

COMPLICITY IN THE WIRE TRANSFER PROCESS
A CAUSE FOR INCREASED
MONEY LAUNDERING

by

Jason M Plantin

A Research Project Submitted to the Faculty of

Utica College

August 2014

In Partial Fulfillment of the Requirements of the Degree

Master of Science Economic Crime Management

UMI Number: 1564626

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI 1564626

Published by ProQuest LLC (2014). Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against unauthorized copying under Title 17, United States Code



ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

© Copyright 2014 by Jason M Plantin
All Rights Reserved

Abstract

There are conservative estimates that the amount of money laundered each year is anywhere between 2 and 5 percent of the annual gross domestic product of the world economy. That figure in dollars is between \$800 billion and \$2 trillion in U.S. dollars. Research has shown that the majority of money that is laundered across the globe either enters the United States or comes from the United States. It can be argued that the use of wire transfers is the preferred method used by criminals to move their funds. By using wire transfers it is more difficult for those tasked with prevention and investigation to track the money.

Wire transfers have become the preferred method for criminals to launder money. This is because they are fast, secure and very hard to trace. It is electronically sending cash to another individual or account. It can be sent to another account or sent to an individual for immediate pick-up depending upon the type of service a person chooses to use.

This paper researches the argument that there is complicity within the wire transfer system that has supported this method for illegal activity and money laundering. The research argues that given the lack of effort by financial institutions and Federal regulations and enforcement efforts this activity will continue to increase. There have been successful efforts employed to reduce money laundering through wire transfers. These methods have not been embraced by the larger community of enforcement officials nor the Federal Government.

By using proven methods and analyzing trends and data within the wire transfer process an effective set of tools can be deployed by regulators, investigators and financial institutions to mitigate money laundering.

Keywords: Economic Crime Management, Wire Transfer, Money Laundering, Ray Philo

Table of Contents

List of Illustrative Materials.....	v
Introduction.....	1
Literature Review.....	5
Evidence of Complicity.....	12
Discussion.....	20
Recommendations	27
References.....	37
Appendices.....	39
Appendix A – FinCen Section 314(a).....	39
Appendix B – FinCen Section 314(b).....	41

List of Illustrative Materials

Figure 1 – Money Laundering Cycle.....	3
Figure 2 – Illustration of Wire Transfer.....	4
Figure 3 – Map and Ranking BASEL Index Countries.....	19
Figure 4 – BASEL Index Definition.....	20
Table 1 – Top 20 Money Laundering Countries.....	35

Introduction

Money laundering is a global problem and the use of wire transfers to commit the act of money laundering is an increasing crisis. But why does money laundering continue to grow each year? Why is the United States the top destination country for this activity? Why do wire transactions continue to be the favorite choice of criminals when attempting to launder money? The United States banking system has the ability to prevent money laundering through wire transfers by following a successful program implemented by the State of Arizona as well as the suggestions of experienced individuals in the banking industry and law enforcement. Yet the issue has continued to grow with little action from the Federal government and those in the highest level of banking to stop it.

This project will assess the available data regarding money laundering and the use of wire transfers. The research and literature review will analyze data from money transfer companies, scholarly articles and books. The project also reviews data from the Federal government and World Bank regarding global transaction information and trends. The project provides arguments that suggest there may be complicity within the banking system in the United States as well as that the financial institutions and government have created an environment difficult for those laundering money. In the end it will provide recommendations on how to improve the current system in order to help prevent the growth of money laundering through the use of the wire transfer.

A wire transfer is as close to sending cash as an electronic transaction can be to handing someone a stack of bills, regardless of the denomination. Wiring money is easy, fast and can be done from anywhere there is an internet connection. With the increase in globalization there is almost no where you cannot send money quickly. However, even with the increase in ease and

ability to send funds across the globe the United States remains to the top destination for criminals in terms of money laundering. This is in spite of an environment and culture that appears to have strong anti-money laundering laws and regulations in place at the Federal level. Yet, it is difficult to distinguish the difference between the global economy and that of illicit funds as they have become so intermingled it is difficult to distinguish between them. In fact, each separate economy is dependent upon one another. This argument helps support the theory that banks have become complicit in the use of wire transfers for the laundering of money. The average cost of sending a wire transfer through a traditional bank for domestic outgoing transfers is \$26.40; an outgoing foreign transaction is \$45.50; the cost an incoming domestic transaction is \$14.70 while the incoming a foreign transaction is \$17.50 (Kim, 2013). These are some of the highest fees a bank charges to a customer. They charge not only for sending a wire transfer but also for receiving one. After all, banks are in the business of making money and showing a profit at the end of the year. One way to help be successful is to conduct as many transactions for a fee as possible. Institutions such as Western Union and MoneyGram make a business of sending wire transfers, and rates vary depending on the dollar amount of the transaction. Without charging fees for their services these companies would not exist. The globalization of the economy has made it possible for money to be transferred to regions that just a few decades ago were not open to the larger market of money transfers. The United States has the ability to extend its laws to international money laundering and wire transfers should some part of the transaction be conducted through a bank in the United States.

The United States Federal statute against wire fraud can be found in 18 U.S.C. §§ 1343 and the statutes against money laundering can be found in 18 U.S.C §§ 1956 & 1957. These statutes make it a Federal crime to commit these acts. In addition the United States Federal

government regulates financial institutions regarding where they can send money and who can do business with through The Office of Foreign Assets Control, OFAC. This part of the Department of Treasury administers economic and trade sanctions based on U.S policy. The goal is to control funds used by narcotics traffickers, terrorists and others the United States believes to be a threat to national Security. These statutes and regulations provide the United States with some of the strictest anti-money laundering laws in the world. They also provide Federal prosecutors with a number of tools in order to convict those responsible for committing these crimes.

Money laundering as defined by the United States Treasury is financial transactions in which criminals and terrorists attempt to disguise the proceeds, sources and nature of their illicit activities. The Treasury states that money laundering threatens the integrity of the financial systems (U.S Department of the Treasury, 2014). An illustrative depiction of a traditional money laundering scheme can be seen in the figure below.

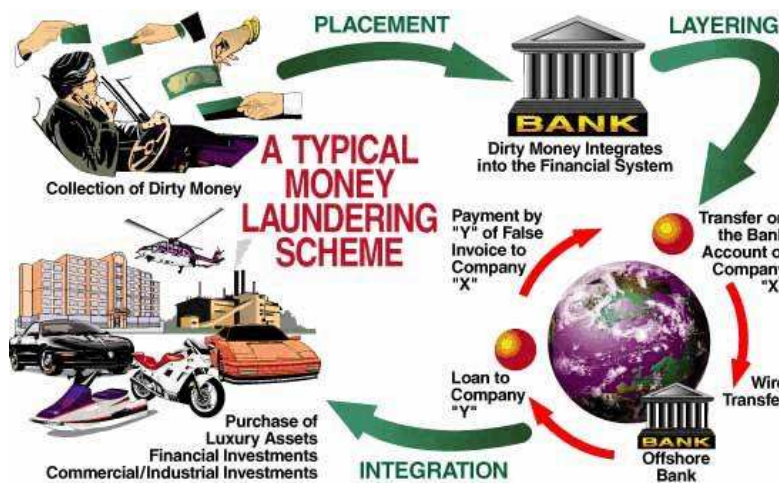


Figure 1. Illustration of the money laundering cycle. Adapted from United Nations Office on Drugs and Crime, <https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html>

Wire transfers are an electronic transfer of money from one person to another. It also can include transferring funds electronically from one bank, or credit union, to another. The wire transfers that involve sending money from the United States to another country are called a remittance transfer (ConsumerFinancialProtectionBureau, 2013). These transactions are considered to be a safe and reliable way for someone to send money to another person or themselves. Many businesses also use wire transfers as a way to pay invoices or for goods and services. An example of how a wire transfer works can be seen in the illustration below.

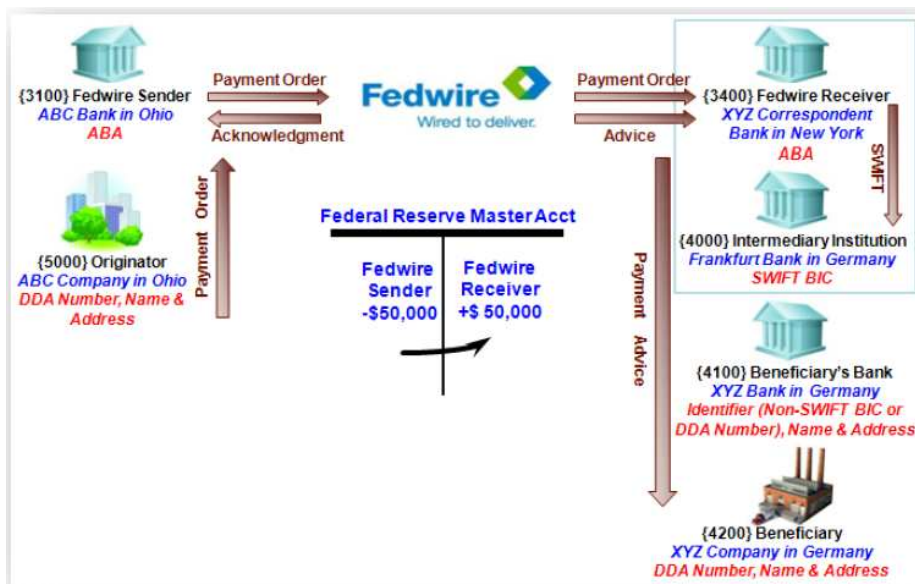


Figure 2. Illustration of a wire transfer. Adapted from Federal Reserve Board, http://www.frbservices.org/fedfocus/archive_fedwire/fedwire_0511_01.html

This method of sending money has become the main tool in which global money launders are able to quickly and anonymously wash their illegal funds and integrate them back into the larger economy.

