "nest" in other foreign banks and obtain access to U.S. banks that way. They can open a correspondent account with a foreign bank that already has a U.S. correspondent account, and then take advantage of the correspondent chain to access the U.S. financial system… The possibility that terrorists are using such banks to conduct their operations is one that cannot be ignored.[65]

This is clearly a process that can be replicated globally and is not anchored solely in the American system.

The largest fund transfer banks, known as money center banks, process up to US$1 trillion in wire transfers a day.[66] The most attractive component of the correspondent system for high value criminals and terrorists is the unfettered access to international transfer systems. This facilitates the rapid transfer of funds across international boundaries and within countries.[67] Hidden among such a volume of financial traffic, the illicit transfer becomes the proverbial needle in a haystack for commercial fraud investigators and law enforcement investigators.

The most effective method of manipulating correspondence accounts for terrorist groups and international criminals is to own a bank, or at least a sizable share of one. This method has been used successfully and with damning efficiency many times, none more serious than Osama bin Laden's Al Shamal Islamic Bank.

Exploitation of Western Banks through Correspondence Relationships

Case Study – Al Shamal Islamic Bank

When Osama bin Laden relocated to Sudan in the mid-1980s he devoted a lot of time and money to developing infrastructure, conducive to his aims, within his new environment. To that end he was influential in establishing Al Shamal Islamic Bank into which he placed $50 million of his own money.[68] Officially open for business since January 1990, Al Shamal is a public limited company incorporated in Sudan that defines itself as "a financial commercial banking institution that conducts its operations in accordance with the Islamic Sharia."[69]

As an Islamic bank, Al Shamal was immediately connected to the Middle Eastern banking networks. Simultaneously, by quickly establishing correspondence relationships with western banks, Al Shamal succeeded in putting on the ruse of a reputable financial institution. Via these relationships, bin Laden was able to send money to his operatives globally with impunity.

Al Shamal's Correspondence Relationships

Al Shamal included among its network of correspondence banks some of the most prestigious American, European and Asian banks on the map. It is documented that up through the late 1990s, Al Shamal was connected to both Citibank and American Express.[70] While these accounts had been closed as of a 2001 report, other major relationships remained open.[71]

Al Shamal is known to have had active correspondent relationships with Credit Lyonnais in Switzerland, Commerz Bank in Germany, ING Bank in Indonesia and Standard Bank in South Africa, each of which retains correspondent accounts with U.S. and other western banks.[72] The current status of these accounts is unknown to the author, but recent reports have not mentioned any type of closure or suspension.

Senator Carl Levin, chairman of the Permanent Subcommittee on Investigations, verified al Qaeda's extensive use of the bank:

> Jamal Ahmed al-Fadl, who had handled financial transactions for al Qaeda, testified that al Qaeda had used half a dozen accounts at the Shamal bank; one account was in the name of bin Laden. He described a 1994 incident in which the Shamal bank was used by al Qaeda to provide al-Fadl $100,000 in U.S. $100 dollar bills which he was directed to take on a plane to an individual in Jordan, which he did. This testimony shows that, in 1994, the Shamal bank maintained accounts used by bin Laden and al Qaeda and was supplying bin Laden operatives with funds.[73]

Senator Levin continued:

> Testimony also demonstrated how a U.S. bank was used by bin Laden to send money from the Shamal bank to a bin Laden associate in Texas using a correspondent account. Essam al Ridi, who worked for bin Laden, testified that he received a $250,000 wire transfer at his bank in Texas that was sent by the Shamal bank, which he then used to purchase a plane for bin Laden and which he later delivered himself to bin Laden.[74]

The Senator concluded:

> That means any customer of the Shamal bank – including a member of bin Laden's organization – could penetrate the U.S. banking system by going through one of these other correspondent accounts.[75]

The exploitation of American financial networks by terrorist groups is clearly a small manifestation of how terrorist groups are manipulating international financial connections. These groups are not limiting their focus to the United States and are willing to use any and all mechanisms at their disposal in support of their terrorist aims.

