

Abstract

Many different types of organizations attempt to launder money. However, unlike organized crime syndicates and drug cartels, terrorists, such as Islamic fundamentalist terrorist organizations launder money for other purposes. While money laundering relies on making dirty money look clean, terrorists often rely on money generated from seemingly legitimate means for illegitimate purposes. This process is referred to as reverse money laundering, which is often considered synonymous with terrorist financing. However, this is not the only way terrorists finance their operations. Therefore, the purpose of this paper is twofold: Distinguish reverse money laundering as a subset of terrorist financing, and attempt to determine the best way to help detect and prevent reverse money laundering. In an effort to help identify such an approach, it is the hypothesis of this study that the best way to help detect and prevent reverse money laundering is by making intelligence gathering on Islamic fundamentalist terrorist organizations the primary focus of any effort to try to stop the money from reaching its intended targets. Experts from different perspectives from the anti-money laundering community, including the public sector, consulting, compliance and technology were interviewed and an analysis of their responses appears to indicate that while they recognize the important role intelligence plays in the attempt combat reverse money laundering, it appears information sharing is considered a slightly higher priority.

Detecting Reverse Money Laundering:

Is Intelligence the Key?

By

Seth M. Schwartz

A Thesis Submitted to the Faculty of

Utica College

March 20, 2006

In Partial Fulfillment of the Requirement for the Degree

Master of Science in Economic Crime Management

Copyright © by Seth M. Schwartz, 2006. All Rights Reserved.

Members of the Advisory Committee:

Donald J. Rebovich, Ph.D., Professor, Utica College of Syracuse University, Utica, N.Y.
– Senior Thesis Advisor

Thomas Bock, M.S., Director, KPMG Forensic – Professional Reader

Richard Kinville, M.S., Director – Anti-Money Laundering Unit, Prudential Financial –
Professional Reader

Table of Contents

Introduction.....	1
<i>Money Laundering</i>	7
<i>Significant Laws and Regulations</i>	8
<i>Reverse Money Laundering</i>	9
<i>Formal Financial Sector</i>	17
<i>Increased Scrutiny</i>	25
Literature Review.....	32
<i>9-11 Commission, FATF and GAO</i>	32
<i>Research Based on Interviews</i>	35
Hypothesis.....	46
Methods.....	48
Research Design, Data and Methods	49
<i>Subjects</i>	49
<i>Apparatus</i>	51
<i>Procedure</i>	52
<i>Data Collection</i>	55
Findings.....	59
Conclusions.....	85
References.....	97
Appendix A.....	101
Appendix B	104

List of Illustrative Materials

Figure 1. Summary of Responses: Question #4.....	63
Figure 2. Summary of Responses: Question #5.....	66
Figure 3. Summary of Responses: Question #13.....	83

Detecting Reverse Money Laundering:

Is Intelligence the Key?

Introduction

Since the later half of the 20th Century, money laundering has been a significant problem addressed by governments and communities around the world, particularly in the United States. Prior to the terrorist attacks of September 11, 2001, the focus of money laundering detection and prevention was on its use by organized criminal enterprises and drug traffickers to clean dirty money and not on terrorists who finance operations (National Commission on Terrorist Attacks Upon the United States Monograph on Terrorist Financing (hereafter referred to as “9-11 Commission Monograph”), 2004). As a result, many of the rules and regulations reflect this emphasis. This focus shifted following the terror attacks of September 11, 2001 when a new priority was given to the detection and prevention of financing terrorist activities, specifically those connected to Islamic fundamentalism. According to the 2006 International Narcotics Control Strategy Report, \$150 million in funds related to terrorist financing have been frozen by 47 countries and, since the terrorist attacks of September 11, 2001, \$64.6 million has been seized as a result of investigations with possible links to terrorism (U.S. Department of State, 2006). However, the money laundering techniques used by terrorists often differ from the techniques used by traditional money launderers. In the traditional archetype of money laundering, the funds are generated from illegal or criminal activity and then cleaned through financial institutions to make the funds look legitimate.

Although this type of activity is more commonly associated with organized crime syndicates and drug cartels, terrorists also use illegal means to generate funds to finance their operations. However, in common occurrences of terrorist financing, the money is often derived from legal activity and then used for illegal means. This latter technique is a crucial component of what is referred to as “reverse money laundering.” Because this is the perhaps the most publicized form of terrorist financing, reverse money laundering is often used as a synonym for terrorist financing but, after reviewing terrorist financing activities, reverse money laundering appears to be a sub-set of terrorist financing and should not be considered one-and-the-same. As it is, money laundering is very difficult to detect, but reverse money laundering offers even greater challenges. Therefore, detecting terrorist financing through reverse money laundering is a vital component to the shift in priorities taking hold in the post September 11, 2001 environment of the 21st Century.

Despite the increase in priority given to stopping terrorist financing, specifically for Islamic fundamentalist terrorist organizations, and the increase in information provided by certain domestic and international entities, there is very little published information that references the term reverse money laundering. There are even fewer publications specifically dedicated to the topic of reverse money laundering as it relates to terrorist financing because most do not distinguish reverse money laundering as a distinct form of terrorist financing. Those that do specifically reference the subject only identify it in passing, and do not provide any detail of how it is actually performed. Additionally, they do not offer any guidance on how to prioritize the effort to combat

reverse money laundering. Because much of what has been published under the topic of terrorist financing actually describes reverse money laundering, it is easy to see why many consider terrorist financing to be synonymous with reverse money laundering. Therefore, the purpose of this study is twofold: 1) Distinguish reverse money laundering as a subset of terrorist financing by focusing on Islamic fundamentalist terrorist activity and 2) Attempt to determine the best way to help detect and prevent reverse money laundering. It is the hypothesis of this study that the findings will indicate that the best way to help detect and prevent reverse money laundering by stopping the money before it reaches its intended targets is by increasing the effort spent on gathering intelligence on terrorist organizations and their financial conduits.

This paper will serve as a reference for those looking to research terrorists' use of reverse money laundering to finance their organizations and operations and identify the techniques used to carry out such goals. Additionally, a goal of this paper is to identify areas where efforts should be focused to better detect those who attempt to launder money in this fashion. To accomplish this, several key questions need answering. These questions include: What is reverse money laundering? Why is it so difficult to detect? How does reverse money laundering relate to terrorist financing? What distinguishes reverse money laundering as a subset of terrorist financing? What is currently being done to detect reverse money laundering? Are the current approaches working, and if not, then why? What different courses of action should be taken?

To identify the techniques associated with reverse money laundering and help answer these questions, information was collected from previously published reports from agencies such as the National Commission on Terrorist Attacks Upon the United States (9-11 Commission), the General Accountability Office (GAO) and Financial Action Task Force (FATF). Additionally, subject matter experts were interviewed in order to provide valuable insight on how best to tackle the issue of detecting and preventing reverse money laundering. By analyzing these responses, it is the hope that this will provide a clear indication of what approaches will lead to better results with the goal of determining whether or not the hypothesis proposed in this study is correct.

Before going much further, there are a few key terms that need to be defined to help set the stage for understanding the environment surrounding reverse money laundering. These terms include:

Bank Secrecy Act (BSA): Passed in 1970, this is the first major piece of legislation that addressed the problem of money laundering.

Financial Action Task Force (FATF): FATF is an inter-governmental body organized to promote policies and procedures designed to help combat money laundering and terrorist financing.

Financial Crimes Enforcement Network (FinCEN): FinCEN is an agency of the United State Department of the Treasury tasked with working to communicate and share information among law enforcement agencies, regulators and members of the financial services community.

Financial Institution: Financial institutions, as defined by Section 5312 of The Bank Secrecy Act, include, but are not limited to, federally insured banks, broker/dealers, Money Services Businesses (MSB), telegraph companies, casinos and card clubs, insurance companies, pawnbrokers, travel agents, operators of credit card systems, and sellers of vehicles such as automobiles, boats and aircraft.

Informal Value Transfer System (IVTS): IVTSs involve the transfer of money outside of a recognized or regulated financial institution, such as a bank or a registered MSB.

IVTSs are often found in ethnic minority neighborhoods, and are used to transfer money to other countries. Sometimes these are the only form of money transfer systems recognized in a particular country and can be a cheaper way to send money than by using a bank. An example of an IVTS is a *hawala*, which is prominent in Islamic communities. This is a common way for terrorists to send money without it being detected, monitored or reported to the government.

Link Analysis: The utilization of technology to mine data to identify connections between entities based on shared pieces of information, such as address, telephone number, account number, or identification number.

Money Laundering: This involves taking funds generated from illegal activity, such as narcotics trafficking, gambling, kidnapping, or bribery, and moving them, through the financial system, to make it look like the funds came from a legitimate source.

Non-Governmental Organizations (NGO): Not-for-profit organizations usually established with the goal of addressing social problems. These organizations are not associated with a government agency or private businesses.

Office of Foreign Assets Control (OFAC): This is a department of the United States Department of the Treasury responsible for enforcing economic sanctions on countries and specially designated nationals, organizations, companies and vessels. OFAC maintains a list of these persons and entities with which United States companies and individuals are prohibited from conducting business.

Reverse Money Laundering: This involves taking funds generated from legal activity, such as charitable donations or legitimate businesses, and using them for illegal purposes, such as financing terrorist cells or operations.

September 11, 2001: The date on which the United States was the victim of terrorist attacks carried out by al Qaeda operatives. They hijacked four airplanes and guided one each into One and Two World Trade Center in New York, New York and one into the Pentagon in Washington, D.C. The hijackers of the fourth plane were overtaken by the plane's passengers who forced the plane to crash in Pennsylvania before it reached its target.

Suspicious Activity Report: When financial institutions detect suspicious activity, they report such activity to the Financial Crimes Enforcement Network. The reports are required to include the parties involved (if known), the amount involved and a summary of the activity including why it is thought to be suspicious.

Terrorist Financing: This is a broad category including the various methods through which terrorists raise, transfer and distribute funds to support their organizations or operations. Terrorist financing can be performed through both legal and illegal operations.

USA PATRIOT Act of 2001: The Uniting and Strengthening America by Providing the Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) was passed in the wake of the September 11, 2001 attacks. Title III of the USA PATRIOT Act provides a minimum set of standards for money laundering programs, but does little to adapt current anti-money laundering detection requirements to, or develop new requirements specifically designed for, the ways that terrorists finance their organizations and operations. The primary proactive requirement to intercept and obstruct terrorists is only referenced in Section 326, which deals with financial institutions requirements to perform identification procedures prior to establishing a new relationship with a customer in an attempt to determine if they are or have been identified as a terrorist suspect or if they are affiliated with any known terrorist organizations.

Money Laundering

As indicated above, a common definition of money laundering is the process of making proceeds from illegal activity appear legal by “washing” them through other organizations such as financial institutions or businesses that deal in a high volume of cash. Money derived from illegal activities, such as illegal narcotics sales, extortion, or cigarette smuggling, are activities most often associated with money laundering. However, these illegal sources of revenue do not apply to reverse money laundering. Instead, reverse money laundering, as the name implies, takes the distribution of money in the opposite direction. Reverse money laundering involves the distribution of what appears to be the proceeds of a legal business or enterprise and passes it to those who intend to use it for illegal activities, such as terrorism performed by Islamic

fundamentalists. The money can come from a number of seemingly legitimate sources. These activities include distributing money generated from charitable donations, (FATF, 2002) or collected in religious facilities, such as mosques, during religious services (9-11 Commission Monograph, 2004). Money is also generated by revenue from businesses selling commodities such as items like honey (Gerth, 2001). All of these provide a legitimate cover for generating money that can be funneled to organizations promoting terrorist activities. Because the money appears to be from legitimate sources, terrorists can disperse the money through wire transfers or alternative remittance systems, access it from international bank accounts, and physically transport it via traveler's checks or cash (9-11 Commission Monograph, 2004). In effect, the terrorists are hiding their money in plain sight.

Significant Laws and Regulations

Money laundering is not a new problem, but it is a major one. It is estimated that between US \$500 billion and US \$1 trillion is laundered worldwide annually (GAO, 2003a). Significant anti-money laundering legislation has existed in the United States since 1970. The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970, most commonly referred to as The Bank Secrecy Act (BSA), was enacted as a result of drug traffickers using financial institutions, specifically banks, to integrate funds generated from illegal narcotics sales into the mainstream economy. One of the main components of the BSA is its requirement for banks to report cash transactions over \$10,000 (31 U.S.C. §1051). In the years that followed, additional legislation was enacted to address the problem of money laundering. The Money

Laundrying Control Act of 1986 criminalized the act of money laundering and prohibited structuring transactions to evade bank reporting requirements (Federal Deposit Insurance Corporation, retrieved 9/11/2004). Additional legislation followed, such as the 1992 Annunzio-Wylie Money Laundering Suppression Act, which required the filing of Suspicious Activity Reports (SARs) (Federal Deposit Insurance Corporation, retrieved 9/11/2004). Most recently, the USA PATRIOT Act required financial institutions to implement anti-money laundering programs (Federal Deposit Insurance Corporation, retrieved 9/11/2004). Even though the USA PATRIOT Act purportedly targets terrorist financing, the primary focus of this legislation, and the others before it, is on funds derived from the techniques associated with traditional money laundering. The anti-money laundering requirements identified in these pieces of legislation are more appropriate for combating money laundering derived from criminal activity because traditional money laundering requires a clandestine introduction of illicit funds into the financial community. However, this is not required for reverse money laundering because the funds already appear to be legitimate and can be moved easily and without raising many red flags.

Reverse Money Laundering

While many familiar with money laundering acknowledge that the end goal of terrorist financing is different than that of traditional money launderers, they do not see any distinction between the different methods used by terrorists to generate and distribute money. The common misconception is that all terrorist financing involves reverse money laundering, which is not the case. In fact, terrorists have funded, and continue to fund,

their organizational activities through criminal proceeds. Narcotics trafficking, credit card fraud, infant formula fraud, and cigarette tax fraud have all been used to finance terrorist activity (Counterterror Initiatives in the Terror Finance Program: Hearing of the Senate Banking, Housing, and Urban Affairs Committee, 2003). Because money is generated from such illegal activity, terrorists need a way to clean the money so it can be distributed to other members. When this process is utilized to generate and distribute funds, it is more akin to traditional money laundering as opposed to reverse money laundering.

Given the fact that the heightened scrutiny applied to terrorist financing has materialized in the last few years, the concept of reverse money laundering is relatively young. Not until the investigation of the September 11, 2001 attacks and terrorist financing was researched in greater detail did it become highly publicized that terrorist financed their operations differently than traditional criminal organizations such as organized crime rackets and drug cartels. The key difference, as stated earlier, is that sometimes terrorists rely on legally obtained funds to support their cause (FATF, 2002). While this fact has been well documented, little has been published on the specific topic of reverse money laundering. Instead, those looking to research this topic further must identify reports and publications that describe the characteristics of reverse money laundering rather than specifically identifying the topic itself. This has contributed to the fact that many consider terrorist financing and reverse money laundering the same. The National Commission on Terrorist Attacks Upon the United States (9-11 Commission) was tasked with investigating the September 11, 2001 attacks. As a result of its

investigation, the 9-11 Commission released a report on its findings of terrorist financing. While the 9-11 Commission's Monograph on Terrorist Financing describes in great detail the efforts terrorists go through to raise and distribute funds, it does not specifically mention the term "reverse money laundering." However, terrorists' use of charities, wire transfers and bulk cash transfers are all referenced, and the report clearly illustrates examples of how terrorists generate and distribute money. Instead of specifically referring to these activities as reverse money laundering, researchers are forced to look for themes and characteristics common with this form of activity. Such a practice of identifying a theme from multiple observations is a form of inductive reasoning.