Literature Review

Money laundering is a major concern for financial institutions and Money Service Businesses around the globe. There are a number of government regulations in place that require these institutions and companies to report suspicious activity that may involve the laundering of money. These companies are also required to have programs in place to review and monitor customer activities as well as their accounts in effort to identify any suspicious transactions. The purpose of these regulations is to uncover criminal activity as well as potential terrorist financing. The main goal of money laundering is to conceal the proceeds of criminal activity by integrating it into the legitimate economy. Additionally, the more steps in the process the harder it becomes to track the flow of the funds. Likewise, the quicker and more anonymously it can be accomplished, the better. One of the fastest and most convenient ways to send money is through a wire transfer. A wire transfer is a monetary transaction between two parties in near real time; it is the electronic equivalent of sending cash. A wire transfer can be conducted from any number of locations across the globe. It can be initiated through a traditional bank, brokerage firm or from the privacy of a home computer. There are also many one-off locations that provide these services, such as Western Union or MoneyGram. Some of these businesses are run as standalone locations while others are operated as a part of gas stations, supermarkets or convenience stores. This makes the availability of sending money through a wire transfer convenient to a substantial number of people. While the majority of the transactions conducted using wire transfers are legitimate, there are still quite a few transactions that are either fraudulent or conducted for the purpose of laundering money; and these cannot be minimized. There have been arguments made that it has become impossible to distinguish between what is legitimate economy and is illicit economy.

Since the 1990's there has been an ever increasing globalization of economies and the world is becoming a seemingly smaller place. Through the use of the Internet it is now possible for people to have instant communication with someone else thousands of miles away. It is an everyday occurrence to hear of a news story from distant geographical locations; many times these stories are due to natural disasters or civil unrest. We can sit in front of our computers and watch an event unfold live from thousands of miles away. One of the other aspects of this globalization is the ease in which a person has the ability to send money to different locations across the globe. This is also a result of increased completion to expand business into new markets. It is possible for anyone to create an account through MoneyGram or Western Union on a computer and send money across the globe with the ease of a few button clicks; especially when the currency exchange is automatically made within the system. There is information that needs to be entered to help comply with the Know Your Customer regulations; similar to a traditional bank in accordance with Customer Identification Programs. However, the fact is that it is no longer necessary to initiate a transfer face to face. In many cases when using a traditional bank or brokerage firm a person can send and receive funds without ever having to physically interact with another human. Many of these advances and changes in the world economy and business have been beneficial. The revolution of online banking has made it simpler and more efficient for people to send money to those in need or to their family members back home; while also aiding in the success of large scale relief efforts. However, it has also made it easier for those who wish to launder money to find ways to use the established system to go undetected. It was argued in Niam's book *Illicit*, published in 2006 (Naim, 2006) that our global economy and that of illicit funds has become so intermingled that it is now incredibly difficult to distinguish between the two. The book also argues that each separate economy is in fact dependent upon

one and other (Naim, 2006). This argument helps support the theory that banks have become complicit in the use of wire transfers for the laundering of money. He argues that “it is increasingly difficult for any bank, mutual fund, wire transfer provider, check casher, or other financial institution to be absolutely sure that 100 percent of the funds it moves are clean (Naim, 2006). This is due mostly to the increase in globalization and opening of the financial systems of countries around the world. As evidence the daily volume of currency exchange grew to \$1.88 trillion dollars a day in 2004; a big jump up from \$590 billion in 1989. According to the Federal Reserve quarterly report the average value of a wire transfer in 2004 was \$3.8 million dollars. At the end of 2013 that dollar figure has grown to \$5.3 million; totaling an increase of almost a 40% (Federal Reserve Board of Governors, 2014). That rise suggests there is large amounts money wired between people and financial institutions within the United States that when compared to the average American income can begin to look suspicious. According the United States Census Bureau the median household income in 2012 was \$51,324. However, some of the volume and dollars of money can be attributed to business to business wire transfers; who may inflate the average. As an example, according to the 2012 annual report from Western Union, they conducted 432 million business payments to 231 million customer-to-customer payments which translated to 53% more business to business than customer to customer transactions (Western Union, 2013). The counter argument in regards to some of those transactions is that it assumes those business to business payments are not all legitimate and do not account for any shell companies that have been established by criminals. When you apply the generally accepted rule of thumb on estimated money laundering as it relates to total GDP at anywhere between 2 and 5 percent of the total world GDP, that equates to 4.6 million in customer-to-customer money laundering transactions and 8.6 million in business payment transactions that could potentially be

involved in money laundering. Those estimates are probably closer to anywhere between 115,500 and 216,000 transactions when you apply an average industry fraud percentage rate of 5 basis points. The fact is that the actual figures are difficult to determine due to many undiscovered transactions that are related to an actual money laundering scheme. Taking a conservative approach to estimate the number of transactions potentially related to money laundering that flow through the FedWire system it equates to be 625,516 up to 2,502,062 when applying the same logic. In continuing to use the arguments developed by Naim as they related to the numbers from Western Union and the FedWire system, he states it is impossible to review each of these transactions. In 2004 there were over 2 trillion transfers conducted by financial institution, wire transfer businesses and others. Given the volume of transactions there are simply too many for an institution to regulate without causing too much strain on the day-to-day business transactions. The rise of technology makes it possible for any institution, especially those that previously had been somewhat sheltered of any money laundering activity, to potentially be impacted from a scheme. It is now easy to send money to a small or moderate sized community supermarket or bank in near real-time and receive funds. Gone are the days of having to transfer funds to large banks or large cities where money transfer services are traditionally more popular. In addition to the rise of technology the need for businesses to continually expand and increase profits still exists. A small banking institution may miss out on the opportunity of collecting a significant amount of fees if it does not offer these services; the same is true for the local convenience and/or grocery store.

There are arguments that some of the regulations and rules in place for wire transfers have made it more difficult for money laundering to occur using these services. In an article from the Stanford Paper, written in 2009 by Joyce Dela Pena, suggests that due to a reporting

requirement instituted in 1996 criminals are no longer able to hide the origin of their funds when conducting transfers within the United States. That regulation change has required banks to include all identifying information on wire transfers (Dela Pena, 2012). Another example of such an argument comes for a paper written by Michelle Segura. Her paper on the use of wire transfers by narcotic traffickers suggests that with these changes wire transfers that were not being reviewed would be reviewed after implementation (Segura, 2010). Segura also proposes that while wire transfers may continue to be used by narcotic traffickers the payment regulations that have been enacted make it more difficult and will be subject to tougher regulations. In addition Segura argues that through enhanced OFAC screening and regulations (even from transactions that originate in a foreign country) the system is safer and will increase the amount of perceptible money laundering. Additionally, she argues with the enhanced regulation, including following OFAC screens procedures and enhanced messaging; the use of wire transfers to launder money has become more difficult. To further the argument is the fact that many financial institutions and money transfer service businesses have established compliance departments as well as anti-money laundering and fraud prevention units in order to review suspicious transactions. Deborah Landron De Guevara suggests in an article written in 2012 for BAI.org (a financial service association) that by using a combination of Know Your Customer strategies in addition to technology solutions an institution will improve their ability to prevent, detect and deter the use of wire transfers for money laundering. By taking the approach that an institution has a reasonable belief the applicant is who they say they are and using a third party to verify the information, it is enough to open an account or send money. In short DeGuevara argues that by using the current method and strategies available, while also observing the United States Federal Regulations in regards to compliance, an institution will be more proficient at

uncovering fraudulent wire transfers (Landron De Guevara, 2012). While the Federal Financial Institutions Examination Council (FFIEC) suggests that institutions with effective policies and procedures in place, including those associated with regulatory requirements and transparency, with other financial institutions regarding wire transfers will retain a greater risk reduction. This includes taking a risk based approach to transaction monitoring and due diligence activities. It is generally accepted in the banking industry that FFIEC recommendations should be followed. Many would assume that by following these suggestions of implementing procedures and departments solely focused on combating money laundering the risks of a company's exposure to criminal activity and regulatory fines will be reduced. However, given the continued use of traditional and non-traditional financial institutions of wire funds for the purposes of money laundering the application of these measures seem to be relatively ineffective. This suggests that the primary reason an institution implements a program is to comply with the regulations enacted. Given some of the language used in regulations regarding a company's determination of its own risk in related to money laundering activity, as well as acknowledgement that only certain transactions can be reviewed without ceasing business. In fact these procedures are predominantly applied in effort to protect a company from lawsuits or government fines. An example of this is in a telling answer from *Illicit* in which Niam asked a private banker in Zurich how difficult it was for him to hide money from authorities in the current environment compared to a number of years ago. To which the banker answered, "the main difference is that I charge more." This again suggests that despite numerous regulations and enforcement it is still fairly effortless for someone to launder money.