There is one further piece of the Al Shamal puzzle which must now be revealed. In addition to bin Laden, a consortium of other Islamic individuals and institutions assisted in the establishment of the bank. Al Shamal Islamic Bank was backed from the outset by Faisal Islamic Bank of Sudan (FIBS),[76] "whose principal patron was the Saudi Prince, Muhammad ibn Faisal Al Saud."[77]

In 2002 a huge, multi-trillion dollar lawsuit was brought to Saudi Arabia by 600 relatives of 9/11 victims. While refraining from placing blame squarely on the shoulders of the government, the lawsuit did name some individuals and financial institutions as being behind the attack. Among those named were Al Shamal Islamic Bank, Faisal Islamic Bank (parent of FIBS) and Prince Muhammad ibn Faisal Al Saud[78] (who was later released from the lawsuit due to diplomatic immunity).[79]

Despite all of this information, Al Shamal Islamic Bank continues to operate unabated and remains listed on the Khartoum Stock Exchange.[80]

Despite a decade of learning lessons the hard way about the exploitation of correspondence relationships, changes have not been internalized and terrorist entities continue to exploit the correspondence channels of western banks. This method was recently used by Hezbollah.

Case Study – Funding Hezbollah
Some of America's largest banks, including JP Morgan Chase, Wachovia and American Express Centurion Bank, have recently been linked to a Hezbollah fundraising campaign.

Hezbollah's official global television network, *al-Manar*, often presents fund requests for its parent movement during commercials. Recently, *al-Manar* requested that donors deposit into the accounts of four Lebanese banks.

These banks, Libanaise, Beirut Riyad, Byblos and Fransa, have recently received donations:

> …solicited for Hizballah itself (under the name 'The Organization for the Support of the Islamic Resistance in Lebanon'), as well as money gathered by Hizballah funds such as 'The Intifada in Occupied Palestine Fund,' 'The Palestine Uprising,' ' 'The Resistance Information Donation Fund,' and 'Support the Resistance Media al-Manar Television.'[81]

This apparently mundane fundraising campaign is exacerbated by correspondence relationships between several major U.S. financial institutions and these Lebanese banks. These relationships represent the potential support of terrorist activity by American banks.[d] [82]

Calling attention to these connections is not intended to cause embarrassment to unsuspecting financial networks. It simply demonstrates how correspondence channels allow for the manipulation of legal financial networks by terrorist groups, in this case by inadvertently allowing Hezbollah fundraising activities through American financial marketplaces. Correspondence relationships flow in multiple directions and once finances hit a hub, they can be sent out in a near limitless number of directions, all but ensuring they reach their destination, and in most cases without raising suspicions.

A discussion of the commercial implications of correspondent relationships is beyond the scope of this article as their infrastructure represents the core of international financial networks. This vessel for international monetary transfer has been consistently exploited by the underbelly of society. While correspondent relationships have proven an effective way to maneuver around regulatory hurdles, such movements have become more suspect and subject to inquiry. While detection of an illicit transfer may be too late to prevent successful receipt of that specific wire, it could call into question the channel. For this reason, terrorists and criminals alike have been searching for less visible methods of moving money.

Shunning oversight entirely can be accomplished through offshore and shell banks. These financial options exploit legal loopholes and many provide new services created specifically to thwart the latest regulatory hurdles. The discussion now shifts to analyzing the commercial implications and illicit financial flows connected to offshore and shell banking.

Offshore and Shell Banking

---

[d] U.S. institutions affiliated with the above-named Lebanese banks include: Wachovia (correspondent bank for Libanaise, Beirut Riyad and Byblos); Bank of New York and JP Morgan Chase (correspondents for Byblos, Fransa and Beirut Riyad); Citibank (correspondent for Byblos); American Express Bank correspondent for Byblos and Beirut Riyad); and Standard Chartered Bank (correspondent for Byblos).

John Perry Bujouves, C.E.O. of Bayshore Bank and Trust, a major offshore player, noted, "The ability to understand and utilize the laws of more than one jurisdiction has become the most valuable tool available to professionals in ensuring the effective representation of today's high net-worth clientele."[83]

While financial planners and managers historically have used offshore locations as tax havens they are now being fostered in order to hide money from the watchful eyes of "Big Brother" and governmental oversight. Offshore institutions offer protection and anonymity to their clients, despite new international regulations. Panama Offshore Legal Services is one of many corporations offering a "dual entity" offshore structure intelligently designed to make a client's assets invisible. Composed of a dummy Private Interest Foundation holding ownership of an International Business Corporation, the layers provide an impenetrable mesh of red tape effectively separating an individual from his money for taxation, legislative or tracing purposes.[84]

To understand the role of the foundation within this structure, one must first understand the composition of the foundation. The Private Interest Foundation has four main parts:

> Founder: The founder is the person or entity that forms the foundation in the public registry. Our firm generally provides a nominee founder, and provides you with a pre-signed, undated letter of resignation from the founder immediately upon incorporation of the foundation. At that point, the founder holds no control.
>
> Foundation Council: The council serves the same function to the foundation as directors do to a corporation. The council's names and passport numbers are registered in the public registry when the foundation is incorporated. For protecting the privacy of our clients, we generally provide a nominee council, and provide pre-signed, undated letters of resignation from the nominee council. At that point, the council holds no control.
>
> Protector: The Protector is the ultimate controller of the Foundation. Immediately upon incorporation of the foundation, the council appoints a Protector, through a notarized Private Protectorate Document. Since the document is a private, non-publicly registered document, the Protector remains 100% anonymous. Moving forward, the Protector fully controls the foundation and its financial assets.
>
> Beneficiaries: The Beneficiaries are appointed through a Private Letter of Wishes written by the Protector. The letter of wishes is a private document, so beneficiaries remain 100% anonymous. The letter of wishes can be changed or modified at any time by the Protector only.[85]

All this is available for $2,999 from Panama offshore legal services, but similar products are available online for as little as $595.[86]

There are a number of offshore and stringent privacy zones around the globe exploited by criminal and terrorist elements. A report from the 2004 Asia Bankers Conference

specifically named the Cayman Islands, the Netherlands Antilles, Aruba and Cyprus as examples of offshore banking havens which have been used or are confirmed to be used by criminal organizations for laundering the proceeds from their illicit activities.[87]

As the offshore market expands, its profitability has caught the attention of some of the western majors. HSBC[88] and Barclays[89] now offer a variety of offshore solutions to their clientele. One particularly disturbing aspect of this phenomenon is most offshore financial institutions have correspondent relationships with enough banks to provide their clients civilian or criminal access to the western market.[90] This analysis now investigates how Islamic terrorist groups and their support structures manipulate offshore havens.

Islamic Offshore Networks

Case Study: Muslim Brotherhood

Banking networks, Islamic and otherwise, have been exploited since their inception. For the most part, individuals and groups intending to take advantage of a bank or financial entity are viewed as villainous, but the Muslim Brotherhood represents an organization whose activities are embraced by a large portion of the Muslim populace. Although the Muslim Brotherhood was founded in an effort to inspire a return to religious Islamic practice, the movement is now one of the driving financial forces behind the Jihadists in the counter movement to the West's war on terror. With representation in over 70 nations,[91] controlling assets of US$10 billion and terrorist spawn like Hamas and Islamic Jihad, the Muslim Brotherhood is sitting at the epicenter of the Jihadist earthquake.[92]

A frequently overlooked element in analysis of the global Jihadist movement, the Brotherhood is actually a unifying factor, creating an ideological and financial nexus which includes western financial support. In 2003, then counter-terrorism czar Richard Clarke said:

> …the issue of terrorist financing in the United States is a fundamental example of the shared infrastructure levered by Hamas, Islamic Jihad and al Qaeda, all of which enjoy a significant degree of cooperation and coordination within our borders. The common link here is the extremist Muslim Brotherhood—all these organizations are descendants of the membership and ideology of the Muslim Brotherhood.[93]

Through their global ideological and financial networks, the Muslim Brotherhood has successfully transformed itself into:

> …the spine upon which the funding operations for militant pan-Islamicism was built, taking funds largely generated from wealthy Gulf state elites and distributing them for terrorist education, recruitment and operations widely dispersed throughout the world, especially in areas where Muslims hoped to displace non-Muslim or secular governments.[94]

It has even been considered: "…if al Qaeda were to run into serious financial difficulty, its coffers could easily be quietly replenished through the Brotherhood's offshore structure with very little danger of being interdicted."[95] So, how does the Muslim Brotherhood use offshore networks to launder funds and finance terrorist operations?

Money Laundering via Islamic Offshore Networks

As mentioned earlier, some Islamic financial institutions knowingly support terrorist entities and launder money to assist to their violent aims. Following in the mold of Al Shamal, one popular and secretive way of achieving this financial movement is to establish entire banking entities, onshore and off, in support of these goals.