The process of inductive reasoning is required of other research as well. The Financial Action Task Force is "an inter-governmental body" created to monitor global money laundering issues and provide guidance on policies to combat money laundering (FATF, retrieved 9/11/2004). Among FATF's many publications, is an annual report that describes developing trends and specific analysis of money laundering typographies. Just as the 9-11 Commission failed to mention reverse money laundering specifically, so too has FATF in its annual reports. However, this does not mean that these annual reports are not helpful in researching the topic. The FATF annual reports discuss terrorist financing through wire transfers, alternative remittance systems and non-profit organizations or charities, which are all indicative of reverse money laundering. While the characteristics of reverse money laundering are present, these reports fail to specifically make the connection.

However, the one thing that these reports do bring to light is the difficulty of detecting the techniques that fit the characteristics of reverse money laundering. Because reverse money laundering appears to be grounded in legitimate commerce, it is difficult to determine when money is being used to assist a terrorist organization or operation. So where should efforts be focused to detect reverse money laundering and prevent the money from getting to its intended targets? Who should take the lead in this operation? Should the legislators assume primary responsibility for addressing this issue? Should it be the financial services industry? Should it be their regulators? Should the technology community be responsible for developing new tools used to detect reverse money laundering? All have increased their presence in this capacity, but have their efforts led to successful results?

As previously stated, reverse money laundering involves using legal funds for illegal purposes. However, reverse money laundering is more complex than that definition implies. There are two components that are crucial to the success of reverse money laundering; 1) How the funds are generated and 2) How the funds are distributed. As you will see, both make detecting reverse money laundering very difficult. Because the funds look like they come from legal sources, they are easier to move and therefore become easier to distribute. Since stopping terrorist financing has become a priority, more resources have been dedicated to the effort to identify and freeze terrorist assets. As a result, terrorists have had to use alternative means to move money (Zarate, 2004). However, this prospect of moving funds through alternative means is easier if the funds look like they are generated from a legitimate source.

One component of reverse money laundering that makes it so difficult to detect lies in the fact that the funds involved are generated from legal sources. These funds can come from a variety of means. Some of these sources favored by terrorists include the use of charities, religious entities, and front companies. Because each of these serve a legitimate purpose in society and business, it is easier for the terrorists to raise and move money because it disguises the ultimate use of the funds.

Without a doubt, one of the favorite methods of raising money for terrorist financing is through the use of charities because it has been one of the most effective ways of raising funds (FATF, 2002). Because charitable donation, or *zakat*, is one of the five pillars of Islamic faith, as a religious requirement, this serves as a readily available source of funds for terrorist to take advantage of (9-11 Commission Monograph, 2004). Charities work so well because they lack significant oversight and because they tend to rely on cash transactions and donations, which makes raising and moving money easier, especially to areas of conflict (GAO, 2003b and 9-11 Commission Monograph, 2004). Those within the charitable services community are keenly aware of this problem. In 2001, shortly after the September 11, 2001 attacks, Khalid Saffuri, president of the Islamic Institute, a group that works to build Muslim political influence, acknowledged that money raised and sent abroad could be used for nefarious purposes because there is no way to control the money once it reaches its destination (Kurlantzick, 2001). Even as the oversight begins to improve, it is still difficult to monitor each transaction to ensure the funds reach the destination its donors intended. To disguise this process, money

raised by charities may not head directly to terrorists. For example, a well-respected and well-intentioned charity in the United States may send the money it raises to a satellite office or to another charity in a country like Somalia or Afghanistan. However, once these smaller charities get the money, which is completely legitimate, these funds may be diverted to terrorists (9-11 Commission Monograph, 2004). Because these countries lack the proper oversight or the ability to ensure that the funds are distributed to their intended causes, as opposed to being diverted to terrorist organizations or their operations, this diversion often occurs without the knowledge of the charitable organization that originally raised the money.

This lack of oversight is one of the reasons terrorists use charities and non-government organizations (NGOs) so efficiently. Terrorists are able to control charitable funds and divert them elsewhere due to the lack of financial controls to ensure the funds end up where they are intended (GAO, 2003b). Even though the use of charitable organizations has been well documented, many are unaware that the funds they provide to charities are being diverted to terrorist organizations (9-11 Commission Monograph, 2004). In 2002, the Benevolence International Foundation was indicted for allegedly fraudulently soliciting and obtaining “donations by falsely representing that the funds would be used solely for humanitarian purposes, while concealing that some of the funds were to be used to support armed fighters” in places like Bosnia-Herzegovina and Chechnya by providing soldiers with military supplies and equipment (9-11 Commission Monograph, 2004).

Another advantage to using charities is the accessibility to a liquid asset. Because charitable donation is often made in the form of cash, it is already in a form that can be transferred quite easily. The difficult step of converting assets to cash has already been accomplished given the very nature of these business transactions. As a result, linking the cash flow back to the source or following it to the terrorist operations or groups has proved difficult (9-11 Commission Monograph, 2004). This was the case when the United States was investigating Ahmed Nur Ali Jumale, the founder of al-Barakaat, a money-remittance system anchored in Somalia. Two non-governmental organizations made unusually large deposits into the account of a charity official in Kuwait for which Jumale had power of attorney. After the funds were deposited, they were moved out of the account in the form of cash. In order to justify this activity, Jumale stated that the funds were forwarded to Somalia for charitable causes. However, because these transactions were made in cash, no other records related to these transactions existed (9-11 Commission Monograph, 2004). Despite reputed connections to Usama Bin Laden, this lack of documentation was a key reason the Federal Bureau of Investigation could not build a substantial case against al-Barakaat and its links to terrorism (9-11 Commission Monograph, 2004).

Because *zakat* is a religious requirement of the Islamic faith, a great deal of money is delivered through donations in mosques or is raised by *imams*, Islamic religious leaders. Financial facilitators, tasked with raising money for terrorist organizations, will often rely on radical imams to divert *zakat* donations at religious facilities or influence imams to encourage the “support of radical Islamic causes” (9-11 Commission

Monograph, 2004). In one case, a place of worship was constructed in part to conceal the illicit activities of a terrorist organization in two different ways (FATF, 2002). One way was to serve as a safe house for “clandestine ‘travelers’ from extremist circles” and the other way was to collect funds with the intent of distributing them to the terrorist organization by funneling millions of dollars from wealthy businessmen (FATF, 2002). Another example of religious leaders supporting terrorists was discovered during the investigation of the Global Relief Foundation (GRF), a charitable organization suspected of supporting al Qaeda. During the inquiry of GRF, following the events of September 11, 2001, investigators considered that an imam at a mosque in Maryland to have supported and raised funds for an international jihadist movement (9-11 Commission Monograph, 2004, 100). Additionally, as a response to the al Qaeda linked bombings of a housing complex for Westerners in Riyadh in May 2003, the Saudi Arabian government removed collection boxes from mosques and banned cash contributions at mosques because of the fear that this money would end up in the hands of terrorists (9-11 Commission Monograph, 2004).

While charities and religious organizations may be the preferred methods of raising funds, it is not the only way terrorists have used legitimate funds to further their enterprises. Legitimate business activities such as selling foodstuffs, selling publications, collecting subscriptions, and charging fees for social or cultural events often serve as fronts to mask the underlying operation of generating funds to support terrorism (FATF, 2003). Yemen, a high-risk area for terrorist activity, produces some of the region’s most expensive honey, so it would not be difficult for terrorist supporters to use this as a

conduit for funneling terrorist funds (Gerth, 2001). In particular, Usama Bin Laden has been linked to using a network of honey shops to generate income to support the al Qaeda terrorist network (Gerth, 2001). The use of honey as a terrorist financing channel is not exclusive to al Qaeda. Egyptian Islamic Jihad, which in effect, merged with al Qaeda in 1998, has also been known to use honey shops to further its cause (Gerth, 2001). Since honey is a staple of life in the Middle East, not only does it provide an air of legitimacy, but it also provides a network with which to move money due to the popularity and multitude of honey shops (Gerth, 2001).

Formal Financial Sector

It is true that terrorists would not be able to operate without sufficient finances, but the ability to raise money would be wasted if terrorists could not get it to where it needed to be. This is where the ability to move funds becomes a critical component of reverse money laundering. Because the funds generated through charities, religious groups and businesses appear legal, it becomes easier to move them through the financial community. Terrorist organizations have successfully transferred money through banks without raising suspicion, not only because they look legitimate, but also because most transactions are small and do not trigger most transaction monitoring thresholds (FATF, 2004).

Financial institutions operating in the United States are required to monitor transactions for suspicious activity and rely on manual or automated transaction monitoring techniques. Manual transaction monitoring, as the name implies, involves

manually reviewing transactions or ad hoc reports summarizing individual or groups of transactions to identify instances of potentially suspicious activity. These reviews are designed to identify types of known money laundering activity, such as structuring, which is the repeated depositing or withdrawal of cash just under the regulatory reporting requirement of \$10,000, or instances where large amounts of cash are deposited into an account and then quickly wired out. Manual transaction monitoring requires analysts to recognize such activity from the reports and develop cases to investigate further.

Automated transaction monitoring is more advanced than manual transaction monitoring and attempts to recognize suspicious activity and report it directly to an analyst for investigation. Automated transaction monitoring can assist in the identification of types of known activity such as structuring or velocity of funds into and out of an account. Automated transaction monitoring is used to consolidate instances of potentially suspicious activity into one system, making investigations much easier. Advanced transaction monitoring through the use of profiling and pattern recognition can also be incorporated into automated transaction monitoring. Profiling involves the analysis of a customer's current transactional behavior against a customer's historical activity, and identifies any significant variations in behavior. A customer's activity can also be compared to that of its peers, which is known as peer profiling. Profiling is not required and is expensive because of the need to compile and standardize the data for the system requirements and the need to support the system. As a result, profiling is most common in large financial institutions where the level of risk may warrant such an investment.

When money is raised through charitable donation or as a result of a seemingly legitimate business, it becomes harder to distinguish between terrorist financing and a normal business transaction. The September 11, 2001 hijackers were able to use wires sent by financial institutions because their transactions looked like they were coming from an acceptable origin. One of the reasons these transactions did not raise suspicion is that they were so different than what typically alerts banks to money laundering activity. There is a difference between the large amounts of money that are laundered by criminals and the smaller amounts of money that are acquired and distributed from seemingly legitimate sources (Kochan, 2003). Additionally, once the funds are transferred to and from seemingly legitimate sources, it becomes almost impossible to track the funds (Elizur, 2002).

Even when the transactions are larger than normal, they still tend to avoid raising any red flags because they lack the suspicious traits that may be identified by the transaction monitoring techniques utilized by banks and other financial institutions to detect suspicious activity (Kochan, 2003). In 2001, just before the attacks, plot facilitator, Ali Abdul Aziz Ali, sent wire transfers to ringleaders Muhamad Atta and Marwan al Shehhi, including one for \$70,000, which went from the United Arab Emirates through Citibank (9-11 Commission Monograph, 2004). Khalid Sheikh Mohamed, one of the financial backers of the September 11, 2001 terrorist attacks, was upset that Ali would risk sending \$70,000 in one transaction because he was worried the size of the transaction would raise suspicion (9-11 Commission Monograph, 2004).

However, Ali did not share this sentiment because the funds had been sent under the auspice of a transaction involving a Dubai computer company which had been set up to provide cover for just this reason. It was customary for computer companies in this region to transfer sums of money that size, so Ali was not worried that the activity would set off any warning signs (9-11 Commission Monograph, 2004). As it happened, Ali was correct because nobody was alerted to the fact that these funds were intended to support the would-be hijackers.

Additionally, since much of the financing used to support terrorists is generated from cash, it is easy to get people to physically move it in large enough quantities to help support a mission, but small enough not to be detected. But perhaps the most successful way terrorists are able to move money is through the use of informal value transfer systems (IVTS) such as *hawalas* and unregistered money service businesses. As a result, terrorist funds can move freely in and out of the business and the financial world.

Informal Value Transfer Systems

Since the events of September 11, 2001, it has become more difficult for terrorists to move money through financial institutions because greater scrutiny is being given to the funds transfer and high-risk destinations. As a result, terrorists have had to reassess their methods of moving money, and are being forced to move money across borders in bulk cash shipments via cash couriers. Since money donated at mosques or to charities is often in the form of cash, it is already in a form that is easy to move. Additionally, because most terrorist operations do not cost much money to carry out, they can continue

to be supplied with enough cash to sustain their operations until they have been completed. The practice of smuggling money in and out of countries becomes even easier where border security is lax or non-existent. For example, cash couriers will fly into a country with a sealed envelope full of cash. Once on the ground, the couriers could be directed to an address where the envelope would be dropped off, or are met at the airport by a stranger who picks up the envelope (DeYoung, 2001). Often, these couriers turn around and go right back home never knowing the ultimate destination or purpose of the transaction (DeYoung, 2001). While this type of transaction may limit the amount of money a courier can bring into a country at any one time, given the right circumstances, transporting cash across the border in bulk can be very effective. According to reports, al Qaeda was able to move approximately \$1 million from the United Arab Emirates into Pakistan where the money was then couriered into Afghanistan (9-11 Commission Monograph, 2004). While this practice was in place prior to September 11, 2001, it was not used as frequently because of easy access to the mainstream financial community.

Moving money through financial institutions is efficient but it has become riskier for terrorists to do so. Moving cash across borders is perhaps a bit less risky but only if done in quantities small enough to go undetected. As a result, terrorists need a way to send money in larger amounts while at the same time not exposing the true nature of the transaction. To accomplish this goal, terrorists organizations such as al Qaeda, Hizballah, HAMAS (Harakat al-Muqawama al-Islamiya – Islamic Resistance Movement), and others have turned to IVTSs as an alternative to transmitting money via financial institutions (GAO, 2004). While IVTSs are unregulated money remittance services, all

are not conduits for illegal activity. IVTSs provide the ability to send money quickly to almost anywhere in the world, including places of conflict and places where a formal banking system has not been established. In many parts of the world, such as Somalia, these IVTSs are the only way to send and receive money. A *hawala* is perhaps the best-known example of an IVTS.

Hawala, which means “transfer” in Arabic is an alternative remittance system primarily used in immigrant ethnic communities to transmit money, based on a system of trust, through established relationships and connections in other geographical regions (United States Department of the Treasury, 2002; GAO, 2003b). An example of a hawala transaction looks something like this: A person in the United States wants to send \$2,000 to someone in Somalia. The person in the United States visits a *hawaladar*, an individual hawala dealer, who will make arrangements with a local hawaladar in Somalia to deliver the amount, less a service fee, to the recipient in Somalia (United States Department of the Treasury, 2002). The hawaladar in the United States will not actually send the money but instead collects it from the sender. The hawaladar in the Somalia will settle up with the hawaladar in the United States at a later date, or the hawaladar in Somalia may instruct the hawaladar in the United States to pay another hawaladar on his behalf (Passas, 2004). This form of money remittance is a favorite of immigrant ethnic communities because they can often get a better exchange rate than they would by going to a bank or licensed Money Services Business (MSB) such as Western Union (Passas, 2004).