In a working paper on gravity models of Trade-Based Money Laundering for the bank of the Netherlands, Jaras Ferwerda, Mark Kattenberg, Han-Hsin Change, Brigitte Unger, Loek

Grott and Jacob Bikker argue a different model is more effective to measure global money laundering. That model uses a trade based approach to more accurately explain money laundering flows. In fact they suggest that trade-based money laundering in general is a more precise measurement of the impact money laundering has on an economy. This model uses data based on import and exports of the United States as well as other countries. Their research suggests a similar pattern of elevated money laundering rates in countries that take a more meticulous approach, compared to those which observe less cautious regulations. They argue this type of measurement and method of money laundering implies a new trend for the way money is being laundered between countries. A few examples of this new trend of money laundering would include bottles of standard ketchup being sold for \$50, a household football for \$3,000 dollars and a Gucci watch worth \$100,000 that was reported as a \$50 Swatch watch on the import bill of laden. The suggestion is that transactions that involve abnormally high or low prices are indicative of money laundering (Ferwerda, et al., 2011). However, this argument is in accord to the suggestion that wire transfers are the primary method used to launder money. In a report authored by Barry Peterson titled *Red Flags and Black Markets: Trends in Financial Crime and the Global Banking Response* for the Journal of Strategic Security, he states that wire fraud is probably the most common method in which illicit funds are transferred. He argues that wire transfers are in fact the preferred method of moving illegal money. He also makes the case that globalization has made wire transfers the easiest way to move money. This is due to the fact that wire transfers are simple and swift; a fact that also makes it extremely difficult for anyone to monitor. Peterson suggests that the enhanced training of front line staff will help to identify money laundering more quickly and effectively. Another one of the interesting red flags in the report relates to business to business wires. Peterson suggests a more thorough review of

transfers between businesses in unrelated industries. He also outlines some examples of the most popular industries in which money laundering occurred; such as used car importers and exports, flower shops, precious metal companies, real estate and recycling companies. Again these suggestions rely mostly on a traditional method of detection or an increase in manual review of wire transfers. Peterson also proposes an increase in collaboration with other financial institutions in order to provide a more holistic approach to the identification of suspicious activity (Peterson, 2013). This suggestion mirrors those of the FFIEC and others at it related to sections of the USA Patriot Act sections 314(a) and 314(b). This is an approach that has been successful in other industries; an example being the sharing of information regarding credit card fraud between banks and law enforcement. However until more companies prioritize the reduction of transferring illicit money, as well as ceasing to implement procedures and processes solely for regulatory reasons, it will continue to be easy for fraudsters to conduct business.

Evidence of Complicity

In a paper first published by the Immigration Policy Center by former Arizona Attorney General Terry Goodard (updated for the Arizona State University Morrison Institute for Public Policy) Goodard makes the argument that the Federal Government and states can do more to combat money laundering through wire transfers. He exclusively applies evidence from Arizona to make his argument specific as it relates to those crimes involving drugs and human smuggling. Wire transfers are the payment method most utilized by these groups because the payments are fast and anonymous. It was found, in Arizona that for every dollar that left the state \$100 entered. In a review of transactions over \$500 it was discovered that more than \$500 million per year was being wired into the state between 2003 and 2011. At its peak of volume in 2005 there were transactions of \$36 million per month coming into the state. There is evidence, and

admissions by the state's law enforcement official, that it is well known that wire transfers are the primary and preferred method. It also suggests that little effort has been employed to combat this issue. The State of Arizona implemented a plan in 2003 that required additional information to be added in the messaging of wire transfers for specific transaction. This was through the use of what was termed Geographic Targeting Orders (GTO's). Once a transaction met certain criteria and was determined to be suspicious a damming warrant was issued to divert the funds to a holding account. A total of \$17 million was detained as a part of these damming warrants; none of which were successfully challenged in court. As evidence of a successful program the dollar amount of incoming wire transfers into Arizona fell from its peak of \$36 million per month in 2005 to \$2 million in 2006. Also, at the highest volume locations for money transfers, the incoming transaction rate of 100 to 1 fell to 3 to 1. In the year 2010 Goddard provided testimony in front of Congress in an attempt to increase Federal action to combat money laundering. In response the U.S. Government Accountability Office (GAO) made a recommendation to the Department of Homeland Security shortly after the testimony to study and follow the Arizona model:

A second opportunity involves assessing the financial investigative techniques used by an Arizona Attorney General task force. The task force seized millions of dollars and disrupted alien smuggling operations by following cash transactions flowing through money transmitters that serve as the primary method of payment to those individuals responsible for smuggling aliens. By analyzing money transmitter transaction data, task force investigators identified suspected alien smugglers and those money transmitter businesses that were complicit in laundering alien smuggling proceeds.

This recommendation has still not been implemented. More importantly, an opportunity to utilize a successful program that combats money laundering has been ignored (Goddard, 2012). When reviewing instances of Suspicious Activity Reports (SAR's) from the *2013 SAR Activity Review Trends Tips and Issues* by the Financial Crimes Enforcement Network (FinCEN) there continues to be a trend of increased money laundering and wire transfers at it relates to both insider activity of officers at financial institutions and Certified Public Accountants (CPA's). The data for officers of financial institutions illustrates an increase in money laundering in the SAR's filed between 2003 and 2011. Among the activities that are included in the money laundering category are wire transfers. The number of SAR's regarding wire transfers rose from 652 in 2003 to 1,729 in 2011. In addition the number of SARA in which it specifically categorized wire transfer fraud rose from 57 in 2003 to 233 in 2011. As for the numbers relating to accountants and CPA's, there were 6,029 SAR's involving money laundering and 319 that related to wire transfers. The activity of CPA's using wire transfers accounted for 63% and 26% of the total number of suspicious activity respectively reported.

The report offers a number of examples in which the activity of laundering money through the use of wire fraud was conducted. One example from the SAR report is of an officer, described an Assistant Vice President who embezzled funds by wire transfers from one of the company's general ledgers to his own account. In an example from the SAR report regarding CPA's, one trust account under trustee ship received wire transfers of \$1 million dollars from offshore addresses and accounts from foreign countries. There was also multiple other examples of instances in which wire transfers were identified as being suspicious with transactions to and from foreign locations. In some cases it appeared to be from shell corporations and other offshore companies. In one extreme example, a CPA pleaded guilty to wire fraud by diverting

\$1 billion from his firm to a shell company. Another example of a large dollar loss from the report detailed a case in which a CPA admitted to stealing over \$30 million in a scheme that included securities fraud, wire fraud and money laundering (BSA Advisory Group, 2013). These examples provide an argument that the use of wire transfers for money laundering purposes continues to be the preferred method for criminals. It may be suggested that the use of the SAR report by financial institutions helped provide a tool to catch and convict the fraud. There may also be a counter argument that due to the magnitude of money involved there remains opportunities within the wire transfer system to prevent, detect and deter this activity more quickly. While one financial institution may file a suspicious activity report on questionable activity it takes a number of similar reports and sharing of information with law enforcement to be successful.

James Petras, Professor of Sociology at Binghamton University, authored an article for the *Center for Research on Globalization* about the complicity of banking systems in the United States in regards to money laundering. In his argument Petras cites evidence from United States Congressional Investigators, as well as the banking community (both internationally and within the United States), that between \$500 billion and \$1 trillion is laundered annually: half through U.S. banks alone. Those figures equate to between \$5 trillion and \$2 trillion per decade. A conservative estimate puts a dollar figure for money laundering at \$5.5 trillion to \$3 trillion flowing into banks within the United States during the 1990's. He argues that without the flow of illicit money into the U.S economy the living standards would decline and the dollar would weaken. Petras discovered that the inflow of criminal money was higher than the revenue of IT companies (where there was a higher amount of money laundering) combined with the net transfers by all major U.S. oil producers, military industries and airplane manufacturers. He then

argues that the most prevalent U.S. banks receive a high percentage of their profits from the servicing of money laundering accounts. His argument points out that in order to achieve profits most banks ignore the government regulations in place to deter money laundering activity as well as internal banking procedures. Another example of the involvement of banks in regards to money laundering, according to Petras, is the establishment of correspondent banking (CB). This service is where one bank provides assistance to another, usually allowing a bank outside the United States to conduct business within the United States. These relationships also offer noteworthy profit opportunities for banks. Petras points out that some of these biggest CB relationships specializing in international fund transfers process up to \$1 trillion in wire transfers daily. Some of the other examples cited are the cases involving money laundering at Citibank. The examples totaled almost \$400 million dollars and included money from drug dealers, former Pakistani government officials, a former dictator and other foreign government officials from OFAC sanctioned countries. In furtherance of his argument Petras notes that after these customers of Citibank were arrested money movement to secret accounts continued. In addition, no banking official at Citibank was brought to trial. He summarizes his argument that this type of criminal activity has embedded itself within the current economics of the capitalist market place. In short, illicit money is the new way for banks to increase profits (Petras, 2001).