To this end, the Muslim Brotherhood runs a vast financial network of holding companies, subsidiaries, shell banks and financial institutions stretching:

> …to Panama, Liberia, British Virgin Islands, Cayman Islands, Switzerland, Cyprus, Nigeria, Brazil, Argentina, Paraguay and beyond. Many of the entities are in the names of individuals like Nada, Nasreddin, al-Qaradawi and Himmat, who publicly identify themselves as Brotherhood leaders.[96]

The most visible part of the network, offshore shell banks in the Bahamas, did merit some investigation immediately after 9/11. The Treasury Department publicly stated Bank al Taqwa and Akida Bank International were "involved in financing radical groups such as the Palestinian Hamas, Algeria's Islamic Salvation Front and Armed Islamic Group, Tunisia's An-Nahda, and Usama bin Laden and his al-Qaida organization."[97]

The structure of Bank al Taqwa[e] and Akida Bank in Nassau followed the pattern of other offshore endeavors. The bank was a virtual entity affiliated with the al Taqwa Management Organization, owned by another Yousef Nada entity in Switzerland. The real banking activity, however, was carried out through correspondent relationships with European banks.[98] While some pressure was brought to bear on those particular banks, many of the other institutions remain untouched and open for business.

Additionally, many of the Brotherhood's businesses are registered as offshore companies via local trusts in Liechtenstein, where corporate ownership is not identified, and businesses are not required to keep accurate records of transactions and business activities.[99]

By running a loosely interlaced patchwork of financial institutions, both clandestinely offshore and via correspondence relationships with western banks, the Muslim Brotherhood ensures the support of its Jihadist message and operations. The commercial and security implications of these revelations are immense. From a security perspective, the West realizes its foe is educated and dynamic, ready to adapt to further its own aims and exploit weaknesses.

[e] See Money Laundering Series Introductory Paper for more information on the Bank al-Taqwa Network.

Commercially this is evidence of a manifestation of the so-called flattening of the world, in which there will be greater global financial integration. As financial needs are no longer met solely by Islamic networks, more hidden assets will be exposed to western financial systems. What remains to be seen is who will get the better of whom.

Until this point, the discussion has been based entirely on traditional brick and mortar financial entities. While various, these methods of hiding and transferring assets have existed for some time. As technology improves, so do opportunities for its exploitation.[f] One of the biggest and most direct causes for concern appears from the merging of offshore banking entities and the Internet, where products are easily accessible and the scope of services is immeasurable.

Offshore Money Laundering - Online

At present, a Google search for offshore banking yields a return of 2.1 million web pages.[100] If an individual wants to incorporate in Belize or set up a Delaware, USA based LLC, the question is not where to find a specialist, but how to choose the best and most cost effective service offering. Many offshore companies are willing to bend and break nearly every major international, financial regulation in the name of privacy and anonymity. Most of these services can be provided through the Internet in only a matter of minutes.

Searching through the returns for offshore corporation creation or trusts will yield some excellent services, but those who look closely might find a diamond in the rough known as Asset World Pro.

A guardian of personal privacy against the evil forces of "Big Brother" and bureaucracy, Asset World Pro has worked diligently for over 30 years to hide money from the prying eyes of governments by setting up shell corporations and foundations for some of today's wealthy elite. Not merely content to offer privacy services, they make the following guarantee:

> **Guarantee of Privacy**
>
> The information you provide us will remain confidential and private, period. You will be given a secret I.D. Code #
>
> We will not divulge any information about you even if we are presented with a legally signed court order or subpoena to do so.
>
> We will fight any court order "at our expense" in your behalf and that's a promise.

[f] For a detailed account of terrorist financing / money laundering activities online, see Money Laundering Series Introductory Paper.

> By the way, for the past three decades we have never received any court order or government notice demanding or requesting information about any of our clients and we don't ever expect to receive any such notifications. I guess they already know our answer.[101]

Like other offshore banks, Asset World Pro is comfortable setting up trusts, federations, corporations, etc. Akin to some of their competition, they offer passport acquisition services, in which they explain and aid in the process of acquiring a second or third nationality in order to escape detection and tax penalties by the home country, or access a western nation clandestinely. However, Asset World Pro continues where the competition stops, by providing an extradition program, among other services. As taken directly from their website (all emphasis present in original):

> The Extradition Program is specifically designed for the client who has placed himself in the position of violating U.S. (IRS) tax laws or tax laws of some other country.
>
> For our general purposes, extradition is when an individual is presently living in country [B] to avoid possible arrest and conviction of a supposed tax crime in his home [A] country.
>
> But don't let the above comments discourage you. There are legal ways that you **[can]** be completely protected from any extradition attempts made against you and this is where we can be of definite help to you and be **[100 %]** successful.
>
> And to make you feel better, there are some countries that do **[not]** recognize tax crimes as crimes. This means that the tax treaties and extradition treaties will have **no effect** on you.[102]

Asset World Pro, in addition to bank wire via an account with Banco Cuscatlan de Costa Rica which has an active correspondent relationship with Bank of New York,[103] accepts eight different payment methods, including Western Union, Paypal, and E-gold, all of which received particular attention in the introductory paper of this series. As was discussed in that paper, an e-gold digital currency account can be set up with fraudulent information and financed via bank wire or credit card. Any terrorist with stolen identification can set up and fund an e-gold account. Once the account is funded with a stolen credit card, the e-gold can be manipulated and moved into countless other forms online, also untraceable. The system allows for the set up of complete offshore enterprises which then can be used as treasure troves for illicit or terrorist entities.