In the United States' response to terrorists' use of IVTSs, section 359(a) of The USA PATRIOT Act expanded the definition of MSBs to include:

a licensed sender of money or any person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institution system (2001).

Hawalas are covered by this definition, and as a result, are required to register with the FinCEN (United States Department of the Treasury, 2002). As a registered MSB, there are certain requirements that accompany this designation. Some include the filing of Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs) and record keeping requirement (United States Department of the Treasury, 2002). These reporting and record keeping requirements are meant to help identify and investigate suspicious transactions before any damage can be done. However, not every hawala registers with FinCEN, and as a result there are quite a large number of unregistered hawala brokers within the United States (Passas, 2004). Since the activities at many hawalas are not being monitored, terrorists can use these resources to transfer cash generated from charities or front companies throughout the world without having to worry about who is watching.

It is exactly this point that seems to be one of the biggest problems in detecting terrorist financing through the use of underground IVTSs. Terrorists like to use hawalas and underground IVTSs because there is no customer identification requirement.

Usually, there is little documentation maintained by hawaladars when they do business with their customers. As indicated above, not all IVTSs and hawalas are used to support

terrorist networks, and those operating these organizations may be unaware of the true nature of the transaction, but some reports indicate that in certain instances when hawaladars know their customers are breaking the law, the true identity of the customer is not required and no notes or documentation are kept at all (United States Department of the Treasury, 2002). However, there have been cases where detailed evidence of hawala transactions has been recovered. While some transactions are kept in code and destroyed shortly after the transaction is complete (United States Department of the Treasury, 2002), other hawaladar records have been discovered in electronic ledger format covering almost five years worth of activity (Passas, 2004). While hawala transactions may be encoded to protect the identity of those involved, hawaladars still need to keep records that prove the money was delivered, even if it is encoded (Passas, 2004). Sometimes it takes a little cooperation to decode these transactions (United States Department of the Treasury, 2002).

While those familiar with money laundering may not be as equally familiar with reverse money laundering, the principles and techniques associated with reverse money laundering have been well documented. Terrorists, in particular, have used this technique to successfully support their organizations and fund their operations. The money raised through reverse money laundering is generated from sources such as charities, religious associations and businesses. This makes it easier for terrorists to move money than if it was derived from criminal activity because the money appears to be coming from a legitimate source. Any transactions involving these funds appear to be part of the normal course of business. If a terrorist wants to send money to Jordan, it can be done via a wire

transfer through formal financial institutions under the guise of the disbursement of a charitable contribution. Under a different example, if a terrorist wants to send money to a country such as Iran, the money can be withdrawn from the account of a charity and sent via an IVTS such as a hawala. The combination of raising and transferring money in this fashion helps establish the process of reverse money laundering and are contributing factors for making it so difficult to detect.

Increased Scrutiny

Following the September 11, 2001 attacks, the USA PATRIOT Act was passed in an attempt to increase efforts to prevent terrorist operations and terrorist financing, specifically with regard to Islamic fundamentalist terrorist organizations. Also, since that time, regulators of the financial services industry, such as the Federal Reserve and the Office of the Comptroller of the Currency, have increased the number and intensity of their BSA examinations and levied increasing fines for failure to comply with anti-money laundering rules and regulations. Additionally, banks have spent millions of dollars on new technology, personnel and compliance procedures to enhance their anti-money laundering capabilities. However, these measures are primarily directed at traditional money laundering techniques and fail to adequately address reverse money laundering.

The USA PATRIOT Act was constructed to target terrorist financing but several of its requirements may not help prevent reverse money laundering. For example, the customer identification mandate of Section 326 is meant to increase the amount of information financial institutions know about their customers by requiring them to collect

the name, date of birth, address and identification number, such as Social Security Number or Tax Identification Number, of all new customers (USA PATRIOT Act, 2001). However, this only requires financial institutions to have a reasonable belief that they know the true identify of their customers. Additional information such as source of wealth or how the account will be used would help financial institutions know their customers better. While financial institutions will be required to take reasonable steps to ascertain this additional information for their private banking customers, there is no such requirement to collect this information for all of their other customers (31 C.F.R § 103.178). Additionally, the customer identification requirement of Section 326 only applies to new customers and does not apply to customers that already have an existing relationship with the financial institution (31 C.F.R § 103.121), meaning that if an existing customer was already conducting reverse money laundering, they may be less likely to undergo this type of scrutiny. Because reverse money launderers appear to be legitimate, and their credentials may prove to be valid, the customer identification requirements may not aid in preventing this type of activity.

An additional mandate of Section 326 requires financial institutions to check the names of its customers against terrorist watch lists, but at this time, there is no official terrorist watch list that financial institutions are required to check against (USA PATRIOT Act, 2001). Instead, the list maintained by the Office of Foreign Assets Control (OFAC) is the only one resembling such a terrorist watch list, but all United States companies, not just financial institutions, were prohibited from conducting business with entities on this list prior to September 11, 2001. OFAC falls under the

United States Department of the Treasury (Treasury) and has a long history of applying the economic sanctions of United States foreign policy. Its roots can be traced back to before the war of 1812 when sanctions were imposed against Great Britain for harassing United States sailors (Office of Foreign Assets Control, retrieved 2/20/06). Congress passed the “Trading With the Enemy Act” during the United States Civil War, which imposed trading sanctions on the Confederacy that were administered by Treasury (Office of Foreign Assets Control, retrieved 2/20/06). The Trading With the Enemy Act was updated in 1917 to address sanctions related to World War I, and following the invasion of Norway in 1940, the precursor to OFAC, the Office of Foreign Funds Control, was created in an attempt to prevent the Nazi regime from benefiting from an occupied countries foreign exchange (Office of Foreign Assets Control, retrieved 2/20/06). OFAC was officially created in December 1950 when China entered the Korean War and President Truman ordered the blocking of all Chinese and North Korean assets subject to United States jurisdiction (Office of Foreign Assets Control, retrieved 2/20/06).

In the wake of the September 11, 2001 attacks, President Bush, using the authority granted under the International Emergency Economic Powers Act and the National Emergencies Act, issued Executive Order 13224 which expanded the entities on the OFAC list to include approximately 30 terrorist entities and ordered the blocking of their property (E.O. 13224, 2001). The entities identified in Executive Order 13224 were only the beginning as, over the next few months, hundreds more were added to the list. The number of entities on the OFAC list continues to grow with new updates and there

have been over 150 updates to the OFAC list or country sanctions programs since October 2001.

The USA PATRIOT Act also requires enhanced due diligence for certain types of relationships considered higher risk, such as private and correspondent banking. A private banking account, as defined by Section 312 of the USA PATRIOT Act, is an account established on behalf of one or more individuals with a direct or beneficial interest managed by a representative from a financial institution acting as a liaison between the financial institution and the beneficiary of the account and requires a minimum aggregate of no less than \$1,000,000 (2001). The USA PATRIOT Act defines a correspondent account 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” (2001). In other words, a correspondent banking relationship, in this case, is one that exists between a United States bank and a foreign bank where each bank can conduct business with each other on behalf of their customers. These banking relationships are considered high risk because of the secretive nature of private banking and the lack of knowledge of the ultimate beneficiary or originator associated with correspondent banking transactions. However, because statutory parameters identified in the USA PATRIOT Act limit the enhanced due diligence requirements to private banking accounts with a mandatory minimum aggregate of \$1,000,000, a financial institution could avoid conducting enhanced due diligence on its private banking customers by lowering its mandatory balance requirement to \$999,999. Additionally, Section 312 of the USA PATRIOT Act limits the enhanced due diligence

requirements for correspondent banking to those operating under an offshore banking license, operating under a banking license issued by a country designated as noncooperative with international money laundering guidance or operating under a banking license designated “by the Secretary of the Treasury as warranting special measures due to money laundering concerns” (2001). These statutory requirements are extremely focused, allowing for the potential gaps in coverage to be exploited.

In addition to enhanced legislation and regulatory requirements, financial services regulators are conducting more frequent and more intense BSA examinations. Many of these examinations have resulted in increased fines. In 2004 Riggs National Corporation, the parent company of Riggs Bank NA was fined \$25 million for failing to report suspicious activity (O’Brien, 2004). Later in the year, AmSouth Bancorporation was fined \$50 million for similar reasons (Goodman, 2004). While the banks are paying the penalty for noncompliance, these measures are reactive in nature and are the result of violations of BSA requirements developed to combat traditional money laundering.

While new and more robust automated anti-money laundering technology is being implemented on a wider scale, much of the technology is geared to detecting patterns of money laundering based on historical activity and the development of profiles that fit traditional money launderers. While it is encouraging to see more financial institutions enhancing their money laundering detection capabilities, this may not be the best approach for combating reverse money laundering. What makes these tools so successful for detecting money laundering is the fact that these systems rely on profiles built from

historical activity. However, as noted by the 9-11 Commission, there has been no successful attempt to profile Islamic fundamentalist terrorists or terrorist activity (9-11 Commission Monograph, 2004). I believe that this inability to develop a profile of a terrorist limits the effectiveness of much of the anti-money laundering technology and helps contribute to the difficulties of detecting reverse money laundering.

Even though money laundering detection tools currently have a gap in detection capabilities, this does not mean that anti-money laundering technology could not be successfully utilized for reverse money laundering scenarios. One of the advantages of employing automated money laundering detection tools is that they provide a great deal of coverage; something that could never be accomplished manually. Therefore, money laundering detection tools can help identify terrorists if they know what and who they are looking for. This means that if given the right set of indicators or targets, money laundering detection tools can examine financial transactions in an attempt to identify the given parameters they have been instructed to look for. However, the tools need to be configured to know what they should be looking for, and in the case of reverse money laundering, this requires specifics. Perhaps the best way to provide the tools with specific information is to increase the intelligence gathered on terrorists so this information can be distributed to the financial community, which can then feed that information into their money laundering detection tools. While it is important to obtain the necessary intelligence, it is also important to pass on that information to those that will benefit from knowledge sharing if that information coincides with the data gathered from the financial community. Companies in the financial services industries would therefore be alerted

when transactions involving these entities are detected. Additionally, the investigators that review the transactions would be better equipped with better intelligence to determine if the activity identified by the money laundering detection tools are indicative of terrorist activity through reverse money laundering. Not only would this increase the efficiency of the interdiction tools but also it would increase the efficiency of the investigators. Moreover, because financial institutions would be gathering additional information about the parties involved and techniques observed through reverse money laundering scenarios, this would further contribute to the amount of intelligence gathered on terrorist activity if shared throughout the financial community. However, this all stems from the specific knowledge of whom and what financial services companies should be looking for. Without this knowledge, financial services companies are forced to rely on anti-money laundering tools that are geared toward traditional money laundering detection and face a gap in detecting this type of terrorist financing activity.

Literature Review

The 9-11 Commission, Financial Action Task Force (FATF), and Government Accountability Office (GAO), as well as sources not affiliated with any official agency, all produce valuable works related to money laundering. Because these reports touch on the wide spectrum of money laundering, they can be used to study reverse money laundering as well. Stefan D. Cassella is one of the few that has a published body of work focusing on this topic, but while Cassella does specifically reference reverse money laundering, he does not offer the level of detail identified by other works where reverse money laundering is identified by technique, as opposed to by name. Instead of focusing on the techniques and providing detailed examples or a case study of any of these techniques, he chooses to focus on current legislation that could be used to help combat this problem (Cassella, 2003). The 9-11 Commission Monograph is of particular importance because it is one of few sources that provide such detailed examples of how terrorists, particularly al Qaeda terrorists, move money through the use of these techniques. However, as we begin to analyze these reports and publications, it is important to understand the methodology used to generate the results because the choice of methodology results in different imperfections.

9-11 Commission, FATF and GAO

The 9-11 Commission is perhaps the most authoritative work on money laundering related to terrorist financing because it provides detailed examples of how the terrorists carried out their attacks on the United States on September 11, 2001. However,

when using the 9-11 Commission's Monograph on Terrorist Financing, the reader must be aware of the scope of this report. For example, the 9-11 Commission Monograph focuses on the events of September 11, 2001. While other terrorist attacks are mentioned, the primary focus is on the hijackers and the events surrounding that event. Because the attacks were carried out by al Qaeda, it is understandable that most of the references to terrorist financing related to al Qaeda, and specifically how it funded the 9-11 attacks (9-11 Commission Monograph, 2004). Much of this information was obtained from interviews conducted with members of the intelligence community, investigations conducted by law enforcement, and information previously reported to intelligence agencies. Based on the nature of the 9-11 Commission's task, the use of these methodologies seemed most appropriate. Other research options such as conducting a survey asking the same questions of each interview subject would not provide the in-depth responses required to understand what happened leading up to September 11, 2001. The events of September 11, 2001 touched so many areas, that in order to conduct a comprehensive survey, not all components would be applicable to the backgrounds of each interview subject. To address this issue, conducting interviews, performing investigations, and relying on previously produced reports and research provided the appropriate focus and level of detail required for the 9-11 Commission to accomplish its goals.

FATF uses a similar approach to produce its reports on money laundering typologies. FATF collects information on money laundering from its worldwide members when it holds its annual meetings to discuss existing and new emerging money

laundering trends. Based on these meetings, FATF publishes a list of the topics covered during these sessions and provides examples of each. The information gathered here is based on interviews of fellow members, field research, and content analysis. The information that gets published comes from members who share their experiences, and previous incidents related to money laundering. In order to protect ongoing investigations or the integrity of reports, country names, currencies, and other identifying details, are modified in these typology reports (FATF, 2002).

The GAO reports on money laundering also reflect these types of approaches. For example, the GAO report on terrorist financing through the use of alternative financing mechanisms relied on reviewing documentation and conducting interviews with officials from United States agencies including the Departments of Justice, Homeland Security, Treasury, State, Defense, and several intelligence agencies (GAO, 2003b). In addition to these United States agencies, the GAO report also relied on information provided by non-government entities, and conducted field work, which involved interviewing officials in foreign jurisdictions with other international agencies like INTERPOL and the European Union (GAO, 2003b).

When reviewing the various research methodologies used by these sources, interviews appear to be a common element in each. Given the complex nature of reverse money laundering, it appears that this would be the best approach to take when conducting research on this topic because of the careful distinction that needs to be made between traditional money laundering and reverse money laundering. However, before

the research begins, it is necessary to clearly understand and define what it is we wish to study.

Based on the results of current research, conceptualizing reverse money laundering does not appear to be a high priority. “Conceptualization is the process by which we specify precisely what we mean when we use particular terms” (Babbie, 2005). But this is difficult to do when referring to reverse money laundering because most research does not even mention this as a distinct genre. As previously mentioned, reverse money laundering is often included with traditional money laundering, even though they are quite different. Very few published reports make the distinction between the two. The 9-11 Commission Monograph, the GAO reports on alternative financial mechanisms and challenges faced by law enforcement, and the money laundering typologies published by FATF, all fail to draw a distinction between reverse money laundering and traditional money laundering (9-11 Commission Monograph, 2004; GAO Terrorist Financing, 2003; GAO Combating Terrorism, 2004; FATF Report on Money Laundering Typologies, 2002-2004). However, while each fail to conceptualize this issue, each describes the processes and techniques associated with this topic in great detail. As a result, a reader is only aware that these techniques can be applied to the study of reverse money laundering if the reader knows what reverse money laundering is in advance.