John Walker and Brigitte Unger from the University of Wollongong, Australia have developed “The Walker Gravity Model” in an attempt to measure the impact of money laundering on economies of the world. The argument that increased regulations, prosecution and deterrence will in fact prevent money laundering is not proven when using Walkers model. In all actuality the model finds the contrary to be true; where more frequent and stiffer punishment leads to higher levels of corruption and criminal activity. The Walker Model measures money laundering

using a combination of data collected regarding criminology, economics and finance. His mathematical formula is $(\text{GNP/capita}) \cdot (3\text{BS}_j + \text{GA} + \text{SWIFT}) - 3\text{CF}_j - \text{CR}_j + 15$ Distance; where GNP/capita is GNP per capita, BS is Banking Secrecy, GA is Government Attitude, SWIFT is SWIFT member, CF is Conflict, CR is Corruption. It makes assumptions that crime generates income in all countries. Income from crime depends on the prevalence of different types of crime and the average proceeds of those crimes; i.e. the more sophisticated and organized the crime the more income it generates. While richer countries generate more income per crime than that of poor countries, income inequality or corruption may support a richer criminal class, even in poor countries; keeping in mind that not all income from criminal activity is laundered. The model also assumes that not all money leaves a country when being laundered. More corrupt countries provide better environments for money laundering. As a result money launderers seek countries that provide tax havens and lax banking regulations in addition to low risk, stable economies (Walker & Unger, 2009).

Hitesh Patel and Bharat S. Thakkar used information from Walkers theory and research in a chapter titled “Money Laundering among the Globalized World” for the book *Globalization – Approaches to Diversity*. In reviewing the top 20 origins and destinations of money laundering the United States was at the top of the list. They suggest it is due to the strength of the U.S. dollar. In 2009 the United States accounted for an estimated 30%, totaling \$800 billion, of laundered money worldwide. They also point to the advancement in technology for increasing the ease of money laundering. Patel and Thakkar argue that because banking institutions are able to provide a variety of different services to their customers, they are the preferred agent used to launder money. Banks are able to transfer funds between institutions or different branches of an institution across geographical locations. This includes the transfer of money across

international borders. Due to the nature of strict bank secrecy laws the transfer of funds is more anonymous, making it easy to cover and hide the source of the money. It is also suggested that there has been an increase in professional money launderers. Those professions that possess specific knowledge and tools, such as lawyers, accountants and trust companies, offer the ability to hide the source of funds through shell companies and offshore accounts. They are able to provide anonymity in the ownership and management of accounts for criminal activity. Patel and Thakkar also offer statistics from the United States Internal Revenue Service related to money laundering investigations which also suggests an increase. In the year 2009 there were 1,341 money laundering investigations while 1,597 occurred in 2010 and 1,726 in 2011. This is an increase of 28% in the number of cases investigated by one law enforcement agency within the United States (Patel & Thakkar, 2012). The United States arguably has one of the strongest economies in the world as well as some of the strictest anti-money laundering regulations; accounting for the argument that money laundering occurs in those economies in which there is a stable environment with strict regulations and laws. And based on these numbers it appears this is a trend that will likely increase.

According to the BASEL Index on money laundering, which is an index based on data aggregated from the Financial Action Task Force (FATF) ranking the risk of money laundering by country, the World Bank and the World Economic Forum provides a list of the top ten risky countries for money laundering.

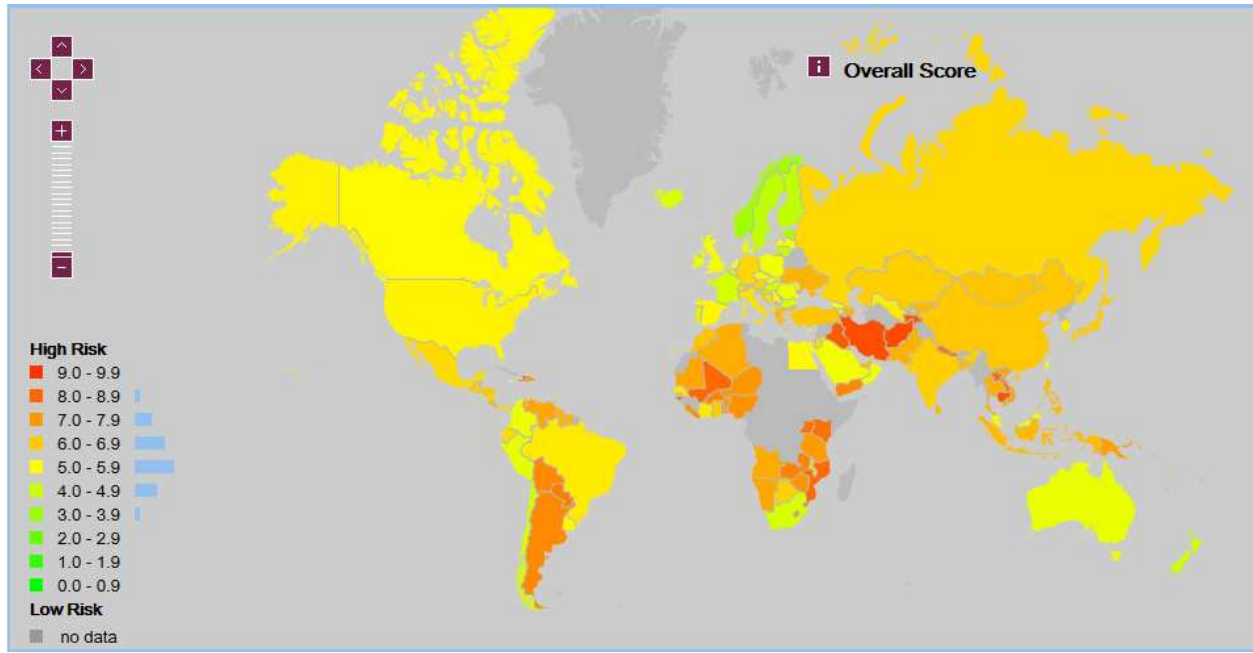


Figure 3. Map and ranking of the
Adapted from The Basel AML

Rank	Country	Index
1	Afghanistan	8.55
2	Iran	8.48
3	Cambodia	8.35
4	Tajikistan	8.27
5	Iraq	8.19
6	Guinea-Bissau	8.17
7	Haiti	8.09
8	Mali	7.95
9	Swaziland	7.9
10	Mozambique	7.9

10 Highest Risk countries.
Index,

* Source: Basel AML Index
2013

<http://index.baselgovernance.org/index/Index.html#map>
The BASEL Score is determined using the following information.

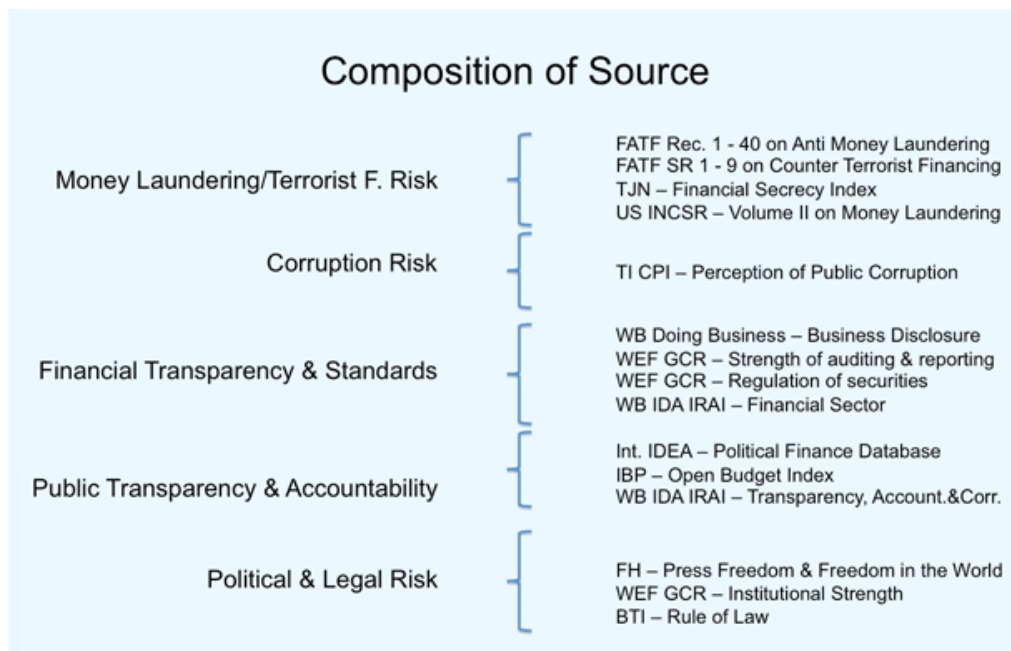


Figure 4. Definition of the BASEL Index Score. Adapted from The Basel AML Index, <http://index.baselgovernance.org/index/Index.html#methodology>

In comparison, FATF (an inter-governmental body whose objective is the implantation of legal, regulatory and operational measures for combating money laundering and other threats to the international financial system) provides a list of high risk and non-cooperative jurisdictions. It published this list in February 2014 which included Iran and North Korea as two countries subject to increased pressure due to money laundering. In addition it noted that the following countries, Algeria, Ecuador, Ethiopia, Indonesia, Myanmar, Pakistan, Syria, Turkey and Yemen, all had severe deficiencies in addressing money laundering.