The political implication of such offshore businesses should be reflected in expanded oversight or attempts to regulate the industry, by legislation such as the Patriot Act. The commercial implication however has been a rise in popularity of offshore networks specifically designed to thwart any policy meant to regulate them. This trend will

continue as long as an underground method of currency transfer exists in an atmosphere free of oversight.

Critical Analysis

On paper, great strides have been made in the fight against money laundering and terrorist financing. New legislative practices have been instituted globally, and religious scholars have added their considerable weight to cracking down on this menace. Unquestionably, these practices have born fruit through deterrents such as fines, publicity and increased fear of detection. In practice however, until punishments are severe enough to keep desire for profit in check, there will be those who ignore legal precedent and ramification in order to profit. The fact that much of this money comes from drug or weapon sales or goes to finance terrorist groups is not as important to the multinational bank as the amount of money under its management.

According to Manhattan District Attorney Robert Morgenthau, "This enormous flow of illegal money poses a grave threat to our security. It is also apparent much more needs to be done, particularly by banks and other financial institutions, to know with whom they are doing business."[104]

At the end of the day, the fundamental commercial implication of terrorist money laundering is the global network of financial entities does not mind where the money comes from and is not particularly concerned with where it is going and to what end. As long as a profit can be made, banks are willing to work with it, and as long as the banks are willing, terrorist groups will continue to exploit.

From the side of the criminal or terrorist, use of the legal financial system is simply a means to and end. If more pressure is mounted upon financial entities, money launderers are apt to look for other avenues, and banks will miss out on their pot of gold. Therefore, as constraints become more severe, banks increasingly look for new ways to keep their customers satisfied. Peter Lilly comments:

> Money launderers are clever – thus they are constantly looking for new business opportunities. The regulatory spotlight that has been shone on banks means that they have sought out other types of businesses where anti-money laundering regulation is either non-existent or not as advanced as in the banking environment.[105]

The unfortunate truth is, for the time being, the criminals and terrorists have the upper hand. The international financial system is theirs for the taking and banks are happy to be used, even seeking out dirty money as evidenced in the case of Riggs Bank. The deterrents in place pose no actual deterrent to doing business with criminals and terrorists. But, there is a crackdown coming. One day, there will be another major terrorist attack, and then another and another. Each time, the regulatory net will get tighter until the criminals and terrorists go underground. They will go back to Hawala or

to more obscure offshore or online locations for moving their funds. When that happens, the banks will be without access to that slice of the pie, and the legislative, investigative eye will screen financial centers for any shred of complicity with terrorism. On that day, punishments will outweigh profits.

Until then, "…you can purchase an offshore bank over the Internet by credit card for as little as $25,000. Presumably the ideal way to achieve complete anonymity is to buy your bank using your anonymous credit card."[106]

---

[1] Walker, J. 1998. *Modelling Global Money Laundering Flows - Some findings*. http://www.johnwalkercrimetrendsanalysis.com.au/ML%20method.htm.

[2] Agarwal, J.D. and Agarwal, A. 2004. *International Money Laundering in the Banking Sector*. Asia Pacific Banker's Conference 2004. March 26.

[3] Levi, Prof. M. 2005. *Controlling the International Money Trail: A Multi-level Cross-national Public Policy Review.* Future Governance Research Initiative. Cardiff University. March 10. Available online at: http://www.esrcsocietytoday.ac.uk/ESRCInfoCentre/ViewOutputPage.aspx?data=%2fFrXHTl993qdotZ%2fUfKfjlXOGk5S19C8PuXlOwsA0bX%2ffX2YcpHVRSzvRY%2fhis619iglLGWEnq1QIQB9nOdTqw3gle2IKopJLhzwBtTjFjbm0jltgJqeUVQJiw2F09NNb9kDUbqgLQZ8xMZAHnP5ohKkHTqcJtZ76aODq5QTwpzBOTvwD8kDZvpRM0g8tvv5Gpo0Hm%2fgJbImhhdDuTHzrXsz61QZIId%2b7TXd%2bgCQZobdaEpggqLeyGQ7OIKWxmexwZFcQuyyaict%2bfF4TgG%2bGKA35oilx6odW7xYIH92bHMT4JQiJoQ3GhdObcnD2W077kIp4bHeaEZwqtCGwvEMbmgQJ5kM0cy1gIvMwP7JGloDj0pC2%2butLF9ObEG7EmC%2f0R14wJYFLr%2b6fDyGB9UK1F%2fjnS%2bPoo9P&xu=&isAwardHolder=&isProfiled=&AwardHolderID=&Sector= (Accessed May 6, 2007).