Research Based on Interviews

Since very few sources refer to reverse money laundering as a concept different from traditional money laundering, it is important to identify the ones that do. One in

particular is written by Nick Kochan. In his article *Money-laundering Controls Look All Washed Up*, Kochan discusses terrorist financing but makes a point to distinguish reverse money laundering as distinct from traditional money laundering. His information is gathered from interviews with subject matter experts who are aware of the differences between money laundering techniques. One such expert identifies reverse money laundering as “turning clean money into dirty money to use it as an instrumentality for terrorism” (Adam Bates, as quoted in Kochan, 2003). While this is a very simplified version of reverse money laundering, clearly the concept has been identified. Furthermore, it represents a working definition allowing readers to understand what is meant by this concept (Babbie, 2005).

Once this concept is defined, the focus turns to measurement. Measurement is crucial to research because it “involves actually making observations and assigning scores” to the observations (Babbie, 2005). When conducting interviews, measurement relies on the qualification of statements from the interview subjects as opposed to the quantification of numbers or figures gathered from statistical analysis. Interview studies typically draw from a smaller pool of candidates than other research methods because they tend to be more in depth. For example, the national census, which is about as comprehensive a study as there is, relies on survey questions because the scope is so large that it would take too long and be far too expensive to conduct an interview of every person in the United States (United States Department of Commerce, Bureau of Census, 2000, retrieved 10/14/2004).

When conducting a study based on interviews, measuring the concept starts with asking questions and analyzing the answers, and in an interview methodology, it is the answers that provide the results. For example, when authors attempted to identify the vulnerabilities charities face that contribute to the facilitation of terrorist financing, it is very difficult to quantify this kind of information. As a result, authors probe those in the field to get a better understanding of what these vulnerabilities are and how they can be exploited. Christopher H. Schmitt, Joshua Kurlantzick and Philip Smucker approached exactly this topic and chose to gather information in an interview methodology. By interviewing executives of Islamic organizations such as Khalied Saffuri, President of Islamic Institute, a Washington D.C. based group that attempts to build Muslim political influence, and others associated with this area, the authors were able to assess these vulnerabilities through the responses they received to their inquiries. They were able to analyze their results and helped raise awareness to the fact that terrorists were using charities, and other not-for-profit organizations, as conduits to supporting their networks (Kurlantzick, 2001).

While interviews are particularly successful methodologies when trying to qualify data, they can still be used effectively when trying to quantify data. One such example is the 9-11 Commission's task of investigating the September 11, 2001 attacks. One of its goals was to determine how much it cost to fund the attacks themselves. Much of the information that was gathered to assist with the calculations was gathered from interviews of investigators who tracked the terrorists' activities prior to the attacks. Based on these interviews, the 9-11 Commission was able to quantify the terrorist attacks

and estimate that it took approximately \$400,000 - \$500,000 to coordinate the attacks (9-11 Commission Monograph, 2004).

But why did the 9-11 Commission decide to collect data in this manner? Certainly there were other ways of gathering information about such activity. However, these other options presented obstacles that could not be overcome given the scope of the task confronted by the 9-11 Commission. One such option, which ultimately was not chosen, was reviewing SARs for terrorist related activity. Although, prior to the events of September 11, 2001 banks were required to file SARs regarding any banking activity that is considered suspicious, consulting these reports did not seem like the best approach. SARs have been filed with FinCEN since 1996 and contain the parties involved, the amounts involved, and a summary of the suspicious activity. On the surface, SARs seem like they would be a good source from which to collect the dollar amounts involved in the terrorist attacks because of the historical information that they contain. However, prior to the September 11, 2001 attacks, terrorist financing was not given the same attention it is given today, and may not have been captured by SAR filings. The SAR Activity Review Trends and Tips published in October 2001 did not even include a category for terrorist financing (Financial Crimes Enforcement Network, 2001). An additional problem of SARs is that they rely on the activity actually being detected and reported, and it has been well documented that the September 11, 2001 attackers' financial activities went largely undetected and unreported. The 9-11 Commission's ultimate view on using SARs to detect terrorist financing was that the "analysis appears to be of little use in ferreting out a sophisticated terrorist fundraising

operation” (9-11 Commission Monograph, 2004). As a result, when compared to the other option of reviewing historical SAR filings to piece this puzzle together, the approach taken by the 9-11 Commission seems like an appropriate methodology.

As previously stated, no research study is impervious to error. The value of the study is gauged on the reliability and validity of the research methodology and the measurement of its results. “Reliability is a matter of whether a particular measurement technique, applied repeatedly to the same thing, will yield the same result each time” (Babbie, 2005). This is a crucial component to any research because if the methodology is not reliable, the research cannot be trusted and it may yield results that are wrong or inaccurate. When the methodology of a study relies on the results of interview subjects, it is important to understand how the data was collected. Perhaps the most important element of interviews is the selection of the subjects. If the researcher conducts interviews of people from different perspectives on the same subject matter, the study may lack reliability (Babbie, 2005). In order to get reliable answers, the researcher must be able to rely on the way he or she collects data. For example, if the questions asked during an interview are not clear and easy to understand, the subject might not be able to provide accurate answers because he or she is unable to comprehend the concept of the interview (Babbie, 2005).

While establishing reliability is an important component of a successful study, judging the validity of that same research is just as important, if not more so. In fact, a reliable study does not necessarily guarantee that it is a valid study. Validity embodies

the critique of whether or not the study accurately reflects what it was designed to measure (Babbie, 2005). To demonstrate this concept, let us use an example of a study examining the insurance industry's vulnerability to money laundering. If the researcher conducting this study decided on an interview methodology to gather data, the researcher may decide to interview the vice presidents of corporate security, compliance and account opening at various insurance companies, as well as interviewing state regulators that govern the insurance industry. This study seems like it would have the components of a reliable study, but that does not automatically make it valid. How could this happen? If the researcher did not ask the right questions the researcher would not get the answers he or she needs. For example, if the researcher interviewed these individuals and only asked about their awareness of money laundering in banks or money service businesses, the answers provided by those questions would not contribute to the validity of the study because the real goal was to discuss money laundering and the insurance industry.

The United States Department of the Treasury's report to Congress on underground banking systems demonstrates the concept of validity. Like other government reports, the data that makes up the results of this report was gathered from interviews with law enforcement from federal, state, local, and foreign offices as well as representatives from the Federal Reserve Board and international financial organizations (United States Department of Treasury, 2002). Since these sources are common of government reports, what makes the validity of this report stand out is the consultation with Nikos Passas, then of Temple University (United States Department of Treasury, 2002). Passas is a recognized expert in the field of informal value transfer systems and

has spoken with other anti-money laundering experts at conferences such as “How Money Moves: A Threat to Public Security” held in September 2004 at Rutgers University. His contribution to this report on underground banking systems provides a basis with which to judge the findings presented in this report.

Edward Alden also demonstrated the appropriate use of interview subjects when he examined the proposed anti-money laundering regulations governing correspondent banking in July 2002. Mr. Alden’s goal was to gauge the financial industry’s reaction to the proposed regulations that would require United States banks to closely examine its business relationships with foreign institutions. To accomplish this goal, Alden could have used a number of different methodologies. A survey of banking officials would have been appropriate, as would a study on the number of complaints written in response to the proposed regulation. However, given the nature of the publication and time constraints involved with generating results, an interview methodology seemed most appropriate. To gather his research, Alden interviewed a member of the Association for Finance and Trade and an attorney at the law firm Akin Gump who specializes in money laundering regulations (Alden, 2002). Because Alden was focusing on anti-money laundering regulations related to banks, he interviewed seemingly reliable sources; one being a member of a trade group for that particular industry and the other an attorney whose primary focus was the topic at hand. The identification of the proper interview subjects was also demonstrated in an article published by Robert O’Harrow Jr., David S. Hilzenrath and Karen DeYoung. These authors attempted to identify the flow of money used to support terrorist operations. To provide a better understanding of the topic, they

interviewed a deputy director of the Center for the Study of Terrorism and Political Violence at St. Andrews University in Scotland (DeYoung, 2001). The goal of their article was to understand the flow of terrorist money, so by going to an expert in the field, the results of this research would appear to be valid. Based on the area of expertise possessed by these interview subjects, it would appear to the readers that the choice of these authors was valid.

The primary goal of the 9-11 Commission Monograph was to identify the root of al Qaeda's terrorist financing of the September 11, 2001 attacks and what factors contributed to the success of the plot. The methodology chosen to gather much of this research included interviewing intelligence analysts, law enforcement agents and government officials (9-11 Commission Monograph, 2004). As a result, it is probably safe to say that the results can be considered reliable, excluding for a moment the impact of the different variables that may impact an interview, which will be addressed a little later. But while the results of the research appear reliable, are they still valid? Keeping in mind the 9-11 Commission's goal of identifying the root of al Qaeda's financing, a review of the commission's findings must be undertaken. In the end, the 9-11 Commission was able to identify how the al Qaeda operatives were financed, how they raised and moved money, the failures of the intelligence community to detect such activity, and a lack of cooperation from foreign governments (9-11 Commission Monograph, 2004). Based on the goals of the proposed task identified by the 9-11 Commission, the results of their research would appear to be valid. The data collected and conclusions reached from the results of the investigation are the result of the 9-11

Commission's methodology of interviewing individuals with experience and direct involvement with this area of interest and asking pertinent questions.

While interviews offer the ability to obtain a level of detail that may not be available from other research methodologies, interviews are not without their limitations. One such limitation is the personnel required to conduct research via interviews. Because interviews require a person to ask questions and document the responses, at least one representative from the research study needs to be present for each interview. Finding people to conduct this work can be difficult enough, but finding qualified people can be even tougher. In addition to staffing concerns, there are also timing issues involved with conducting interviews. Since interviews tend to be in-depth, they generally take much longer to complete and require more planning than other research methods, such as a survey.

While interviews may have some drawbacks, perhaps more challenging are the different variables that naturally present themselves and may influence the outcome of the research. Because subjects provide different answers and each set of answers is dependent on the interview subject, it is very difficult for interviews to maintain reliability. However, because in the case of this study interviews will be conducted with subject matter experts, they will prove to be more valid, which in this case is more important than being reliable. The variables from interview to interview are difficult to manage because each interview is a unique event. For example, in advance of an interview a researcher may try to manage the variables by compiling a list of question to

ask the interview subject. However, not every interview will have the same response. These different responses may lead to unscripted questions that, while not planned for, might provide valuable information that contributes to the research. Another variable may include the interviewers, as different people may interview different interview subjects. Other variables that could contribute to a varied degree of results include the interview environment, the experience of the interviewer or the experience of the interview subject. An interview conducted in a private conference room may yield different results if the same person were interviewed at his or her desk in front of colleagues or supervisor. An inexperienced interviewer might not ask the appropriate follow up questions that a more experienced interviewer would. Also, the answers or perspective provided by an interview subject who has been working in the field of interest for five years may differ from that of somebody in the same position for 20 years or from somebody who has been in the same position for the same period of time, but at a different company. Some of the variables are inherent to the interview methodology, but it is important to try to manage these variables to maintain the integrity of the research results.

Even with these drawbacks and variables, interviews are a valuable way to gather information when given the right research environment. Given the time involved in organizing, preparing for and conducting interviews, they work very effectively on smaller research assignments. Additionally, if the researcher is dealing with a small research group, the interviewer can devote more time to spending with the research subjects and obtain in depth responses. Furthermore, interviews provide the opportunity

for subjects to expand on any questions asked by the interviewer or clarify any questions that may appear unclear. When reviewing the various research methodologies, the interview approach would appear as a logical choice to study reverse money laundering.

Hypothesis

The characteristics of traditional money laundering that lend themselves to aid in its detection are much different than those involved in reverse money laundering. Traditional money laundering usually involves large, frequent, structured, or anomalous transactions. Current anti-money laundering techniques, particularly transaction monitoring, are geared toward detecting such unusual activity. However, as we have seen, this type of activity is not typical of reverse money laundering. Instead, transactions that are part of reverse money laundering schemes appear to be transactions normal for a business or enterprise, and as such, they appear innocuous, which make them extremely difficult to detect. Compounding this problem is the fact that many of those that perpetrate reverse money laundering do so outside of the formal financial sector where the regulation and monitoring of transaction activity is almost non-existent. Therefore, we must take a different approach to detecting and preventing reverse money laundering than we do with detecting and preventing traditional money laundering.

But what should that approach be? Should the focus be on developing new technology? Perhaps the answer lies in additional legislation increasing the “watchdog” requirements of financial institutions? Regardless, any new efforts to try to detect and prevent reverse money laundering will sprout from intelligence gathered on those involved in reverse money laundering and the types of mechanisms used in the process. Otherwise, how will we know how to configure the technology without first knowing what to look for? How will the financial services community be able to increase its vigilance without knowing who and what industries, geographies or organizations its

members should be aware of? Therefore, it is the hypothesis of this study that the best way to help detect and prevent reverse money laundering is by increasing the effort spent on gathering intelligence on those that carry out reverse money laundering schemes, particularly Islamic fundamentalist terrorist organizations, so that we may enhance our efforts and make our prevention and detection techniques more efficient.

Methods

Quantifying the impact or cost of reverse money laundering is very difficult because the metrics that are used to report money laundering do not account for reverse money laundering. However, identifying the potential impact of reverse money laundering is important because it provides an idea of the amount of damage it contributes to and helps justify that it is a major problem worth investigating further. For example, the September 11, 2001 attacks were catastrophic in terms of physical damage. The insurance industry was faced with a \$30 billion payout and the airline industry required a \$15 billion bailout from the federal government (Rubin, 2001). Then there is the loss of human life, which cannot easily be measured in financial terms. While financial institutions are required to report money laundering and terrorist financing, the Suspicious Activity Reports used to report such activity do not specifically identify reverse money laundering as a category for reporting purposes. As a result, researchers are required to rely on other areas of analysis to qualify the impact of reverse money laundering. One of the most effective ways to accomplish this is by collecting data from industry experts through interviews.

Research Design, Data and Methods

Subjects

The information for this study was gathered from interviews with subject matter experts. The goal was to get a consensus of the best approach to detect and prevent reverse money laundering, so interviews were conducted with representatives from different areas that serve the financial services industry. These different perspectives came from interviewing current members of the public sector tasked with investigating and prosecuting money laundering and terrorist financing cases, former federal investigators turned consultants, current or former anti-money laundering compliance officers at financial institutions, and representatives from the technology sector specializing in transaction monitoring software designed to detect suspicious activity. This setting established the dependent and independent variables (Babbie, 2005). Given the goal of this study, the different perspective of each interview subject was important and represented an independent variable. The answers provided by the interview subjects indicated an area of focus that will enhance the detection and prevention of reverse money laundering, which represents the dependent variable.