Discussion

With the introduction of the Internet in the 1990's we have become more connected than ever to people and places around the globe. This is especially true in the business world. There are more and more businesses that are conducting relationships within other countries. Financial Institutions, banks, and money transfer services are prime examples of the expanding global economy. All of these companies are engaged in growing their business in new areas. This has

resulted in an opening of markets in areas previously closed to international business. Companies like MoneyGram and Western Union provide fast and easy methods to send money across the globe. International wire transfers are a quick, processed closed to real time, and easy way to conduct these transactions. The majority of these are legitimate; however it has also opened the market for those who conduct illegal activities. These individuals take advantage of the same systems in place to launder money. Estimates place the dollar figures related to money laundering in the trillions each year. This figure continues to grow despite a number of governments across the world taking an aggressive approach to the identification of money laundering. There are numerous law and regulations, as well as best practices published by government bodies, in order to combat this issue. Yet the problem seems to be increasing. Some, such as Niam, even suggest there can no longer be a distinction between dirty money and clean money. That each economy has become dependent on the other. That without an influx of dirty money into the financial system some economies may suffer greatly. In fact, some countries economies could potentially cripple and no longer exist. This co-mingling of money has created an environment in which despite of efforts to address the global issues there is little appetite to address this issue. The Gross Domestic Product, the ratio in which economies are measured, relies on dirty money.

There are examples of cases of money laundering in which bank after bank appears complicit in the activity through its institution. The \$400 million dollar case at Citibank is the prime example in which employees at the bank took total disregard for internal controls and government regulations in order to conduct business with known criminals. The primary reason, as argued by Petras, is that banks are able to make a significant profit by serving these customers and their transactions. This mirrors the argument by Niam that the economy, of not only the

United States but globally, has to a degree become reliant on the profit banks can earn by conducting these transactions and holding the money at their institutions. The other suggested profit increasing relationship that is argued to cause financial institutions in the United States to be complicit in money laundering is correspondent banking relationships. The relationships that have been able to develop due to the globalization of the economy and the opening of markets in countries that prior to the 1990's did not have the ability to wire money internationally. Given the estimate of a trillion transactions conducted each day by banks through these relationships the profits can be significant. A further argument could be made that while the sharing of certain customer and banking information regarding these transactions has increased there are still areas in which improvement can be made.

There are arguments that propose combating the use of wire transfers to facilitate money laundering can be increased. There are also arguments suggesting that it has become increasingly difficult to launder money in today's environment of increased regulations and focus by financial institutions. However, the evidence suggests that even with the increase of regulations and enforcement actions money laundering is increasing across the globe. The research by Walker and others suggest that money laundering in fact increases in an environment in which stiff penalties exist. That argument has also been shown that the United States is in fact the country most favored to launder money. Many would argue the United States ranks among the countries with the strictest anti-money laundering regulations in the world. It is the United States that publishes a list of those countries that are the most risky for doing business as it relates to money laundering. The U.S also hands out sanctions against countries and individuals it deems as risky, either for financial institutions to increase due diligence or with to not conduct transactions. Yet the United States does not recognize itself as being the highest risk country

through which money is laundered. In addition there are many examples in which the use of wire transfers is used to launder money on U.S soil. This evidence comes from case examples from Suspicious Activity Reports submitted by financial institutions and investigated by Federal Law Enforcement. These reports make it somewhat difficult to measure the use of wire transfer to launder money because they are submitted using two primary categories, money laundering or wire transfer. However, when viewed together and those specific cases mentioning the use of wire transfers is measured the numbers have been increasing for the past three years. The dollar amount of the transactions related to wire transfers is also increasing, both in regards to money laundering and within the industry as a whole. According the Federal Reserve the average dollar amount for a wire transfer is over \$5 million.

The other fact is that most of these transactions are business to business transactions. Western Union itself conducted over 50% more business to business transactions than person to person transactions last year. This is an area where little is done to verify the legitimacy regarding those involved. Given the number of business transaction and the average dollar amount of these transactions more can be done in reviewing these for potential money laundering activity. It is a simple task for a fraudster, or a person working in conjunction with a fraudster, to establish shell companies in order help facilitate the money laundering process. Once a company has been established and a bank account opened the process to wire money between accounts becomes ridiculously simple. Financial institutions still have to follow the Know Your Customer guidelines when establishing an account for a business. Depending on the type of business being established an account can be opened online. The only documentation that needs to be provided is a social security number or business tax identification number, a business license and a certificate showing business ownership. There may be other documents such as Limited

Liability Partnership documents and agreements showing the names of ownership and/or Articles of Incorporation. All of these can be drawn up legitimately or through the help of a lawyer who may be working with those laundering money. The focus of many financial institutions when monitoring for suspicious transactions relating to money laundering is to use aggregate data based on monthly activity. As long as a business conducts roughly the same number and dollar amount of transactions each month there is no suspicious activity. There is little review of what type of company is sending and receiving money. As evidence suggested by Peterson of Wells Fargo in his paper regarding global trends in banking he notes suspect businesses that may be more likely to launder money. Since there can be little review of business to business transactions it is also important to train all staff members involved in the transactions on what may be suspicious and how to handle those situations appropriately. This is important given there is a lack of collaboration between financial institutions regarding suspicious behavior. The State of Arizona has become an entry point into the United States through which a number of illicit activities are conducted. This is done through the illegal drug trade and through human smuggling. It follows that there is also a lot of money laundering through the state in order to conduct those businesses. It was proven by the States Law Enforcement community that wire transfers were the primary method for which these transactions were being conducted. An analysis of incoming and outgoing transaction was completed showing that a 100 to 1 ratio of money was coming into the state versus going out of the state through wire transfers over an eight year period. At almost \$40 million per month at the peak of activity it can be argued that it was very safe to wire money into the state without raising any red flags. There has been no other such analysis conducted by another state in an attempt to find similar activity. There has also been no other analysis conducted at the Federal level to identify if any other state experiences a

similar disproportionate amount of wire transfer activity. Arizona took a hard line approach to review and subpoena information on high dollar wire transfers coming into the state as well as obtaining more information regarding the sender and receiver of money. When a transaction appeared to be suspicious the state would obtain a court order to hold the money. Throughout the entire eight years this program was implemented, zero transaction holds were successfully challenged in court. The result was a decrease in both the number of incoming wire transfers and the dollar amount of those wire transfers. This would suggested by reviewing specific wire transactions while taking appropriate actions to prevent them and recover funds there can be a decrease in money laundering. However, when the Attorney General of Arizona testified before congress there was little notice and no similar plan implemented. This was also the case even after the program was suggested by United States Government Accountability Office. This suggests there may be a general lack of interest in combating money laundering through the use of wire transfers.

Every financial institution is required by law to file a Suspicious Activity Report through the Financial Crimes Enforcement Network when they identify activity that appears to be related to fraud or money laundering. This data is summarized for review each year with trends and case examples in order to provide information in order to learn what issues they encounter in the future. The number of examples of cases involving the use of wire transfers to commit fraud and money laundering activity continues to increase year over year. This data is found in reports specific to the use wire transfer to launder money as well as in those categorized as money laundering. There are examples of cases involving insider activity as well as external activity. The dollar amounts reported in these cases are sometimes in the millions. Also they often times involve the use of shell companies that were set up in order help facilitate the structuring of the

money to make it more difficult to identify. Due to the increase in the use of wire transferred identified in Suspicious Activity Reports it could also suggest more emphasis is being placed on review by financial institutions to identify this behavior. However, if financial institutions were placing more importance on reviewing wire transfer transactions it can be argued the dollar amounts reported would be decreasing suggesting they would be identified more quickly. This has not been the case since transaction amounts and incidents have both increased.

One of the methods that have been proven effective in measuring the amount of money laundering that occurs within a country was developed by John Walker. His equation has been successfully applied to a number of different countries including the United States. His model is best explained by using the money laundering originating in each country. It takes into account crime as a whole and the extent of crime within a country. It also estimates the amount of money laundered for each crime and the economic environment of the country the crime is committed. It argues that a country with a low crime rate and economy that does not provide profit motives for a criminal enterprise is a country that cannot generate a reasonable amount of money to be laundered. Therefore, a country with a high crime rate and fiscally rich environment for profit can generate a sufficient amount of money to be laundered. Other dependencies involve the level of corruption, bank secrecy regulations, governmental attitudes and proximities in social and economic demographics to the originating country. The data that has been analyzed using the Walker Model for measuring global money laundering shows that the United States is the second highest rated country to launder money. It also shows the United States is the top originating country and the top destination country for which to launder money across the globe. It can be suggested that the attractiveness weighting in the formula is a primary reason it ranks so high. The strength of the economy and the U.S. dollar provide attractive environment for money

launders. Patel and Thakkar applied Walker's model and argue that even with the strict anti-money laundering regulations in the United States it remain the primary country in which money is laundered. Again the weight of attractiveness variable in the Walker model outweighs other factors such as crime rate. The amount of money that can be made per crime can be argued as increasing the likelihood the United States ranks at the top of the list as well.