[4] Tompkins, J.B. Jr. 2002. *The Impact of the USA PATRIOT Act of 2001 on Non-US Banks.* Prepared in Connection with the International Monetary Fund Seminar on Current Developments in Monetary and Financial Law. Washington D.C. May 7-17.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] USA PATRIOT ACT 2001. Section 312, subsection 3 (a) (b). Available online at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf (Accessed May 7, 2007).

[9] Kini, S. M. 2006. *Recent Anti-Money Laundering Enforcement Actions: Lessons to be Learned at Others' Expense (PATRIOT Act of 2001). Journal of Investment Compliance*. Volume 7, Issue 3, pp. 38-43.

[10] Ibid.

[11] 2006. Bank Of America Settles Money Laundering Probe. *North Country Gazette*. Available at: http://www.northcountrygazette.org/articles/092706MoneyLaundering.html (Accessed May 7, 2007).

[12] Ibid.

[13] Ibid.

[14] Press Release. 2005. *Banking Department Joins Manhattan District Attorney in Announcing Joint Settlement with Israel Discount Bank*. State of New York Banking Department. December 15. Available online at: http://www.banking.state.ny.us/pr051216.htm (Accessed May 20, 2007).

[15] http://www.ynetnews.com/articles/0,7340,L-3405641,00.html.

[16] Ibid.

[17] 2006. *Bank Of America Settles Money Laundering Probe*. *North Country Gazette*. Available at: http://www.northcountrygazette.org/articles/092706MoneyLaundering.html (Accessed May 7, 2007).

[18] Case Summary Investigation Division Cases - People v. Beacon Hill Service Corporation – Manhattan District Attorney Website Available online at: http://www.manhattanda.org/office_overview/prominent/beacon_hill.htm (Accessed May 21, 2007).

[19] Western Union Price Calculator (Accessed June 5, 2007): https://wumt.westernunion.com/asp/feeCalc.asp?TXNTYPE=DIRECT_TO_BANK&DESTINATION_COUNTRY=MX&CURRENCY=USD&AMOUNT=500.00&STATE=MT&RANGE=300-750.
[20]Ibid.
[21] Fath El Rahman Abdallah El Sheikh. 2002. The Underground Banking Systems and their Impact on Control of Money Laundering: With Special Reference to Islamic Banking. *Journal of Money Laundering Control*. Vol 6, No.1, pp. 42-45.
[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] FATF website – "About the FATF" page. http://www.fatf-gafi.org/pages/0,2966,en_32250379_32236836_1_1_1_1_1,00.html (Accessed May 20, 2007).
[33] Ibid.
[34] FATF – The 40 Recommendations – Recommendation 5. http://www.fatf-gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.html (Accessed May 20, 2007).
[35] FATF – The 40 Recommendations – Recommendation 7. http://www.fatf-gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.html (Accessed May 20, 2007).
[36] FATF – The 40 Recommendations – Recommendation 18. http://www.fatf-gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.html (Accessed May 20, 2007).
[37] FATF Special Recommendations on Terrorist Financing – Recommendation 2. http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf (Accessed May 20, 2007).
[38] FATF Special Recommendations on Terrorist Financing – Recommendation 3. http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf (Accessed May 20, 2007).
[39] FATF Special Recommendations on Terrorist Financing – Recommendation 7. http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf (Accessed May 20, 2007).
[40] FATF website – "FATF Members and Observers" page. http://www.fatf-gafi.org/document/52/0,2340,en_32250379_32237295_34027188_1_1_1_1,00.html (Accessed May 20, 2007).
[41] Levi, Prof. M. 2005. *Controlling the International Money Trail: A Multi-level Cross-National Public Policy Review.* Future Governance Research Initiative. Cardiff University. March 10. Available online at: http://www.esrcsocietytoday.ac.uk/ESRCInfoCentre/ViewOutputPage.aspx?data=%2fFrXHTl993qdotZ%2fUfKfjlXOGk5S19C8PuXlOwsA0bX%2ffX2YcpHVRSzvRY%2fhis619iglLGWEnq1QIQB9nOdTqw3gle2IKopJLhzwBtTjFjbm0jltgJqeUVQJiw2F09NNb9kDUbqgLQZ8xMZAHnP5ohKkHTqcJtZ76aODq5QTwpzBOTvwD8kDZvpRM0g8tvv5Gpo0Hm%2fgJbImhhdDuTHzrXsz61QZIId%2b7TXd%2bgCQZobdaEpggqLeyGQ7OIKWxmexwZFcQuyyaict%2bfF4TgG%2bGKA35oilx6odW7xYIH92bHMT4JQiJoQ3GhdObcnD2W077kIp4bHeaEZwqtCGwvEMbmgQJ5kM0cy1gIvMwP7JGloDj0pC2%2butLF9ObEG7EmC%2f0R14wJYFLr%2b6fDyGB9UK1F%2fjnS%2bPoo9P&xu=&isAwardHolder=&isProfiled=&AwardHolderID=&Sector= (Accessed May 6, 2007).
[42] Lilly, P. 2006. *Dirty Dealing: The Untold Truth about Global Money Laundering International Crime and Terrorism.* London and Philadelphia: Kogan Page Limited, pp. 4.
[43] FATF – NCCT Initiative. http://www.fatf-gafi.org/document/4/0,2340,en_32250379_32236992_33916420_1_1_1_1,00.html (Accessed May 18, 2007).
[44] 2007 State Department Report on Major Money Laundering Countries:

http://www.state.gov/p/inl/rls/nrcrpt/2007/vol2/html/80883.htm (Accessed June 6, 2007).
[45] 2006 State Department Report on Major Money Laundering Countries: http://www.state.gov/p/inl/rls/nrcrpt/2006/vol2/html/62140.htm (Accessed May 7, 2007).
[46] Lilly, P. 2006. *Dirty Dealing: The Untold Truth about Global Money Laundering International Crime and Terrorism.* London and Philadelphia: Kogan Page Limited, Preface, xv.
[47] Ibid, pp. 128.
[48] Petras, Prof. J. 2002. *US Bank Money Laundering – Enormous By Any Measure*. Binghamton University. September 1. Available online at: http://www.rense.com/general28/money.htm (Accessed May 7, 2007).
[49] Tompkins, J.B. Jr. 2002. *The Impact of the USA PATRIOT Act of 2001 on Non-US Banks.* Prepared in Connection with the International Monetary Fund Seminar on Current Developments in Monetary and Financial Law. Washington D.C. May 7-17.
[50] Petras, Prof. J. 2002. *US Bank Money Laundering – Enormous By Any Measure*. Binghamton University. September 1, 2002. Available online at: http://www.rense.com/general28/money.htm (Accessed May 7, 2007).
[51] Agarwal, J.D. and Agarwal, A. 2004. *International Money Laundering in the Banking Sector*. Asia Pacific Banker's Conference 2004. March 26.
[52] Petras, Prof. J. 2002. *US Bank Money Laundering – Enormous By Any Measure*. Binghamton University. September 1, 2002. Available online at: http://www.rense.com/general28/money.htm (Accessed May 7, 2007).
[53] Ibid.
[54] Agarwal, J.D. and Agarwal, A. 2004. *International Money Laundering in the Banking Sector*. Asia Pacific Banker's Conference 2004. March 26.
[55] Ohara, T. and Day, K. 2004. Riggs Bank Hid Assets Of Pinochet, Report Says Senate Probe Cites Former U.S. Examiner. *Washington Post*. July 15; page A01. Available online: http://www.washingtonpost.com/ac2/wp-dyn/A50222-2004Jul14?language=printer (Accessed May 10, 2007).
[56] Ibid.
[57] Ibid.
[58] Ibid.
[59] Ibid.
[60] Ibid.
[61] Ibid.
[62] Petras, Prof. J. 2002. *US Bank Money Laundering – Enormous By Any Measure*. Binghamton University. September 1, 2002. Available online at http://www.rense.com/general28/money.htm (Accessed May 7, 2007).
[63] Gustitus, L., Bean, E. and Roach, R. 2001. *Correspondent Banking: A Gateway for Money Laundering*. Democratic Staff, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate. May. Available online at: http://usinfo.state.gov/journals/ites/0501/ijee/levin.htm (Accessed May 7, 2007).
[64] http://www.senate.gov/~levin/newsroom/release.cfm?id=211390.
[65] http://www.senate.gov/~levin/newsroom/release.cfm?id=211390.
[66] Petras, Prof. J. 2002. *US Bank Money Laundering – Enormous By Any Measure*. Binghamton University. September 1, 2002. Available online at http://www.rense.com/general28/money.htm (Accessed May 7, 2007).
[67] Ibid.
[68] http://www.senate.gov/~levin/newsroom/release.cfm?id=211390 (Accessed June 3, 2007).
[69] http://www.alshamalbank.com/en/index.htm (Accessed June 3, 2007).
[70] http://www.senate.gov/~levin/newsroom/release.cfm?id=211390.
[71] http://www.senate.gov/~levin/newsroom/release.cfm?id=211390.
[72] http://www.senate.gov/~levin/newsroom/release.cfm?id=211390.
[73] http://www.senate.gov/~levin/newsroom/release.cfm?id=211390.
[74] http://www.senate.gov/~levin/newsroom/release.cfm?id=211390.
[75] http://www.senate.gov/~levin/newsroom/release.cfm?id=211390.
[76] http://www.alshamalbank.com/en/index.htm (Accessed June 3, 2007).