In addition to the variable of perspective provided by the different job descriptions, there were other variables involved as well. One such important variable was the experience level of each interview subject. In an attempt to standardize this variable, the interview subjects were selected for this study because each is a recognized subject matter expert with years of experience in their chosen field. These individuals deal with this issue on a daily basis. Additionally, they communicate with others in their

respective fields and have a reasonably strong indication of what others in similar positions would have to say on the topic. As a result, the answers provided by the interview subjects are valid because the interview subjects were appropriate for the area of the study.

Because the focus of this study was an attempt to identify if an increase in intelligence is the most appropriate way to combat reverse money laundering, the focus of the interview questions deal specifically with this issue. This was important because for the responses to maintain validity, they must be relevant to the issue at hand. For example, the first question asked of the subjects attempted to gauge their familiarity with the term “reverse money laundering.” Once this was established, the interview subjects were asked where efforts should be focused in order to enhance detection of reverse money laundering and then asked to choose between intelligence, legislation, information sharing, technology, or “other,” and rank them in order of importance. Following the ranking of their choices, the interview subjects were asked to explain the reason for ranking their choices in that particular order. The rankings were compared with the hope of developing a consensus of where efforts should be focused. Additional questions such as who bears the primary responsibility for detecting reverse money laundering helped establish the interview subjects’ opinion of who should lead this effort. Another question addressed the importance of the dissemination of restricted entity lists whose members are identified as a result of intelligence gathering and what improvements can be made to make the use of these lists more effective. A copy of the interview questions is attached as Appendix A.

Ethical considerations must be addressed in every research scenario. In the case of this study, the research was conducted through interviews. The results of the interview were confidential so the identity of the interview subjects was also protected. Additionally, the participation was voluntary and since there was little risk that the subjects would not participate in the study and the true intent of the study was not masked, there was no need to deceive the participants in order to provoke responses to the interview questions.

Apparatus

The unit of analysis in this study was the individual represented by each interview subject. The purpose of the study was to determine if there was a consensus that an increase in intelligence gathering is the most appropriate way to combat reverse money laundering, and the units of analysis were the individuals interviewed to obtain the information relevant to this process. The individuals represented different groups, such as the public sector, consultants, or bank officers, and they “may be considered in the context of their membership in different groups” but the results were still being measured by the data obtained from each individual (Babbie, 2005)

When conducting research, two concepts must be addressed that could have impacted the units of analysis. One is the concept of ecological fallacy and the other is reductionism. The threat of ecological fallacy appears when conclusions are reached about individuals when the results are based on information gathered from groups

(Babbie, 2005). This study was not vulnerable to ecological fallacy because it did not attempt to make conclusions about individuals based on the results from groups. The converse of this fallacy, the individualistic fallacy, can also be represented when results of groups are based on the findings of individuals (Babbie, 2005). This study made efforts to avoid the application of the individualistic fallacy because it relied on individuals. This study could have fallen victim to individualistic fallacy if the responses of each group member were used to characterize each group they represented. Instead, the focus is on reverse money laundering, as a concept, not how each group should approach reverse money laundering.

The other hazard that can appear when addressing units of analysis is reductionism. Reductionism represents “an overly strict limitation on the kinds of concepts and variables to be considered” when applying the results of the research (Babbie, 2005). This can limit the reliability of the results. For example, a study may only focus on economic factors or may only focus on one field of expertise, thus focusing the variables around one area (Babbie, 2005). By interviewing current members of the public sector, consultants, bank officers, and technology experts, this study avoided reductionism by sampling interview subjects from different perspectives and thus considered different variables.

Procedure

A sampling frame is a list “of elements from which a probability sample is selected” (Babbie, 2005). Therefore, it is important to select the appropriate members for

the sample frame. In the case of this study on reverse money laundering, the sample frame consisted of members who made up the anti-money laundering community. This is a very large and diverse community but because of their knowledge of money laundering techniques and the anti-money laundering methodologies used to detect and prevent it, the individuals selected to participate in this study represented an appropriate sample for this particular study.

The sampling was conducted via telephone interviews whereby the interview subjects were asked a series of open-ended questions identified in Appendix A. These questions were meant to serve as the control in each interview scenario. The different backgrounds and perspectives associated with each interview subject lead to different answers, but the goal was to see if there was a consensus on the importance of intelligence in detecting and preventing reverse money laundering. While a list of questions was developed for this process, one of the advantages of conducting interviews was that it allowed for some flexibility when gathering research. For example, the interview subject may have answered a pre-determined question but in the process, the response may have lead to another interesting and relevant topic that may not have been addressed by the pre-determined questions. These types of responses were an added benefit to conducting interviews and were considered a valuable part of the data gathering process related to this complex issue.

The sample size for this research project was based on interviews of twelve individuals. Based on the specific nature of the topic, the sample procedure of

conducting interviews and the level of detail in the required responses, this was an appropriate number of subjects considering the logistical aspects of coordinating the interviews and time required to analyze the interview responses.

The type of data that was collected resulted from asking questions of the interview subjects. These questions were designed to capture the knowledge and expertise of the interview subjects that they had developed from their years of experience in this particular field. This method shared a characteristic common with many criminal justice research projects in that it focused on a small number of specialized research subjects (Babbie, 2005).

The data was collected through the technique of conducting telephone interviews. Based on the geographical locations of the selected subject matter experts and given the time and budgetary constraints placed upon this study, it was impractical to conduct face-to-face interviews with each subject. Additionally, given the complex nature of the subject and in depth responses required of the questions, an interview scenario seemed most appropriate (Babbie, 2005).

With the exception of three interview questions, the focus of the interview did not involve the gathering of numerical data. As a result, there was little quantification of the responses. Instead, the study relied on qualitative analysis of the responses provided by the interview subjects. The interview subjects were asked to opine on a specific number of questions. These responses were compared to the responses of the other interview

subjects. Based on the analysis and comparison of the responses, conclusions were made as they related to the hypothesis of the study. There were three questions that asked the interview subject to rank his responses in order of importance. To help with the analysis of these responses, each answer was given a numeric value, the lower the value the more importance the interview subject placed on the answer choice. These collective values were totaled for each answer choice, which helped identify trends and a consensus reached by the interview subjects.

Data Collection

Data was collected from single separate telephone interviews with each of the 12 subject matter experts. These experts included three each from the perspective of the public sector, from the perspective of a compliance officer at a financial institution (as defined by the Bank Secrecy Act and amended by the USA PATRIOT Act), from the perspective of a consultant, and from the perspective of a technology expert. The interviews lasted between 45 and 120 minutes and covered the questions listed in Appendix A.

The interview subjects have invaluable experience in the field of anti-money laundering. Of the three interview subjects from the public sector, one has 27 years of law enforcement experience and is currently serving in the United States Immigration and Customs Enforcement focusing on terrorist financing (Public Sector 1), another has served for the last eight years as a trial attorney in the United States Department of Justice's Counterterrorism section (Public Sector 2) and the third is a New York State

trooper who for the last four and a half years has served in the El Dorado High Intensity Financial Crime Area conducting investigations into money laundering and terrorist financing (Publics Sector 3).

The three interview subjects representing a compliance program from financial institutions have focused much of their careers on financial crimes, including money laundering. One of the interview subjects has over 26 years of experience working with financial crimes including six years helping to establish anti-money laundering policies and procedures at one of the largest banks in the United Kingdom (Compliance 1). Another of the interview subjects has over 25 years experience working in financial institutions, including serving as the Global Head of Compliance and Chief Compliance Officer for a large German bank. Additionally, this interview subject has had the opportunity to work with a software company during its development of an automated transaction monitoring platform (Compliance 2). The third interview subject from this category has almost 10 years of experience working in the anti-money laundering area and currently works for a large insurance company in the United States where he helped start the anti-money laundering compliance department (Compliance 3).

The three interview subjects from the consulting sector all specialize in money laundering and terrorist financing. One of the interview subjects has been a consultant for almost three years but before that he was the Chief of Terrorist Financing Operations Section with the Federal Bureau of Investigations where he served for 28 years (Consultant 1). Another interview subject is a consultant with over 15 years experience

serving as a money laundering investigator, compliance officer and counter-terrorist/counter-narcotics consultant where he advises governments, international bodies, regulatory agencies, and financial intuitions on a global basis (Consultant 2). The third interview subject has over eight years experience working with a “Big Four” accounting firm where his consulting primarily focuses on work related to Bank Secrecy Act, USA PATRIOT Act and anti-money laundering related statutes. He also has experience working in the Internal Revenue Service criminal instigation division where he worked on cases related to money laundering and tax evasion (Consultant 3).

The combined years of anti-money laundering experience from the representatives from the technology sector may not be as deep as the representatives from the other fields but that is because the technology field related to anti-money laundering and terrorist financing is relatively young. However, that does not mean that their input or opinions are any less valuable. One of the interview subjects started his career in the database industry and has worked with startup companies since 1988. He has been with his current company, one that specializes in automated anti-money laundering transaction monitoring software, for three and a half years where he is now in charge of business development (Technology 1). Another representative from the technology sector started working with a well-known international automated anti-money laundering transaction monitoring company in 2003 where he serves as the company’s Chief Executive Officer. Since joining the company, he has become a Certified Anti-Money Laundering Specialist (Technology 2). The third representative from the technology sector (Technology 3) has quite a bit more experience working in the financial sector, having done so for over 25

years. He currently serves as a senior manager for enterprise risk management at a large regional financial institution. Prior to that, for four years he served as a business consultant where he helped develop credit card and identity fraud detection technology.

Findings

The findings from the results of the interviews are provided in the order of each question outlined in Appendix A.

Question #1 - Are you familiar with the term “Reverse Money Laundering?”

All but three of the interview subjects were familiar with the term “reverse money laundering.” Public Sector 1, Compliance 1 and Technology 1 had not heard the term reverse money laundering. After providing them with the definition, it was clear each understood the theme surrounding reverse money laundering, if not the actual term itself. Technology 1 equated reverse money laundering with terrorist financing.

Of the nine that had heard the term reverse money laundering, all explained it as using money obtained from legitimate means for illegal or illegitimate purposes. Technology 3 had heard of the term reverse money laundering and indicated he thought it should be called terrorist financing. He also stated he did not see a distinction between terrorist financing and reverse money laundering.

Question #2 - What industries are particularly susceptible to reverse money laundering and why?

Without a doubt, when asked which industry was most vulnerable, the industry representing charitable organizations was the most common response. Each interview

subject from the public sector and consultant categories, Compliance 1, Compliance 3, and Technology 2 all cited charities because of systemic vulnerabilities such as a lack of oversight and transparency, the ease in which money can be raised and the fact that the donors are often not aware of where the money is going. Consultant 1, Consultant 2, Technology 1 and Technology 3 also identified money remitters, such as money services businesses, because of the ease in which money can be moved, and their cultural and ethnic ties. Consultant 1, Compliance 1 and Technology 1 also identified cash intensive businesses such as restaurants, jewelry stores and travel agencies because dealing in cash is common, and the income from these businesses fluctuates. This fluctuation may be considered unusual for some industries but it would be considered normal for these industries, thus making detection of unusual activity difficult.

Additionally, Public Sector 3 stated that reverse money laundering probably would not impact major corporations. Consultant 3 offered a different opinion and stated that any company that matched charitable donations made by its employees would be vulnerable because it may be unwittingly contributing to a charity that is a front for terrorist financing.

Question #3 - If reverse money laundering can be broken down into two components, the raising of the funds and the disbursement of the funds, which presents more of a problem to detect and why?

The responses to this question were evenly diverse. Four subjects said raising the money was more of a problem, four subjects said distributing the money was more of a problem and four subjects said they presented an equal problem. Compliance 2, Compliance 3, Public Sector 3 and Technology 3 responded that raising the funds presented more of a problem due to the fact that they felt raising money was easy because charities can serve as fronts and siphon off donations with or without the donor's knowledge. Technology 3 added that it is more difficult to track how funds are raised because that happens outside the financial system but once funds enter the financial system, they can be monitored.

Technology 1, Technology 2, Compliance 2 and Public Sector 1 stated distribution presented more of a problem because it is so difficult to track the funds once they leave a financial institution. Compliance 2 also indicated that it was easier to identify the source of the money, mostly because of the customer identification programs now required by financial institutions.

Question #4 - What is the best way to enforce the regulation surrounding Money Services Businesses and why?

When the interview subjects were asked to rank the choices of increasing fines for violators, reducing the registration requirements, and increasing the number of investigations to detect violators, there seemed to be an agreement that an increase in the number of investigations was an important start. While Consultant 1, Consultant 2,

Compliance 1, Technology 1 and Public Sector 1 stated that they would choose more investigations as the best way to enforce Money Services Businesses (MSB) regulation and registration, several subjects indicated they would choose an approach other than one of the three choices provided. One such suggestion from Public Sector 1 was to first reach out to the MSB community to make sure they knew the laws requiring registration. Another suggestion from Technology 3 was to provide positive incentives for financial institutions to turn in those that do not register. Reducing the registration requirements was the first choice of Technology 2 and Compliance 3, and Public Sector 1 saw increasing fines as the best approach.

Public Sector 1, Public Sector 2, Technology 2, Technology 3, and Consultant 1 indicated that increasing the number of investigations would be their second choice, and Compliance 2, Compliance 3, Technology 1 and Technology 3 stated that increasing fines would be their second choice. Reducing the registration requirements was seen as the second choice by Consultant 2, but was seen as the last choice by Public Sector 1, Public Sector 2, Technology 1, Technology 3, and Consultant 1.

Consultant 1 indicated he would start with targeted investigations that ended in an organized “take down” of these unregistered entities followed either by fines for failure to comply, or reducing registration requirements. He further indicated that this would be a short-term approach because someone would move in to take the place of those that had been put out of business. He indicated that a long-term approach would require a

marketing campaign to publicize the results of these take downs, which would serve to increase the awareness of registration, and let the fines act as a deterrent.

Technology 1 chose investigations as his first choice because he felt they would improve the ability to detect patterns in distribution points for the money. As suggested by Consultant 1, Technology 1 also suggested utilizing a marketing campaign or publicity to increase awareness of the regulations, and serve as a deterrent for other potential violators.

One sentiment shared by Compliance 2, Compliance 3, Consultant 1, Consultant 3, and Public Sector 2 was the fact that no amount of regulation, reduced registration requirements, or fines for violations would get those money remitters knowingly involved in terrorist financing or reverse money laundering to register because this is the kind of activity that is going to remain underground no matter what.

Below is a table that helps provide a visual summary of the responses collected for this question.

Figure 1. Summary of Responses: Question #4

Answer Choice	Question # 4 - Selected Answers				Other Description
	Increase Fines	Reduce Registration Requirements	More Investigations	Other	
Interview Subject					
Compliance 1	2	3	1	4	
Compliance 2	4	4	4	1	Require every transaction have identification information appended to it.
Compliance 3	2	1	3	4	
Consultant 1	3	3	2	1	Proactive strategy of all these choices but start with investigations to target specific underground businesses.
Consultant 2	3	2	1	2	Better international regulation.
Consultant 3	4	4	1	4	Does not think addressing MSBs the way we understand them is the way to address terrorist financing. Choices A and B are moot because those that conduct terrorist financing do so underground and no fine, no matter how steep, will bring them above ground.
Public Sector 1	3	4	2	1	Outreach - Regulators and FinCEN should make sure MSBs understand the law and encourage them to register.
Public Sector 2	1	3	2	4	
Public Sector 3	4	3	1	2	Monitoring - Once the MSBs are identified, they need to be monitored to know how they are operating.
Technology 1	2	3	1	4	
Technology 2	3	1	2	4	
Technology 3	2	3	2	1	Provide a positive incentive for MSBs to register and Financial Institutions to turn in those that have not.
Totals	33	34	22	32	

The lower the score the more important the answer choice was rated by the respondent.