Data has shown that the United States ranks at the top for both origin and destination for laundered money. This comes from the Walker Model on Global Money Laundering. Petra argues the United States is the primary country for which money is laundered. He cites as evidence Congressional Investigators and people from the banking community both within the United States and Internationally. When he compared the estimates of money laundered through the United States it was larger than revenue from a significant portion of the economy including airline manufactures, oil refineries and Information Technology companies. Those industries account for a large amount of the Gross Domestic Product of the United States. Yet given the statistics the United States does not appear on any list of high risk countries relating to money laundering. Those lists include the BASEL index and that of the Financial Action Task Force. It can be argued that the country with the highest flow of laundered money both into and out of it should be ranked as one of the high risk countries for which this activity can occur.

Recommendations

There are four main themes that can be taken from the data presented above regarding money laundering. The first is there needs to be an emphasis placed on wire transfers between businesses. The data suggests both a large dollar and volume of transactions is conducted between business accounts. Included in this review of transactions between businesses is to educate front line staff regarding what may be a suspicious transaction. This includes reviewing

transactions between businesses that appear to have little in common or do not normally conduct business with each other. This would also encompass examples such as transactions between a flower shop and an importer/exporter of motor vehicles. There are such companies that are traditionally involved in the laundering of money including, car import and export businesses, flower shops, precious metal companies, real estate businesses and recycling companies. This is can be ever changing and a full review should be conducted at a minimum of annually. Another area in which there can be improvement in the prevention and detection of money laundering is collaboration and transparency between financial institutions. This also includes cooperation between financial institutions and law enforcement officials at all levels. This can be difficult given the concerns concerning privacy and potential lack of information available regarding who is sending and receiving money from a wire transfer. However, as in the example from the state of Arizona this can be accomplished. A third area is the use of available data for analysis to help identify trends, cases and areas for improvement. The State of Arizona can be used again as an example in the use data to identify issues and solutions to combat the issue. Also it is possible to review information from Suspicious Activity Reports (SAR's) to find trends identified from financial institutions and law enforcement regarding potential suspicious activity. A new initiative from the Federal Government called Operation Chokepoint can also provide an example of how to identify, prevent and investigate money laundering through wire transfers. The fourth theme is for the United States to recognize itself as the primary country for money laundering. Every major statistic regarding money laundering has shown that the country with the high dollar of money laundered and the highest number of transactions is the United States. However, the United States never appears on a list of the riskiest countries for money laundering since it is the primary author of those lists as well as has a number of laws and regulations

regarding anti-money laundering. With a true self assessment of the data available and recognition of the problem more effort can be exerted to address the issue.

The due diligence surrounding transactions between business accounts is an area in there can be an increased focus in regards to potential money laundering. This ties in very closely with the training of front line staff regarding what to be aware of regarding suspicious activity. In addition to front line staff those in the back of house who review the suspicious transactions should also be made more conscious of potential indicators of money laundering. That includes the reviewing of the automated rule detection systems used by a financial institution to look for anomalous activity. The AML departments should perform more due diligence and know your customer reviews on business accounts. This ought to include a full review of the officers, owners, addresses and the type of business conducted as well as a phone numbers associated with the business and any potential associations linking the officers, owners and other companies. In addition an annual review of those business types that are typically associated with money laundering should be implemented to review the number of wire transactions coming in and going out of the account along with to where and who they are being sent. This information can be compared to annual earnings statements or tax information. This can determine if there is any potentially suspicious activity at an account level and not just at an individual transaction level. Many financial institutions can conduct these reviews with the assistance of data analysis and software programs that can be used to aggregate this data. A few examples of these systems include SAS, IDEA software and i2 Link Analysis. These software solutions are powerful examples of using large amounts of data to analyze trends and provide an end result that is very easy to understand. In addition, each of these tools, while very powerful, provides an easy to use interface that can accomplish these tasks with minimal training expense.

One starting point would be for an institution to review the SAR's it has filed and all fraud cases for the prior year. This would provide an analyst with known instances of suspicious accounts and transactions in order to identify other similar instances that may be hiding within the data and accounts of an institution. This can be cross references with data gathered from external sources such as the BASEL index, OFAC sanction reports, FFIEC information, the FAFT and World Bank. This accomplishes two things for a financial institution; it provides a full assessment of the potential risk of money laundering at an institution to help show Federal Regulator's how robust of a program has been developed. It can also be used to shape the program for the upcoming year to focus on the most risky behavior, accounts and transactions. Furthermore it can be used to provide examples of training scenarios and areas of the anti-money laundering program that need improvement. By using internal data of suspicious transactions it is much easier to develop customized training for all relevant areas of institution required to take annual anti-money laundering training. Combining the internal information with external global industry tendencies can lead to expanded knowledge of trends that may not yet have impacted a specific financial institution. The combination and integration of an enhanced due diligence AML program to identify trends at a macro level while also using it to build a stronger program and provide training go a long way to prevent and identify potential money laundering within an institution. Since there are more business to business transactions conducted annually by wire transfer and the dollar amounts are much larger this would indicate an area that needs more review. By focusing on business accounts, an area generally ignored, a financial institution can take a more aggressive approach to combating money laundering.

A second area in which there can be improvement in the effort to prevent money laundering is through an increase in transparency and collaboration. This is true between

financial institutions as well as between financial institutions and law enforcement officials. There is currently very little collaboration and information sharing between institutions regarding money laundering. One of the primary reasons for this is the data privacy regulations in place within the United States. While these laws are beneficial to society and help protect individuals there needs to be a solution in place for suspicious transactions and accounts. Currently there is no information sharing between financial institutions regarding potential suspicious behavior. A fraud analyst at one institution is unable to verify information regarding an account or transaction with a fraud analyst at another. There are also situations in which areas within the same company cannot share information regarding potentially suspicious transactions with another area. This makes it difficult for any real time identification or money laundering. There are programs available such as information sharing through the 314(a) and 314(b) process but those are timely and dependant on cumbersome processes. There is also opportunity for sharing with Law Enforcement officials. There are many instances in which a transaction, if known to involve money laundering, where a call is placed to a financial institution to gather information regarding to whom the money is being sent, how it was initiated, funded and other important information required for an investigation. Yet instead of providing the information a subpoena is required to release it. By the time a subpoena has been sent the transaction is long since completed and the money has become untraceable. A more real time solution that would help to solve a few of the examples above includes an automated email alert system for institutions that can be provided to law enforcement and other fraud investigators. There could also be the utilization of already established industry groups to distribute information. There are groups such as ACAMS and IAFCI that are dedicated to fraud and money laundering investigations and prevention. Each has member only areas where sensitive information can be shared and

distributed only to those individuals that need to know it. One example of this is the use of a system named CrimeDex by the IAFCI. In this closed system a member of IAFCI can sign into the member's only site, type up an alert regarding suspicious activity and send it out to a select group of individuals who may also be impacted. Those individuals receive an email alert in real time and can then communicate with the originator regarding any similar activity.

A third opportunity is to combine the efforts of a successful example of preventing money laundering, analysis of SAR information and a review of the Federal program Operation Choke point. The State of Arizona took an aggressive approach to the review of suspected money laundering through wire transfers by analyzing the data available for that state. By understanding the data and reviewing those that had been identified as suspicious, investigators and law enforcement officials were able to dramatically decrease the number of wire transfers used to launder money into and out of that state. This program can serve as a model for every state and the Federal government to use but has yet to be followed by anyone. In addition to reviewing the data available for state specific use of wire transfer information the inclusion of known SAR data can be useful to identify trends.

Information and trends gathered from SAR data and released in reports like *The SAR Activity Review, Trends and Tips Issues* can provide valuable information from financial institutions. This information is a compilation of suspicious activity reports and Federal cases involving money laundering and wire transfers. By analyzing real world examples it can provide specific opportunities in which there are opportunities within an organization to review and identify suspicious activity. One suggested change in how SAR information is reviewed and analyzed would be to allow more sharing of information across industries. This sharing would expand on the use of 314(a) and 314(b) requests and allow for a more real time exchange of

information. Since all SAR data is already housed within the FinCen e-filing database there could be a method for financial institutions to submit online queries through the web portal to inquire if another institution has filed a SAR on a similar person or entity. Enabling financial institutions to receive information regarding a potential SAR prior to submitting will make the potential case stronger. It will also help an institution when contacting law enforcement regarding the investigation of suspicious activity. Law enforcement will have the prior knowledge that multiple SAR reports have been submitted making it easier for an investigator to gather the evidence. There could be an internal counter added, such as an audit trail that would alert FinCen and the analysts responsible for reviewing SAR's to see those reports that have multiple inquires. This would also alert law enforcement of a potential trend prior to future activity as well as permit prevention methods to be developed within the financial institutions. The system can be built in such a way so that it does not identify any of the other institutions that have provided the data. A similar example in use today in the credit card industry is administered by the United States Postal Inspection service. Financial Institutions submit known fraudulent address used to commit mail fraud and members are able pull reports in order to identify those addresses. Those reports are used by fraud prevention departments when conducting investigations or building strategies and tactics to prevent certain fraud types such as account takeover fraud.