[77] http://www.photius.com/countries/sudan/economy/sudan_economy_islamic_banking.html (Accessed June 6, 2007).
[78] http://tvnz.co.nz/view/page/425822/124490 (Accessed June 7, 2007).
[79] http://www.cooperativeresearch.org/entity.jsp?entity=saudi_binladin_group (Accessed June 7, 2007).
[80] http://www.mbendi.co.za/orgs/cliz.htm (Accessed June 3, 2007).
[81] Jorisch, Avi. 2003. *PolicyWatch #774 – Hizballah's Unwitting U.S. Bankers*. Washington Institute for Near East Policy. July 22, 2003. Available online at: http://www.washingtoninstitute.org/templateC05.php?CID=1652 (Accessed May 7, 2007).
[82] Ibid.
[83] Bayshore Bank and Trust – Our Services. http://www.bayshorebank.com/main/our_services (Accessed May 18, 2007).
[84] Panama Offshore Legal Services - http://www.panama-offshore-services.com/corporation_offshore_structure_package.htm (Accessed May 10, 2007).
[85] Panama Offshore Legal Services - http://www.panama-offshore-services.com/corporation_offshore_structure_package.htm (Accessed May 10, 2007).
[86] http://www.assetworldpro.com/hotnews.htm (Accessed May 16, 2007).
[87] Agarwal, J.D. and Agarwal, A. 2004. *International Money Laundering in the Banking Sector*. Asia Pacific Banker's Conference 2004. March 26.
[88] HSBC Offshore: http://www.offshore.hsbc.com/1/2/home (Accessed May 21, 2007).
[89] Barclays in Mauritius: http://www.barclays.com/africa/mauritius/offshore_bank.htm (Accessed May 21, 2007).
Petras, Prof. J. 2002. *US Bank Money Laundering – Enormous By Any Measure*. Binghamton University. September 1, 2002. Available online at: http://www.rense.com/general28/money.htm (Accessed May 7, 2007).
[91] Muslim Brotherhood Movement Homepage: http://www.ummah.net/ikhwan/ (Accessed May 21, 2007).
[92] Farah, D. 2006. *The Little Explored Offshore Empire of the International Muslim Brotherhood*. International Assessment and Strategy Center. April 18. Available Online at: http://www.strategycenter.net/printVersion/print_pub.asp?pubID=102 (Accessed May 15, 2007).
[93] Ibid.
[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Ibid.
[98] Ibid.
[99] Ibid.
[100] http://www.google.com/search?hl=en&q=offshore+banking (search conducted on May 17, 2007).
[101] Asset World Pro – About Us. Available at: http://www.assetworldpro.com/aboutus.htm (Accessed May 16, 2007).
[102] Asset World Pro - Extradition Program. Available at: http://www.assetworldpro.com/31-EXT.htm (Accessed May 16, 2007).
[103] Asset World Pro – How to Pay. http://www.assetworldpro.com/howtopay.htm (Accessed May 16, 2007).
[104] 2006. Bank Of America Settles Money Laundering Probe. *North Country Gazette*. Available at: http://www.northcountrygazette.org/articles/092706MoneyLaundering.html (Accessed May 7, 2007).
[105] Lilly, P. 2006. *Dirty Dealing: The Untold Truth about Global Money Laundering International Crime and Terrorism.* London and Philadelphia: Kogan Page Limited, p. 17.
[106] Ibid, p. 12.