One point was assigned if the answer choice was the first choice, two points if it was the second choice, three points if it was the third choice, and four points if it was the last choice or was not chosen at all. Based on this summary, increasing the number of investigations appears to be the most popular choice.

Question # 5 - Who bears the primary responsibility for stopping reverse money laundering?

When asked to rank regulators, financial institutions, vulnerable industries, legislators, law enforcement, or any other sectors, Public Sector 1, Compliance 1 and Consultant 3 indicated that law enforcement was primarily responsible for stopping reverse money laundering. Compliance 3 and Public Sector 3 indicated that financial institutions had the primary responsibility for stopping reverse money laundering. Compliance 2 stated that he thought financial institutions and vulnerable industries shared the primary responsibility because they own the client relationships. He also indicated that outsourced clearing facilities or third party providers working on behalf of financial institutions would be secondary, but still responsible. Technology 1 also indicated that the primary responsibility for stopping reverse money laundering resides with the vulnerable industries. While it may not be clear which sector should take the primary responsibility for stopping reverse money laundering, it appears from the collective responses that financial institutions and vulnerable industries should be the leaders in this effort.

While Technology 2 and Technology 3 considered legislators the highest priority, the consensus was that legislators and regulators have a lower level of responsibility. Law enforcement fluctuated across all sectors between having greater and lesser responsibility.

Consultant 1, Consultant 2 and Public Sector 2 indicated all of the different sectors shared a role in stopping reverse money laundering and Consultant 1 added that in his opinion, the key was cooperation between them all.

Figure 2. Summary of Responses: Question #5

Answer Choice	Question # 5 - Selected Answers						Other Description
	Regulators	Financial Institutions	Vulnerable Industries	Legislators	Law Enforcement	Other	
Interview Subject							
Compliance 1	4	2	3	5	1	6	
Compliance 2	3	1	1	5	4	2	Outsourced clearing facilities.
Compliance 3	5	1	2	3	4	6	
Consultant 1	0	0	0	0	0	0	
Consultant 2	0	0	0	0	0	0	
Consultant 3	5	3	2	4	1	6	
Public Sector 1	3	4	2	5	1	6	
Public Sector 2	0	0	0	0	0	0	
Public Sector 3	2	1	4	5	3	6	
Technology 1	3	2	1	4	5	6	
Technology 2	3	4	2	1	3	6	
Technology 3	2	3	4	1	5	6	
Totals	30	21	21	33	27	50	

The lower the score the more important the answer choice was rated by the respondent. No points were assigned if the interview subject indicated all sectors were equally important or was disinclined to consider the responsibility of one sector greater than any other. One point was assigned if it was the respondent's first choice, two points if it was the second choice, three points if it was the third choice, four points if it was the fourth choice, five points if it was the fifth choice, and six points if it was the last choice or was not chosen at all. Based on the summary of results, it appears that it is the opinion of the interview subjects that financial institutions and vulnerable industries should share the primary responsibility for stopping reverse money laundering.

Question # 6 - Are the current methodologies used to detect money laundering, such as manual and automated transaction monitoring, sufficient to detect reverse money laundering?

This is the first answer in which there seems to be a majority opinion among all of the respondents. The three compliance officers were the only ones that thought current methodologies used to detect money laundering are sufficient to detect reverse money laundering while all the other interview subjects indicated current money laundering detection methodologies are insufficient.

The common response from those that thought the current methodologies are insufficient included the fact that the amounts of the transactions associated with reverse money laundering are usually much smaller than those transactions typically identified with traditional money laundering. Additionally, there is little to distinguish these transactions from normal transactions, and most transaction monitoring is designed to detect the proceeds of crime. Consultant 3 and Technology 1 stated that many of the transactions associated with reverse money laundering take place outside of financial institutions or traditional financial systems, so current money laundering methodologies would never even get the opportunity to detect such activity. Technology 2 also indicated that the current methodologies used to detect money laundering are limited in scope, stating that even if a financial institution had a robust transaction monitoring system in place, it would not be able to trace the money once it left its system. As a result, the institution would never get a complete picture of the entire financial transaction.

One sentiment shared by Compliance 2, Compliance 3 and Technology 3 was the importance of pattern recognition in attempting to help identify the types of transactions

or products used by those that carry out reverse money laundering. Compliance 3 acknowledged that the transaction profiles for reverse money laundering are different but the framework to build such profiles exists and a different approach needs to be adapted.

As an enhancement to the current transaction monitoring methodologies already viewed as sufficient, Compliance 2 indicated that link analysis would be an important additional step in an attempt to identify relationships between transacting parties. He stressed the importance of quality customer information required to make this work. Consultant 3 also indicated that knowing your customers is critical to conducting the appropriate level of due diligence.

Question # 7 - How should the current methodologies change to better adapt?

The answers to this question were quite varied, but some of the same themes that were apparent in the previous responses were again present. Consultant 1, Consultant 2, Technology 1 and Technology 3 indicated that the use of customer profiles or patterns can help identify certain circumstances of reverse money laundering that were previously undetected. Consultant 1 and Consultant 3 also indicated the use of customer information should be better utilized by further incorporating it into the transaction monitoring process. They both view customer due diligence as a vulnerability for terrorists, stressing that the more a financial institution knows about its customers the better position it will be in to detect a potential terrorist financing operation through due diligence or identify unusual activity through transaction monitoring. Public Sector 3 was not sure these

current methodologies could be better adapted because much of this activity takes place in the underground banking and money remittance environment outside the structured financial industries sector.

Compliance 1, Compliance 3 and Consultant 1 indicated the need for better communication between those that have intelligence and those that can benefit from it. Consultant 1 suggested adopting working groups between representatives from the various regulatory agencies, financial services sector, law enforcement, and those that specialize in anti-money laundering technology to enhance the knowledge sharing among those that deal with this issues on a regular basis. Consultant 1 also indicated he would like to see an increase in the amount of human intelligence, a view shared by Public Sector 1. Compliance 1 and Compliance 3 suggested improving the flow of information from law enforcement to the financial institutions, and stated that this would help financial institutions better tailor their resources to focus on certain areas of interest or possible reverse money laundering activity.

Technology 2 suggested having bank examiners from the various regulatory agencies, such as the Office of the Comptroller of the Currency or the Board of Governors of the Federal Reserve System, use the same kind of tools the financial institutions use so they can get a more complete picture of how the money moves across several financial institutions rather than at just one institution. Compliance 2 indicated the need for an increased shift to focus on risk by product, not necessarily by customer.

Consultant 2 also indicated that those involved in monitoring financial activity would benefit from increased training and improved awareness of the differences between traditional money laundering and reverse money laundering. With better training, reverse money laundering can be more readily recognized when current anti-money laundering methodologies do identify anomalous or unusual activity.

Question # 8 - What is more effective for identifying reverse money laundering, transaction monitoring or scanning for entities known to be associated with reverse money laundering?

It is important to note that each interview participant was asked to choose between transaction monitoring and scanning but half of the subjects still elected to choose using a combination of both techniques rather than choose one over the other. All three interview subjects from the technology sector indicated that both transaction monitoring and list scanning must be performed in tandem. Public Sector 2, Public Sector 3 and Compliance 1 shared this opinion. All three of the technology representatives agreed that these techniques needed to be used in conjunction with some type of additional analytical tool such as link analysis, data mining or profiling to determine patterns and links related to historical activity that may lead to the identification of previously undetected activity. Technology 1 also focused on the importance of knowing your customer, stating that scanning would be required at the start of the relationship but if the customer is not on any watch lists, then monitoring the

customer's activity becomes very important to keep track of who the customer is doing business with.

Consultant 2, Consultant 3, Compliance 3 and Public Sector 1 indicated that scanning is the best option. Restricting his comments to the perspective of the formal banking system, Consultant 3 stated that it is faster and perhaps more efficient than transaction monitoring because he thought not enough information is gathered on new customers to make transaction monitoring immediately effective. Consultant 2 indicated that scanning was more effective because it is very difficult to identify reverse money laundering through transaction monitoring. Compliance 3 indicated that scanning would be easiest because most companies already conduct scanning for OFAC so adding a list of known reverse money laundering offenders would be easy to implement. Public Sector 1 based his answer on his belief that the proper intelligence would be provided to those doing the scanning so they could target those they felt were the greatest risk.

Compliance 2 and Consultant 1 both thought transaction monitoring was clearly the better option. Compliance 2 even thought scanning was useless because the lists are public and anyone on that list would use other people or entities absent from these lists. Consultant 1 echoed that sentiment and added that anyone on these public lists would figure out a way to get around that fact through other means. He also indicated that in addition to this, transaction monitoring is proactive so it offers the better chance of sustained success through enhanced profiling and trying to get out in front of emerging trends.

It should be noted that Compliance 3 and Consultant 3 thought that transaction monitoring would be better than list scanning if transaction monitoring was improved or if the government provided greater assistance such as identifying clear cases around which to build rules. However, based on the current environment, they felt scanning was the best option at this time.

The same consultant and compliance officer further qualified their answer and shared the sentiments expressed by Compliance 2 and Consultant 1 adding that the current lists used for scanning, such as the OFAC list, are public lists, and that anybody involved in a complicated reverse money laundering scheme would be smart enough to know they were on such a list and would have someone else move the money for them or disguise themselves enough to fly below the radar.

Question # 9 - Do government lists of restricted entities such as the one maintained by OFAC or other lists like those identifying Politically Exposed Persons, take on greater importance for preventing and detecting reverse money laundering?

The majority of interview subjects, eight of the twelve, indicated that the use of restricted entity lists do take on greater importance in preventing and detecting reverse money laundering. All three interview subjects from the public sector, as well as Technology 1, Technology 3 Consultant 2, Consultant 3, and Compliance 3 responded

yes leaving Compliance 1, Compliance 2, Consultant 1, and Technology 2 believing these lists do not.

Of the eight that responded yes, there were differing opinions of usefulness. Consultant 2 said these lists were useful because they are the easiest to use and that other means of detection have not proved useful as of yet. Consultant 3 indicated that these lists were only useful if they came from law enforcement. Technology 1 shared this sentiment indicating that a single comprehensive list compiled by a multi-national, multi-agency effort would be most useful. Technology 1 thought these lists could be useful in link analysis.

Compliance 3 and Public Sector 2 thought these lists take on more importance because they provide specific targets. Public Sector 1 stated that while these lists are one of the best tools available now, they do not have enough data to make them very useful. His criticism was that the lack of information leads to many false positives.

This was not the only criticism of using such lists. The reason Technology 2, Consultant 1 and Compliance 2 stated such lists do not take on any greater importance was because of the public nature of these lists. As expressed in responses to the previous question, they believe that anyone participating in a reverse money laundering scheme, particularly one related to terrorist financing, would be smart enough to know if they were on one of these lists and would use sufficient techniques to disguise their involvement. Additionally, Compliance 1 added that the outcome of the positive matches

to these lists reported to the appropriate agencies are not getting communicated back to those that are conducting the searches. As a result, those conducting the search do not know if their results are worthwhile.

Question # 10 - What improvements can be made to enhance the information on these lists?

When asked what improvements can be made to these lists, the most common answer by far, as expressed by nine of the interview subjects, was to increase the amount of identifying information provided on these lists. Each of the compliance officers and technology experts as well as Consultant 2, Consultant 3 and Public Sector 1 expressed this view. Many noted that identification of false positives was a problem due to the lack of identifying information provided for the entities on these lists. Technology 1 suggested adding financial information or information shared between national taxation authorities. He suggested this could enhance the customer due diligence by providing the ability to profile such entities by placing them into peer groups. Compliance 3 acknowledged that the identifying information provided on these lists is often limited by the amount of information known by the groups that publish the lists, but suggested that even adding such information as where a person is from, with whom they have been known to do business or whom they have had some connection with would improve the matching and link analysis capabilities.

An additional recommendation from Public Sector 3 included increasing the scanning capability to account for the different common spellings of names, particularly Arabic names, although most screening tools incorporate this already. Public Sector 2 recommended increasing the communication effort between public agencies and private sector entities using these lists. Compliance 2 suggested centralizing the list and using resources such as INTERPOL.

Consultant 3 indicated he thought lists like the OFAC list and requests authorized by Section 314(a) of the USA PATRIOT Act, where FinCEN can request financial institutions search their records for specific entities, were sufficient but stated that lists such as PEP lists are too voluminous and needed to be cut down to focus on high-risk PEPs. Consultant 1 did not think much more could be done to improve these lists because he stressed again the entities on these lists are not the ones that would be perpetrating the reverse money laundering schemes.

Question # 11 - How can these lists be better utilized?

There were quite a few recommendations made by the interview subjects. Technology 1 and Public Sector 3 suggested consolidating or standardizing these lists. Consultant 3 and Compliance 1 each suggested making the lists more focused, stressing bigger is not necessarily better. All three compliance officers suggested improving communication and feedback between those that use the lists and those that generate the lists.

Technology 3 suggested using the lists to determine if any relationships exist between current customers and any entities on these lists. Technology 2 suggested keeping the lists private because he believes the people who are on these lists know they are on these lists and will make sure to stay below the radar. Public Sector 1 took the opposite approach suggesting these lists should be widely available and to make sure other countries are using them as well.

Consultant 2 and Consultant 3 suggested that updates to these lists or lists that are periodically released, such as 314(a) requests, needed to be treated with a greater sense of urgency and checked more often. Consultant 1 thought the lists were already being well utilized by compliance professionals at financial institutions.

Public Sector 3 again suggested incorporating the use of more advanced technology when scanning for names on the lists to account for the different ways names are spelled or variations of the same name in different languages such as Michael and Miguel. Another suggestion made by Public Sector 2 was to provide a better explanation of how to use the lists, particularly the varying sanctions programs surrounding countries targeted by OFAC.

Question # 12 - What obstacles may prevent the implementation of these improvements?

The most common obstacles mentioned by the interview subjects included privacy issues and bureaucracy or politics. Compliance 1, Compliance 2, Consultant 1, Consultant 2, and Public Sector 2 believed that privacy issues would restrict the amount of quality identifying information required to make these lists more useful. Consultant 2 and Compliance 2 specified that certain countries are very protective of this type of data and would be unwilling to share such information.

These last two responses were a hybrid approach covering both privacy and political issues. Two public sector interview subjects also expressed concerns over political limitations, Public Sector 1 from an international perspective and Public Sector 3 from a domestic point of view. Public Sector 1 focused on diplomacy, figuring it would be difficult to continue to pressure foreign countries to follow policy dictated by the United States. Public Sector 3 indicated there might be a turf war or infighting over which United States government agency would be in charge of the list. This view of who would manage the list was also an obstacle seen by Technology 3.