A complimentary program to the prevention of money laundering through wire transfers is the Federal program Operation Choke point. This program aims to identify financial institutions and money transfer services that appear to be ignoring Federal laws. The program has a larger focus than money laundering and wire transfers but with a few alterations can be tailored to be specific at identifying certain types of fraud. By combining the successful program

from the State of Arizona and the Federal program in addition to analyzing data submitted through FinCen through SAR's a program can be developed to identify which wire transfers are most suspicious allowing action to be taken to cease the criminals and recover the funds.

A final recommendation on reducing wire transfers in the use of money laundering is for the United States to recognize itself as the country used to launder money. This is a fact supported by a number of statistics analyzed by different groups around the globe. This lack of recognition provides the countries financial institutions with a key statistic that can be utilized to stop money laundering. There are programs established to review transactions regarding OFAC countries and individuals as well as lists of high risk foreign countries. Transactions that are initiated to others within the United States face less scrutiny since it is believed we have strong laws and regulations regarding anti-money laundering strategies. However, the evidence suggests the majority of money laundering occurs in area where there are strong anti-money laundering laws. In addition, the strength of the U.S. dollar suggests it is the commodity most attractive to money launders. When John Walkers money laundering model is used to measure global money laundering the United States is at the top of the list in every category. Walker's model has been a proven method to measure money laundering in countries across the globe. According to the model the United States is represented six times within the top 20 origins of money laundering and the top destination for money laundering.

Top 20 Flows of Laundered Money

Rank	Origin	Destination	Amount (\$Usmill/yr)	% of Total
1	United States	United States	\$528,091	18.5%

2	United States	Cayman Islands	\$129,755	4.6%
3	Russia	Russia	\$118,927	4.2%
4	Italy	Italy	\$94,834	3.3%
5	China	China	\$94,579	3.3%
6	Romania	Romania	\$87,845	3.1%
7	United States	Canada	\$63,087	2.2%
8	United States	Bahamas	\$61,378	2.2%
9	France	France	\$57,883	2.0%
10	Italy	Vatican City	\$55,056	1.9%
11	Germany	Germany	\$47,202	1.7%
12	United States	Bermuda	\$46,745	1.6%
13	Spain	Spain	\$28,819	1.0%
14	Thailand	Thailand	\$24,953	0.9%
15	Hong Kong	Hong Kong	\$23,634	0.8%
16	Canada	Canada	\$21,747	0.8%
17	United Kingdom	United Kingdom	\$20,897	0.7%
18	United States	Luxembourg	\$19,514	0.7%
19	Germany	Luxembourg	\$18,804	0.7%
20	Hong Kong	Taiwan	\$18,796	0.7%
Total	All Countries	All Countries	\$2,850,470	100.0%

Table 1. List of Top Money Laundering Countries from the Walker Model. Adapted from the John Walker Model on Money Laundering, www.johnwalkercrimetrendsanalysis.com.au/ML%20method.htm

The Walker Model can be used by those in the Federal Government responsible for anti-money laundering programs. It should be used by those setting policy and establishing regulations, from law enforcement to regulatory agencies and law makers. The current method for establishing high risk entities and individuals based on government foreign policy is a narrow approach to a complex issue. This approach does not recognize that money laundering is a global problem committed by many criminal actors through a number of different crimes. It supposes that high profile criminals and terrorists in distant lands are the only people laundering money. The policy and approach is a band-aid at best. The example of money laundering at Citi

bank has proven this to be true. When the United States can apply the Walker Model on money laundering and analyze the data and results a more holistic approach to the issue can begin to be developed. Information may be available to analyze and apply the model at the state level as well. By applying the model at the state level trends such as those identified by the State of Arizona may become apparent. There could be a clear picture of those states that conduct the most risky transactions. Once this information is disseminated it can be incorporated into the decision making at financial institutions when reviewing a transaction. It could also be built into a rules based model used by the financial industry to provide a higher score to those risky transactions. The application of this model is based on mathematics and there bias and potential red lining issues can be avoided. Similar to other rules based models it can be adjusted periodically with new information and adjusting to the current trends and environment of fraud. If the Federal government and financial institutions were to use the Walker Model it could provide for a more enhanced approach to prevention of an issue that needs to be addressed in total, not just in pieces. Until the United States can recognize that it is part of the problem very little will be done to combat money laundering within its borders and the problem will continue to exist.

There is not a single solution that can be implemented to combat money laundering through the use of wire transfers. By reviewing each area of concern, business to business transactions, training, increased collaboration and a thorough analysis of the data an approach can be developed to help reduce the problem. The use of programs that have already had success can be used as models going forward, expanded and implemented at a macro level. Finally, admitting the United States is part of the problem can be used to help push these initiatives forward. Until that time, we will continue to be complicit to global money laundering.

References

- [BSA Advisory Group. \(2013, May\). *Fincen.gov*. Retrieved from Fincen.gov: www.fincen.gov/news_room/rp/files/sar_tti_23.pdf](http://www.fincen.gov/news_room/rp/files/sar_tti_23.pdf)
- [ConsumerFinancialProtectionBureau. \(2013\). *www.consumerfinance.gov/askcfpb/1163/what-wire-transfer.html*. Retrieved from www.consumerfinance.gov/askcfpb/1163/what-wire-transfer.html: www.consumerfinance.gov/askcfpb/1163/what-wire-transfer.html](http://www.consumerfinance.gov/askcfpb/1163/what-wire-transfer.html)
- [Dela Pena, J. \(2012, September\). *Stanford*. Retrieved from Stanford.edu: http://www.stanford.edu/group/journal/cgi-bin/wordpress/wp-content/uploads/2012/09/Pena_SocSci_2009.pdf](http://www.stanford.edu/group/journal/cgi-bin/wordpress/wp-content/uploads/2012/09/Pena_SocSci_2009.pdf)
- [Federal Reserve Board of Governors. \(2014, May 30\). *Federal Reserve Board of Governors*. Retrieved from Federal Reserve: www.federalreserve.gov/paymentsystems/fedfunds_qtr.htm](http://www.federalreserve.gov/paymentsystems/fedfunds_qtr.htm)
- [Ferwerda, J., Kattenberg, M., Chang, H.-H., Unger, B., Groot, L., & Bikker, J. \(2011, September\). *dnb.nl/en/binaries/Working%20Paper%20318_tcm47-258387.pdf*. Retrieved from dnb.nl: http://www.dnb.nl/en/binaries/Working%20Paper%20318_tcm47-258387.pdf](http://www.dnb.nl/en/binaries/Working%20Paper%20318_tcm47-258387.pdf)
- [Goddar, T. \(2012, October\). *repository.asu.edu/attachments/95239/content/2012-how-to-fix-a-broken-border-part-3-follow-the-money.pdf*. Retrieved from ASU.edu: repository.asu.edu/attachments/95239/content/2012-how-to-fix-a-broken-border-part-3-follow-the-money.pdf](http://repository.asu.edu/attachments/95239/content/2012-how-to-fix-a-broken-border-part-3-follow-the-money.pdf)
- [Kim, T. \(2013, April 18\). *www.mybanktracker.com/news/2013/04/18/wire-transfer-fees-2013*. Retrieved from Mybanktracker.com: www.mybanktracker.com/news/2013/04/18/wire-transfer-fees-2013](http://www.mybanktracker.com/news/2013/04/18/wire-transfer-fees-2013)
- [Landon De Guevara, D. \(2012, April 18\). *BAI.org/bankingstrategies/compliance-and-regulatory/compliance/deterring-wire-transfer-fraud*. Retrieved from bai.org: http://www.bai.org/bankingstrategies/compliance-and-regulatory/compliance/deterring-wire-transfer-fraud](http://www.bai.org/bankingstrategies/compliance-and-regulatory/compliance/deterring-wire-transfer-fraud)
- [Naim, M. \(2006\). *Illicit*. New York: Anchor Books.](#)
- [Patel, H., & Thakkar, B. S. \(2012\). Money Laundering Among Globalized World. In D. H. Cuadra-Montiel, *Globalization - Approaches to Divesity*. InTech.](#)
- [Peterson, B. \(2013\). Red Flags and Black Markets: Trends in Financial Crime and Global Banking Response. *Journal of Stragic Security* 6, no.3, 298-308.](#)

- [Petras, J. \(2001, August\). *Centre for Research on Globalisation*. Retrieved from globalresearch.ca: http://www.globalresearch.ca/articles/PET108A](http://www.globalresearch.ca/articles/PET108A)
- [Segura, M. \(2010, December\). *Utica.edu/academic/library*. Retrieved from Utica.edu: www.utica.edu/academic/library/Segura_M_2010.pdf](http://www.utica.edu/academic/library/Segura_M_2010.pdf)
- [U.S Department of the Treasury. \(2014\). *www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Money-Laundering.aspx*. Retrieved from www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Money-Laundering.aspx: www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Money-Laundering.aspx](http://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Money-Laundering.aspx)
- [Walker, J., & Unger, B. \(2009\). Walker Gravity Model. *Review of Law & Economics*, 821-853.](#)
- [Western Union. \(2013, April 17\). *westernunion.com/files/doc_financials/WU2012ARFinalWeb*. Retrieved from Western Union: http://ir.westernunion.com/files/doc_financials/WU2012ARFinalWeb.pdf](http://ir.westernunion.com/files/doc_financials/WU2012ARFinalWeb.pdf)

Appendices

Appendix A – FinCen Section 314(a)

FinCen fact sheet sections 314(a)

Overview

FinCEN's regulations under Section 314(a) enable federal, state, local, and foreign (European Union) law enforcement agencies, through FinCEN, to reach out to more than 43,000 points of contact at more than 22,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering. FinCEN receives requests from law enforcement and upon review, sends notifications to designated contacts within financial institutions across the country once every 2 weeks informing them new information has been made available via a secure Internet web site. The requests contain subject and business names, addresses, and as much identifying data as possible to assist the financial industry in searching their records. The financial institutions must query their records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last 6 months. Financial institutions have 2 weeks from the posting date of the request to respond with any positive matches. If the search does not uncover any matching of accounts or transactions, the financial institution is instructed not to reply to the 314(a) request.