Also among the responses were obstacles common to the implementation of any change, such as resources, money and time. Consultant 1, Consultant 3 and Compliance 3 indicated that the failure to secure the right resources, such as personnel and technology, would hinder the implementation of any change. Linked to these two issues is money, which was identified as an obstacle by Consultant 1, Consultant 3 and Public Sector 3. Consultant 3 also indicated that not having enough time to make any changes

and implement them correctly could also prevent the application of any of these implementations.

Another obstacle seen by both Technology 2 and Public Sector 1 was the lack of an international agreement on money laundering as a crime, and the differing views on the need and extent of anti-money laundering requirements. Each thought it would be very difficult to get an international consensus on the criminalization of money laundering and terrorist financing, especially when in some countries, organizations like Hezbollah are considered political organizations, not terrorist organizations.

Technology 1 viewed poor data collection of customer information as a hindrance to any implementation of improved matching because a lack of quality data would make comparison and analysis of potential matches difficult. Public Sector 2 also noted a connection to customer information indicating that additional responsibilities are being placed on charities to know their donors and know what the money is being used for, but that this was being met with resistance by the charitable organizations.

Compliance 3 indicated that any improvements would be vulnerable to a lackadaisical compliance program. He suggested that sometimes, no matter what improvements are made, some programs are always going to be focused around doing the minimal amount of work to ensure compliance with rules and regulations. Unless the law mandates any changes, compliance programs such as these will never be willing to make any improvements.

Consultant 1 also indicated that any improvements to these lists would do little to address the issue of reverse money laundering reiterating that the people on these lists are usually never the ones on the front line of any reverse money laundering scheme. If any of these people were orchestrating a reverse money laundering scheme, they would most likely know they were on these lists, and would conceal their true identity.

Question # 13 - What is the most important area of focus required to enhance the detection of reverse money laundering?

When the interview subjects were asked to rank in order of importance intelligence (including law enforcement), legislation, information sharing, technology, or any other area where efforts should be focused to enhance the detection of reverse money laundering, the majority of responses indicated that information sharing and intelligence were most important, while legislation seemed to be considered least important. As a note, all three public sector interview subjects came up with the same rankings.

All three interview subjects from the public sector, Consultant 2, Consultant 3 and Compliance 1, considered intelligence most important. The common thread among these responses was “you have to know what it is you are looking for.” Public Sector 1 stressed the importance of having a target because the money associated with reverse money laundering looks legitimate. It would be impractical to review every paycheck, charitable contribution or business transaction. These same interview subjects ranked

information sharing as second most important citing “you cannot share what you do not have.” The interview subjects all identified the importance of sharing information, but indicated that intelligence must first be gathered before it can be shared. Consultant 3 and Public Sector 1 both suggested that vital intelligence would come from local law enforcement, both domestically and internationally, and that it must be communicated globally. They noted that most terrorist activities are planned in one country but carried out in another.

Compliance 1, Public Sector 1 and Public Sector 3 viewed intelligence and information sharing almost as equally important, considering them a “1 and 1a” type relationship. Consultant 1 considered all answer choices related, but indicated that legislation and technology were more effective with intelligence and information sharing than they were by themselves. He also believed that there is a deficiency in training, both in the public and private sectors, because most training is focused on traditional money laundering, and neglects to provide adequate coverage of terrorist financing and reverse money laundering. Therefore, he considered improved training another area of focus but pointed out that it was also driven by intelligence and information sharing.

Information sharing was considered most important by Compliance 3 and all three interview subjects from the technology sector. The three representatives from the technology sector all identified the importance of sharing information to improve either the ability of identifying potential patterns of reverse money laundering or to assist with

link analysis by preventing the money trail from ending once it leaves a financial institution.

Technology 1 and Technology 2 considered intelligence the least important area of focus and Technology 3 stated intelligence was next to last in order of importance. It appeared as if the technology sector placed a greater importance on establishing a proper protocol for processing the gathered intelligence rather than on the intelligence itself. Technology 1 stated that if a correct customer identification framework is built, it actually makes intelligence less important because it stands a better chance of preventing those that conduct reverse money laundering from ever entering a financial institution. However, doing a good job of identifying your customers was a point stressed in previous answers by each technology representative, and this cannot be accomplished without quality intelligence, so there seems to be a bit of a contradiction between these answers and previous answers provided by the technology representatives. Excluding for a moment the responses from the technology sector, all the other interview subjects saw intelligence as either the primary or secondary area of focus.

Compliance 2 indicated that the most important area of focus should revolve around improving the data flow of information that is collected and used in the reverse money laundering detection process. He indicated that the data must be properly transformed into information that can be properly used and beneficial to those with the appropriate knowledge base, which then becomes intelligence used by those investigating situations of potential reverse money laundering. He stressed that the process related to

the collection, distribution, and use of data is vital to the detection of reverse money laundering and noted that quality data is no better than poor data if it is not properly utilized.

Compliance 2 added that after ensuring an appropriate data flow process, intelligence would be the next most important area of focus because for the data flow process to work, you need the data. Compliance 3 stated intelligence was the second most important area of focus because after sharing current information, new information needs to be gathered to update and enhance what has already been shared.

Technology 2 and Technology 3 both selected technology as the second most important area of focus based on the fact that to support the amount and the complexity of the information being shared, a sophisticated technology infrastructure would be required. All three members of the public sector, Compliance 1, Compliance 2, Consultant 2, and Technology 1 saw technology as the third most important area of focus. These interview subjects also indicated that advanced technology would increase the usefulness of information and increase the ability to analyze such massive amounts of data. Public Sector 2 specifically indicated technology would assist with data mining when looking for specific identifiers, citing as an example the scan of a database containing drivers with a license to transport hazardous materials.

Legislation appeared to be the response requiring the least amount of focus, ranking as the last choice by all three members of the public sector, Compliance 1,

Compliance 2, Consultant 2, and Technology 3. Legislation was seen as the second to last area of focus by Compliance 3, Technology 2 and Consultant 3. The reason behind many of these responses, particularly among all three interview subjects from the public sector, appears to be the idea that currently there is enough legislation surrounding money laundering and terrorist financing. Technology 3 and Compliance 2 indicated that legislation was least important because it ends up being watered down. Compliance 2 added that any additional legislation would be “useless” and that reputation risk is more of a deterrent than the threat of breaking the law. He added that self-policing would be more valuable because a financial institution’s need to protect its reputation and avoid any negative publicity would accomplish more than any new laws could. Based on these responses, it appears that when it comes to legislation, many group reverse money laundering with traditional money laundering because currently, there is no legislation specifically geared toward reverse money laundering.

Below is a table that helps provide a visual summary of the responses collected for this question.

Figure 3. Summary of Responses: Question #13

Question # 13 - Selected Answers						
	Intelligence	Legislation	Information Sharing	Technology	Other	Other Description
Interview Subject						
Compliance 1	1	4	2	3	5	
Compliance 2	2	5	4	3	1	Improved data flow.
Compliance 3	2	3	1	4	5	
Consultant 1	1	2	1	2	2	Improved training.
Consultant 2	1	4	2	3	5	
Consultant 3	1	3	2	4	5	
Public Sector 1	1	4	2	3	5	
Public Sector 2	1	4	2	3	5	
Public Sector 3	1	4	2	3	5	
Technology 1	4	2	1	3	5	
Technology 2	4	3	1	2	5	
Technology 3	3	4	1	2	5	
Totals	22	42	21	35	53	

The lower the score the more important it was seen by the respondent. One point was assigned if the answer choice was the respondent's first choice, two points if it was the second choice, three points if it was the third choice, four points if it was the fourth choice, and five points if it was last choice or it was not chosen at all, for example, if an interview subject did not provide a response other than the four suggested.

Conclusions

The goal of this study was to determine if there was a consensus of where our efforts should be focused to best combat reverse money laundering. The hypothesis of this study was that the focus should be on intelligence. Based on the responses from the interview subjects, it would indicate that there is a high degree of agreement, and that the level of agreement partially supports the hypothesis. While intelligence is seen as a priority, the overall responses from the interview subjects indicate that information sharing should be considered a slightly greater priority. The final interview question serves to provide a direct response to the heart of this study, and the responses to the other questions serve to support the answers provided in the final question. While nine of the interview subjects considered intelligence either the first or second most important area of focus, 11 interview subjects considered information sharing just as important, with Compliance 2 the only outlier. Seven of the twelve interview subjects considered intelligence the most important area of focus compared to five interview subjects who considered information sharing the most important area of focus. Two others considered intelligence the second most important area of focus. While six interview subjects considered information sharing the second most important area of focus, it is noteworthy that each of these also considered intelligence as the most important area of focus. The three interview subjects from the technology sector considered information sharing the most important area of focus with intelligence recognized as the least important by two of these subjects and next to last important by the third. Considering the results as a whole, it appears that information sharing is recognized as being very important and additional research should be conducted to better determine why and how its role could improve the

detection and prevention of reverse money laundering. Perhaps there is a level of distrust between those that possess the information and those that do not. Perhaps a level of bureaucracy still exists that prevents information from being shared, something the USA PATRIOT Act was meant to remedy.

While the final question attempts to provide a direct response to the ultimate goal of this study, the answers to the other questions help substantiate the reasoning and support for this finding. After reviewing the answers to the other questions, there are several themes that become apparent. These themes include:

- Cooperation and coordination between all the parties involved in detecting and preventing reverse money laundering needs to improve;
- Watch lists in their current form are not utilized properly;
- Knowing your customer is vital;
- Current methodologies are insufficient for detecting reverse money laundering; and
- Reverse money laundering frequently occurs outside the formal financial sector.

When examined separately, these themes look unrelated but there is an important element that is present in all of these, which is that each relies on the two most important areas of focus identified by this study; the use of intelligence and the sharing of information.

Importance of increased cooperation and communication

The importance of increased cooperation and communication among those involved in preventing and detecting money laundering and terrorist financing, of which

reverse money laundering is a part, was not expected to be as heightened as it turned out to be, but given the importance placed on intelligence this finding seems logical.

Excluding the final question, the theme of information sharing is one that was identified in the answers to other questions by ten of the twelve interview subjects, an issue identified more deliberately than intelligence. This would seem to support the finding of the final question. While it appears a majority has been reached as to the importance of information sharing in detecting reverse money laundering, information sharing still hinges on possessing intelligence with which to share. It also relies on continually distributing new intelligence so those using the information are not relying on stale or outdated intelligence. However, it is important to recognize that the greatest intelligence is useless unless it is in the hands of those that need it most.

Based on the responses of interview subjects, there appears to be a need for a balanced flow of information, particularly between financial institutions, their regulators and law enforcement. Additionally, five interview subjects viewed confidentiality issues as a major concern for sharing information on a global level. Because there are numerous information security requirements for different countries and government agencies, a completely transparent exchange of information may be unrealistic. However, perhaps a list or group of lists, controlled by an international agency such as INTERPOL, could serve as a foundation for this sharing of information between countries with each member country having its own agency responsible for its use and security within its respective country.

Such an exchange or even the compilation of such data is a major obstacle facing those trying to compile similar lists to combat other global issues such as identity theft. Some have suggested compiling a universal consumer index or database with which to verify consumer information when applying for such items as credit cards or loans. This has been met with resistance due to privacy concerns and would be extremely difficult to compile given the sheer number of consumers globally. However, the concerns related to such a database of consumers is much different than a database related to reverse money launderers. The population of those linked to reverse money laundering is so much smaller than the population of consumers. Additionally, many such entities may already be known to law enforcement so such a database would be easier to compile. Because the database would be smaller, it would be much easier to keep current and secure. Additionally, all member countries would be subject to periodic audits to ensure access to the database was being properly restricted, used and secured. Then the countries would be responsible for overseeing and governing its distribution to the financial services community. The database could contain intelligence resulting from investigations related to terrorist financing and reverse money laundering and some of the previously recommended techniques, such as link analysis and pattern recognition, could be put into practice on a global scale. However, if any of this was ever to be realized, it would take legislation on a global level, which as the research findings would suggest, is an issue that attaches itself to another theme identified by this study, the fact that watch lists, in their current form, are not utilized properly.

Watch lists in their current form are not utilized properly

While the theory behind the use of watch lists may be important in the fight against money laundering and terrorist financing, it appears these lists are not being used to their fullest potential. As Compliance 2, Consultant 1 and Technology 2 pointed out on several occasions, one of the main problems is that many of these lists are available to the public. As a result, terrorists know they are on these lists and will make sure to disguise their involvement in any financial transaction subject to scrutiny against these lists. Another problem, identified by three quarters of the interview subjects, is that many of these lists lack an appropriate amount of identifying information to make them very useful. Even with these limitations surrounding the use of watch lists, eight interview subjects still thought they take on a greater importance now. This would indicate that these lists would be useful if properly utilized. Enriching these lists with additional identifying information gathered from increased intelligence would be a good start. This would allow for matching against multiple identifiers, rather than just a name, which would help increase the quality of matches, and allow investigators to focus on a greater number of relevant transactions related to positive matches. This preliminary analysis would then produce additional information that could be shared and used to build profiles and patterns for advanced automated transaction monitoring and help identify additional relationships through the use of link analysis.

Another issue surrounding the use of these lists is the concern over confidentiality of the information contained on these lists, something touched on above. Several interview subjects indicated there would be a hesitation by businesses, organizations and countries to share identifying information of their constituents. One way to help reduce

this concern, as suggested by Technology 2, is to make these lists confidential.

Technology 1 and Public Sector 1 also suggested consolidating these lists would make them easier to manage, and list management was a concern of both Public Sector 1 and Technology 3. By consolidating the lists into a manageable number, making them confidential and governing access to them, greater control and protection of the data would be easier to achieve, which might make the sharing of information more likely.

While keeping these lists confidential seems like a good idea, the classification and consolidation of such lists could only be accomplished through legislation or regulation, which as the research findings would suggest, is not considered a high priority by most of the interview subjects. Additionally, as we saw earlier, privacy concerns are thought to be a major obstacle in sharing information with other countries or jurisdictions. If these lists were to become confidential and many of the various lists, such as the ones maintained by OFAC, the Bank of England and the United Nations were consolidated, this would require global legislation, something that is very difficult to accomplish and as the research would suggest, is not a major area of focus.

Knowing your customer is vital

Knowing your customer is a critical component of financial transactions, and half of the interview subjects, with at least one from each sector, indicated it played an important role in the fight against reverse money laundering. Customer information is important on the front end because it helps with the screening process when trying to keep certain entities out of financial institutions. Information such as name, address, date of birth, and an identification number are the most basic pieces of information that can be

used to identify a customer and now certain financial institutions operating in the United States are required to collect these pieces of information prior to opening an account or initiating a transaction. Additional information, while not required, such as source of wealth, type of account, type of business, how the customer intends to use the account, the types of transactions the customer intends to make, and any financial history help financial institutions build profiles to assist with advanced automated transaction monitoring used to identify potential circumstances of suspicious or unusual activity once the customer has gained access to these financial institutions. This is particularly important because, as several of the interview subjects noted, building profiles or identifying patterns is crucial in the effort to detect reverse money laundering. This information is a form of intelligence, but instead of the intelligence being gathered out in the field by law enforcement, the process that typically comes to mind, it is gathered by financial institutions. As a result, the more financial institutions know about their customers the better position they will be in to detect suspicious or unusual activity that may be a sign of reverse money laundering, and the more information that is known about their customers, the more information that can be shared when suspicious activity is reported to law enforcement. The more information available to law enforcement the more effective law enforcement can be in its investigation and analysis.