FinCEN began processing 314(a) requests in November 2002. This system was temporarily suspended, based on feedback from system users. Following extensive consultations, FinCEN issued FAQ's to implement and streamline the process and resumed operation of the system in February 2003. Since that time, as with any new system, the process continues to be fine-tuned. On March 1, 2005, FinCEN ceased notifying the financial industry with e-mail attachments and began posting 314(a) requests on a secure Internet site.

The Process

Through an expedited communication system, FinCEN's 314(a) process enables an investigator to canvas the nation's financial institutions for potential lead information that might otherwise never be uncovered. The focus quickly zeros in on relevant locations and activities. This cooperative partnership between the financial community and law enforcement allows disparate bits of information to be identified, centralized and rapidly evaluated. It is important to note, however, that Section 314(a) provides lead information only and is not a substitute for a subpoena or other legal process. To obtain documents from a financial institution that has reported a match, a law enforcement agency must meet the legal standards that apply to the particular investigative tool that it chooses to use to obtain the documents. To ensure that Section 314(a) inquiries are being used only for appropriate cases, FinCEN's Section 314(a) process requires law enforcement to provide assurances that the request has been subject to appropriate scrutiny at the agency level and that the matter under investigation satisfies FinCEN's standards for processing a formal Section 314(a) inquiry. FinCEN requires all requesters to submit a form certifying that the investigation is based on credible evidence of terrorist financing or money laundering.

Criteria for Money Laundering Requests

Because money laundering encompasses such a wide range of underlying criminal activity, agencies must determine that a money laundering case is significant before submitting a 314(a) request to FinCEN. To ensure that this standard is met, FinCEN requires documentation showing

the size or impact of the case, the seriousness of the underlying criminal activity, the importance of the case to a major agency program, and any other facts demonstrating its significance. In addition, law enforcement must certify in cases involving money laundering that all traditional means of investigation have been exhausted. The support for the assertion that other investigative alternatives have been exhausted or are unavailable must be provided in the form submitted to FinCEN for review prior to the request being submitted to financial institutions by FinCEN. To date, the 314(a) process already has proved to be successful, as illustrated below. Results have yielded productive leads for both terrorist financing and money laundering investigations. The immediate matches have, for example, led to the identification of new accounts, transactions, indictments, etc. and enabled law enforcement to efficiently direct its use of legal processes to promptly obtain critical evidence in numerous cases.

Examples of 314(a) requests, based on money laundering, include:

- Hawala operation involving a sanctioned country
- Arms trafficking
- Alien smuggling resulting in fatalities
- Cigarette smuggling
- Nationwide investment fraud with many victims
- International criminal network involved in identity theft and wire fraud
- Multi-agency investigation of drug trafficking rings

Appendix B – FinCen Section 314(b)

Section 314(b) Fact Sheet

What is Section 314(b)?

Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities. 314(b) information sharing is a voluntary program, and FinCEN strongly encourages information sharing through Section 314(b). What are the Benefits of 314(b) Voluntary Information Sharing? While information sharing under the 314(b) program is voluntary, it can help financial institutions enhance compliance with their anti-money laundering/counter-terrorist financing (AML/CFT) requirements, most notably with respect to:

- Gathering additional and potentially invaluable information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals.
- Shedding more comprehensive light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions.
- Building a more comprehensive and accurate picture of a customer’s activities where potential money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring.
- Alerting the contacted financial institution to customers about whose suspicious activities it may not have been previously aware.
- Facilitating the filing of more comprehensive and complete SARs than would otherwise be filed in the absence of 314(b) information sharing.
- Aiding in identifying and collectively stemming money laundering and terrorist financing methods and schemes.
- Facilitating efficient SAR reporting decisions - for example, when a financial institution obtains a more complete picture of activity through the voluntary information sharing process and determines that no SAR is required for transactions that may have initially appeared suspicious.

Who is Eligible to Participate in 314(b)?

Financial institutions subject to an anti-money laundering program requirement under FinCEN regulations, and any association of such financial institutions, are eligible to share information under Section 314(b). This currently includes the following types of financial institutions:

- Banks (31 CFR 1020.540)
- Casinos and Card Clubs (31 CFR 1021.540)

- Money Services Businesses (31 CFR 1022.540)
- Brokers or Dealers in Securities (31 CFR 1023.540)
- Mutual Funds (31 CFR 1024.540)
- Insurance Companies (31 CFR 1025.540)
- Futures Commission Merchants and Introducing Brokers in Commodities (31 CFR 1026.540)
- Dealers in Precious Metals, Precious Stones, or Jewels (31 CFR 1027.540)
- Operators of Credit Card Systems (31 CFR 1028.540)
- Loan or Finance Companies (31 CFR 1029.540)
- Associations consisting of the financial institutions listed above

What Information can be Shared Under 314(b)?

Under 314(b), financial institutions or associations of financial institutions may share information with each other regarding individuals, entities, organizations, and countries for purposes of identifying, and, where appropriate, reporting

For more information on the benefits of voluntary information sharing under Section 314(b), including examples of ways in which SAR narratives have referenced 314(b), see Issue 23 of the SAR

Activity Review – Trends, Tips & Issues at

http://www.fincen.gov/news_room/rp/files/sar_tti_23.pdf

In July 2012, FinCEN issued an administrative ruling which clarified the meaning of “association of financial institutions.” For more information, see FIN-2012-R006

(http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2012-R006.pdf)

Section 314(b) Fact Sheet

activities that may involve possible terrorist activity or money laundering. FinCEN has issued guidance clarifying that, if 314(b) sharing participants suspect that transactions may involve the proceeds of specified unlawful activities under money laundering statutes, information related to such transactions can be shared under protection of the 314(b) safe harbor.

In cases where a financial institution files a SAR that has benefited from 314(b) information sharing, FinCEN encourages financial institutions to note this in the narrative in order for FinCEN to identify and communicate additional examples of the benefits of the 314(b) program. Please note, however, that while information may be shared related to possible terrorist financing or money laundering that resulted in, or may result in, the filing of a SAR, Section 314(b) does not authorize a participating financial institution to share a SAR itself or to disclose the existence of a SAR.

How do Financial Institutions Participate in 314(b)?

While FinCEN encourages 314(b) information sharing due to the many benefits of the program, financial institutions may voluntarily choose whether or not to participate. FinCEN regulations (31 CFR 1010.540) set forth the requirements that must be satisfied in order to benefit from 314(b) safe harbor protection, as outlined below. Sharing information without satisfying these conditions does not by itself subject an institution to penalty under FinCEN regulations, since 314(b) participation is voluntary; however, a financial institution will only benefit from the safe harbor protection if it follows the conditions for participation in the program:

1) Submit a Notification to FinCEN Information regarding the 314(b) notification process, including on-line notification, is available on FinCEN's website (http://www.fincen.gov/statutes_regs/patriot/section314b.html). Financial institutions or associations of financial institutions interested in participating in the 314(b) program must complete and submit a 314(b) notification. All notifications are processed within two business days of receipt, and participants will receive an acknowledgment via e-mail.

Specified unlawful activities listed in 18 U.S.C. § § 1956 and 1957 include an array of fraudulent and other criminal activities. For more information, see FIN-2009-G002 (http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-g002.pdf).

SAR confidentiality standards are governed by applicable SAR regulations. See, e.g., 31 CFR 1020.320. October 2013 Section 314(b) Fact Sheet

Sharing information with other 314(b) participants

Prior to sharing information under 314(b), financial institutions must take reasonable steps, such as checking the FinCEN 314(b) participant list, to verify that the other financial institution has also submitted a notification to FinCEN.

To facilitate the identification of 314(b) program participants, the notification acknowledgement will contain details of participation as well as the link and information required to access the most recent 314(b) participant list. FinCEN updates the list on a daily basis. Financial institutions may establish policies and procedures that designate more than one person with the authority to participate in the financial institution's 314(b) program.

3) Safeguard Shared Information and use only for AML/CFT Purposes

Financial institutions and associations must establish and maintain procedures to safeguard the security and confidentiality of shared information, and must only use shared information for the purpose of:

- Identifying and, where appropriate, reporting on activities that may involve terrorist financing or money laundering;
- Determining whether to establish or maintain an account, or to engage in a transaction; or
- Assisting in compliance with anti-money laundering requirements.

Updating Point of Contact Information and Additional Resources