The principle behind knowing your customer is equally important for vulnerable industries, most notably charities, where knowing the beneficiary of the charitable donations is vital. We have seen that charities often represent the first step in making the funds that are destined for the hands of terrorists appear legitimate. The ability to know

specific details and information about where and to whom charitable contributions are going is crucial because, unlike financial institutions that utilize sophisticated transaction monitoring techniques, the opportunity to identify potentially unscrupulous entities or activity may only present itself when the grantor relationship is established.

Additionally, as Consultant 3 noted, businesses that make matching contributions on behalf of employees are also vulnerable to such activity. Therefore, charities, and companies that make such matching charitable contributions, should be required to conduct enhanced due diligence on their beneficiaries before distributing any goods, services or funds. Enhanced due diligence could include verifying the identity of the charity and its board members and determining if it has any links to supporting terrorist organizations.

Based on recent activity, we appear to be heading in this direction. The United States Department of the Treasury recently released for comment, revised voluntary best practices for charities in an effort to combat terrorist financing. This guidance makes recommendations such as vetting senior members of charitable organizations and maintaining sufficient auditing controls to track the distribution of services and goods (United States Department of the Treasury, 2005). The guidance also recommends “basic” vetting of recipients through publicly available information sources, such as the Internet, in an attempt to determine if any recipients have been linked to terrorist activity or terrorist financing (United States Department of the Treasury, 2005). These practices are a good start but they must be more than guidance, to achieve universal implementation, they would require legislation, but this has already been proven to

provoke resistance from industry, civil liberties organizations, and often legislators themselves.

Several interview subjects advanced the importance of customer information to include the quality with which this information is gathered and organized, stressing that transaction monitoring conducted by financial institutions is only beneficial when quality data exists. This is particularly important when utilizing advanced automated transaction monitoring systems where any added benefits that come from using a more advanced system can be negated by poor or incomplete data. Many current advanced automated transaction monitoring systems utilize incomplete, inaccurate, or outdated information, which leads to misclassified peer groups or profiles. As a result, the findings of these systems are often misleading or inaccurate because the systems may be inappropriately configured based on these skewed profiles. If financial institutions use advanced automated transaction monitoring systems that utilize customer profiles, they should make sure they have systems in place to gather enough intelligence to accurately capture the true nature of their customer's business and make sure this is reevaluated on a periodic basis. A thorough process would include a reevaluation of the peer groups and profiles for all existing customers, not just new or recent customers. In fact, older customers may represent a greater risk to the accuracy of the automated transaction profiling process because they may be operating in peer groups they have long since outgrown and it is this intelligence that drives much of the automated transaction monitoring process.

Current methodologies are insufficient for detecting reverse money laundering

While this may not be a new revelation, the answers provided by the interview subjects may help provide some direction toward how they should be improved. Seven of the interview subjects specifically identified or touched on the theme of giving greater consideration to recognizing patterns observed in reverse money laundering scenarios. Additionally, four of these interview subjects, Technology 1, Technology 3, Compliance 2, and Compliance 3 indicated that link analysis should be incorporated to help identify non-obvious relationships between those discovered to be conducting reverse money laundering and customers that may be aiding in this process (but have gone previously undetected).

While the ability to detect patterns of activity and make connections between those involved in reverse money laundering requires some type of advanced technology, they both rely on a platform built on intelligence. Without the investigative capability to research and identify such patterns, the technology is no better than what is currently being used, and without investigating reverse money launderers and subsequently generating a profile of them, the link analysis is incomplete.

Law enforcement is already tasked with investigating suspicious activity reported by financial institutions so it would make sense for them to construct a network of reverse money launderers through the use of link analysis. They could benefit from the information reported across the entire financial services community and would not be limited to information contained in a single institution the way a bank would be. The

information required for the link analysis could be enhanced via requests to financial institutions as authorized in Section 314(a) of the USA PATRIOT Act. Additionally, because law enforcement has the greatest pool of known reverse money laundering schemes, law enforcement is also in the best position to develop and subsequently distribute patterns observed from such cases, which would help raise awareness in the financial services sector and enhance the automated transaction monitoring systems already in place.

Reverse money laundering outside of the formal financial sector

Until this point, the themes and recommendations have focused on the formal financial services community. Also, many of the interview subjects seemed to craft their responses around the assumption that the activity was flowing through the formal financial sector. However, as seven of the interview subjects noted, a great deal of reverse money laundering takes place outside of the formal financial sector. Since a good portion of the funds generated by reverse money launderers will never find their way into a financial institution, investigations by law enforcement and the resulting intelligence gathered on these entities becomes even more important. Because the entities and their funds never enter the formal financial sector, the financial institutions never have a chance to identify such activity through customer due diligence or transaction monitoring, which puts the responsibility for detecting and preventing this kind of activity squarely on law enforcement. It would be impossible to expect law enforcement to identify and shut down every informal value transfer service provider, and as we have seen, not every informal value transfer service provider is a conduit for illegal activity.

Therefore, law enforcement should take a risk based approach and identify specific targets associated with reverse money laundering, and the best way to accomplish this is by conducting investigations resulting in quality intelligence identifying those targeted for shut down.

Summary Conclusions

The research findings indicate that focusing on intelligence alone may not be the best approach to detecting and preventing reverse money laundering. Instead, by prioritizing the gathering of intelligence and coupling it with the sharing of this information, any effort to detect reverse money laundering will benefit. The use of advanced technology such as automated transaction monitoring through the development of pattern recognition, profiles and list matching were also seen as important tools in the effort to detect reverse money laundering, but these tools require the proper information to make them successfully work. When examining different techniques used to combat reverse money laundering, it becomes apparent that intelligence and the sharing of the intelligence provide the foundation from which all other detection and prevention methodologies are built.

References

31 C.F.R. §103.121

31 C.F.R § 103.178

31 U.S.C. §1051

Alden, E. (2002, July 2). Banks Attack Terror Money Campaign. *Financial Times*.
From Lexis database.

Babbie, E., & Maxfield, M. (2005). *Research Methods For Criminal Justice and
Criminology*. Belmont: Wadsworth Thomson Learning.

Cassella, S. D. (2003). Reverse Money Laundering. *Journal of Money Laundering
Control*.. Vol. 7. No. 1. p. 92-94.

DeYoung, K., Hilzenrath, D., & O'Harrow Jr., R. (2001, September 21). Bin Laden's
Money Takes Hidden Paths to Agents of Terror. *Washington Post*. From Lexis
database.

*Counterterror Initiatives in the Terror Finance Program: Hearing of the Senate
Banking, Housing, and Urban Affairs Committee, Senate*. 108th Cong., 1st Sess.
(2003) (testimony of John S. Pistole). From Lexis Database.

Elizur, Y., & Malkin, L. (2002, March 22). Terrorism's Money Trail. *World Policy
Journal*, No. 1, Vol. 19, 60. From Lexis database.

Executive Order 13224. (2001, September 23). *Blocking Property and Prohibiting
Transactions with Persons Who Commit, Threaten to Commit, or Support
Terrorism*. Retrieved August 8, 2005 from
<http://www.treas.gov/offices/enforcement/ofac/sanctions/t11ter.pdf>.

Federal Deposit Insurance Corporation. (n.d.). *History of Anti-Money Laundering
Legislation*. Retrieved September 11, 2004 from
http://www.fdic.gov/regulations/examinations/bsa/bsa_3.html.

- Financial Action Task Force on Money Laundering. (n.d.). *More About the FATF and Its Work*. Retrieved September 11, 2004 from http://www1.oecd.org/fatf/AboutFATF_en.htm.
- Financial Action Task Force. (2002). *Report on Money Laundering Typologies 2001-2002*. Retrieved August 31, 2004 from http://www1.oecd.org/fatf/pdf/TY2002_en.pdf.
- Financial Action Task Force. (2003). *Report on Money Laundering Typologies 2002-2003*. Retrieved August 31, 2004 from http://www1.oecd.org/fatf/pdf/TY2003_en.pdf.
- Financial Action Task Force. (2004). *Report on Money Laundering Typologies 2003-2004*. Retrieved August 31, 2004 from http://www1.oecd.org/fatf/pdf/TY2004_en.PDF.
- Financial Crimes Enforcement Network. (2001). *The SAR Activity Review: Trends, Tips & Issues*. Issue 3. Retrieved October 18, 2004 from <http://www.fincen.gov/sarreviewissue3.pdf>.
- Gerth, J. and Miller, J. (2001, October 11). *Trade in Honey is Said to Provide Money and Cover for Bin Laden*. The New York Times. From Lexis Database.
- Goodman, S. (2004, October 15). *AmSouth Fine Signals Tighter Fraud Policing*. Birmingham News. From Lexis Database.
- Kurlanzick, J., Schmitt, C., & Smucker, P. (2001, October 29). *When Charity Goes Awry*. *U.S. News and World Report*.
- Kochan, N. (2003, September 1). *Money-laundering Controls Look All Washed Up*. *Euromoney*. Vol. 34. No. 413. p. 94. From Lexis database.
- National Commission on Terrorist Attacks Upon the United States. (2004). *Monograph on Terrorist Financing*. Washington, D.C. Retrieved August 23, 2004 from http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf.

- Office of Foreign Assets Control. (n.d.) *Frequently Asked Questions*. Retrieved February 20, 2006 from <http://www.ustreas.gov/offices/enforcement/ofac/faq/answer.shtml#1>.
- O'Brien, T. (2004, May 14). *Regulators fine Riggs \$25 Million*. The New York Times. From Lexis Database.
- Passas, N. (2004, September 22). Address. Presentation at "How Money Moves: A Threat Public Security?" Newark, NJ.
- Rubin, C. and Renda-Tanali, I. (2001). *The Terrorist Attacks of September 11, 2001: Immediate Impacts and Their Ramifications for Federal Emergency Management*. Retrieved August 7, 2005 from <http://www.colorado.edu/hazards/qr/qr140/qr140.html>.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law 107-56). 2001.
- United States Department of Commerce Bureau of the Census. (n.d.). *United States Census 2000 Survey*. Retrieved October 14, 2004 from <http://www.census.gov/dmd/www/pdf/d02p.pdf>.
- United States Department of State. (2006). *2006 International Narcotics Control Strategy Report*. Retrieved March 13, 2006 from <http://www.state.gov/p/inl/rls/nrcrpt/2006/>.
- United States Department of the Treasury. (2002). *A Report to Congress in Accordance with Section 359 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*. Retrieved September 7, 2004 from <http://www.fincen.gov/hawalarptfinal11222002.pdf>.
- United States Department of the Treasury. (2005). *U.S. Department of the Treasury Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities*. Retrieved January 5, 2005 from

http://www.moneylaundering.com/subscribers/resources/pdfs4db/Treas_guidelines_charities_120505.pdf.

United States General Accounting Office. (2003a). *Combating Money Laundering: Opportunities Exist to Improve the National Strategy (GAO-03-813)*. Retrieved July 12, 2005 from <http://www.gao.gov/new.items/d03813.pdf>.

United States General Accounting Office. (2003b). *Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms (GAO-04-163)*. Retrieved August 23, 2004 from <http://www.gao.gov/new.items/d04163.pdf>.

United States General Accounting Office. (2004, March 4). *Combating Terrorism: Federal Agencies Face Continuing Challenges in Addressing Terrorist Financing and Money Laundering (GAO-04-501T)*. Retrieved August 23, 2004 from <http://www.gao.gov/new.items/d04501t.pdf>.

Zarate, J.C. (2004, September 22). Address. Presentation at "How Money Moves: A Threat Public Security?" Newark, NJ.

Appendix A

Questions for Interview Subjects

Please begin by providing a little bit about your background:

- 1) Are you familiar with the term “Reverse Money Laundering?”
 - a) If yes, how would you describe it?
 - b) If no, interviewer provides definition from topic review.

- 2) What industries are particularly susceptible to reverse money laundering and why?

- 3) If reverse money laundering can be broken down into two components, the raising of the funds and the disbursement of the funds, which presents more of a problem to detect and why?

- 4) Informal Value Transfer Systems (IVTS) play an important role in the disbursement of funds generated from reverse money laundering, and recent regulation has been passed to regulate the Money Services Business. What is the best way to enforce the regulation and why? If the interview subject is not familiar with IVTS, interviewer provides definition from topic review.
 - a) Increased fines for violators?
 - b) Reduce the requirements for registration?
 - c) More investigations to detect IVTSs?

d) Other

5) Who bears the primary responsibility for stopping reverse money laundering? Please rank them in order of importance and explain why?

- a) Regulators
- b) Financial institutions
- c) Vulnerable industries
- d) Legislators
- e) Other

6) Are the current methodologies used to detect money laundering, such as manual and automated transaction monitoring, sufficient to detect reverse money laundering?

- a) If yes, why?
- b) If no, why not?

7) How should these current methodologies change to better adapt?

8) What is more effective for identifying reverse money laundering, transaction monitoring or scanning for entities associated with reverse money laundering? Why?

9) Do government lists of restricted entities such as the one maintained by OFAC or other lists like those identifying Politically Exposed Persons, take on greater importance for preventing and detecting reverse money laundering?

- a) If yes, why?
 - b) If no, why not?
- 10) What improvements can be made to enhance the information on these lists?
- 11) How can these lists be better utilized?
- 12) What obstacles may prevent the implementation of these improvements?
- 13) What is the most important area of focus required to enhance the detection of reverse money laundering? Please rank them in order of importance and explain why?
- a) Intelligence (including law enforcement)
 - b) Legislation
 - c) Information sharing
 - d) Technology
 - e) Other

Appendix B

Consent Form

My name is Seth Schwartz. I am conducting a study on Reverse Money Laundering as part of the course requirement for Research and Analytical Methods in Fraud Management in the Master's program of Economic Crime Management at Utica College. I am studying this to better understand the typologies of Reverse Money Laundering and attempt to identify an area where efforts should be focused in order to better detect and prevent Reverse Money Laundering. If you agree to be part of this study you will be interviewed to tell your experiences or opinions on Reverse Money Laundering and anything you think I should know.

The expected duration of interview itself will be approximately 30 minutes. The information you provide will be used in the report but will remain anonymous.

Participation in this study is voluntary. There is no penalty if you do not participate in the study or if you decide to withdraw from it during the research or interview process. You also do not have to answer any question unless you want to do so. Please do not discuss any illegal activities you know about that might occur in the future. If you have questions about the study, I will answer them at this time. Questions related to this project may be directed to me at 203-246-7484 or to Don Rebovich, 315-792-3231 or to Dr. R. Scott Smith, Chair, Utica College IRB, at 315-792-3240.

Documentation that notification has been made and that subject has agreed to participate.

I, _____ voluntarily agreed to participate in this study, after receiving notification about the study.

Researcher's Name (Print)_____ Researcher's Signature_____

Participant's Signature_____ Date _____

