Introduction

During a 2004 Congressional testimony regarding U.S. efforts to combat money laundering, Karen Tandy, former Administrator of the Drug Enforcement Administration, stated;

> *"The motivation for virtually everyone involved in illegal drug trafficking, from kingpin to street dealer, is the money. To make a significant impact on the drug trade in America and around the world, there is no strategy more effective than following the money back to the sources of drug supply and taking away the dirty proceeds of that trade* (Tandy 2004)."

Since then strides have been made to counteract drug trafficking by targeting the finances of criminal enterprises. The capture of the drug kingpin, *El Chapo,* and the seizure of his assets, as well as coordination between U.S. and Mexican federal agencies in operations such as the Merida Initiative or Project Coronado are examples of successful government interdiction into the monetary aspects of the drug trade. However, the events of 9/11 and subsequent bombings around the world have sparked pressure for the U.S. government to focus financial investigative resources on terrorist financing. In effect, the regulation of financial institutions has been severely lacking as is evidenced by recent cases involving large commercial business such as HSBC and Wachovia. Because of these deficiencies, Drug Trafficking Organizations (DTOs) are able to finance operations without detection and continue the spur of violence along the Mexican border that is spilling into the U.S. However, violence is not the only threat our country faces. When DTOs are able to "launder" funds by exploiting gaps in the U.S. anti-money laundering framework they undermine legitimate financial sectors and weaken financial institutions. This ability is arguably because there are remaining vulnerabilities within the government, public, and financial spheres in regards to money laundering. In order to not only defend the U.S. financial sector from these threats but also reduce the power of DTOs, modern money laundering methods

must first be understood so that vulnerabilities within U.S. anti-money laundering policy can be identified and proposed changes can be made.

The Money Laundering Cycle

Money laundering can be defined as the process of concealing the existence, illegal source, or application of income derived from criminal activity, and the subsequent disguising of the source of that income to make it appear legitimate (FATF 2005). Criminals use this process to conceal the origin of accumulated assets in order to prevent prosecution from law enforcement. If federal agencies investigating these crimes were able to accurately trace the origin of assets acquired by criminal enterprise then they could not only build a case against these groups, but also strategically target the flow of cash to disrupt the operations of their operations. Thus, it is in the best interests of these individuals to hide the origins of funds in order to prevent law enforcement agencies from both discovering and tracking their financing.

While money laundering comes in many different forms, typical methods can be broken down to three basic steps: placement, layering, and integration. The combination of these three steps is commonly referred to as the money laundering cycle.

This process typically begins with the consolidation of funds from various illicit activities to a “cash house,” which is used to store the physical currency known as “dirty” money. Cash houses are usually located in large cities such as Dallas, Atlanta or Chicago at the geographical center of the subsidiary drug dealers to make the consolidation process easier (Farah 2011). Also, by storing the currency in one location, the risk of a large sum of money being discovered or lost is minimized. It is important to note that these cash houses never cross paths with any other facet

of the criminal enterprise. This limits the damage to the organization in case one location is seized by authorities.

Cash houses also serve as a currency transfer vehicle when converting small bills into larger ones. Most dealers receive payments in small amounts such as $1 or $5 bills. Two problems are associated with this denomination of payment. The first issue is the weight that is involved with amounts of this size. While the average person does not live their life concerned with their wallet weighing them down, this is a very big problem for money launderers. One pound of currency is the equivalent of 450 dollar bills. Therefore, $1 million worth of currency in dollar bills would weigh more than one ton. The second issue is the suspicion that would arise when making a large deposit in such small amounts. Under the Bank Secrecy Act of 1970 (BSA), banks are required to report any activity related to a deposit they find suspicious to the authorities (BSA 1970). According to the Financial Crimes Enforcement Network (FinCEN), the "frequent exchange or deposit of small bills for larger ones" is an identifier of potential money laundering activity (FinCEN 2003). While it could be argued that there are legitimate reasons for making a deposit in that denomination of currency, most dealers would rather avoid the risk.

Transforming the currency from small size bills to larger ones requires legitimate businesses that receive those forms of currency on a daily basis. Examples include restaurants, bars, hotels, casinos, car washes, vending machine companies, or laundromats. These businesses can exchange this amount of currency for larger bills and thus the first step in disguising the currency is complete.

Placement

Once stored in a more portable form, the manager of the cash house will begin with the placement of funds into circulation of the financial system. This step is achieved most commonly by creating a bank account under the $10,000 limit that is required to be reported by the BSA. This process serves two purposes: 1) it once again further eliminates the need to hide large sums of bulk currency; and 2) it provides easier mobility of the funds. Once within the system, wire transfers, cashier checks, or money orders provide a much more manageable means of transportation. It could be argued that this stage is the most important due to the difficulty in being able to conceal such a large injection of cash through a financial institution.

In order to overcome the $10,000 limit when making cash transactions criminal organizations will initiate multiple payments through the use of "*smursf.*" Smurfs are representatives who conduct legitimate financial transactions at the request of a criminal enterprise such as opening numerous checking accounts in the U.S. using real or fictitious names (ACAMS 2003). The BSA reporting requirement only applies to a $10,000 transaction within one business day. It would be difficult as well as suspicious for one employee to constantly deposit or transfer amounts consistently below that threshold all on their own. Through "structuring", breaking proceeds into multiple deposit sums, transactions with financial institutions avoid being reported (ACAMS 2003).

Layering

Once concealed within the financial system, the next step is to transform the funds to make them appear legitimate. This process, known as layering, requires multiple financial transactions in order to disguise the origin of funds and obscure the audit trail. In this stage

“dirty” cash is comingled with legally acquired business proceeds through different “fronts” to appear “clean ” (Farah 2011). Fronts are legitimate businesses that usually engage in daily transactions involving a large amount of cash and can be owned or not owned by criminal enterprises (ACAMS 2003). Examples of these transactions include wire transfers, offshore investments, or the resale of goods. When conducting these transactions, launderers must ensure they are complex enough to not be easily traced. This step involves the exploitation of loopholes within both judicial and legal portions of the governments in which funds are being moved.

Successful layering requires combining a vast quantity of financial transactions with a certain quality pertaining to banks. When selecting the banks to transfer funds, it is crucial to select those banks in countries with less stringent bank secrecy laws. Because banks in these countries are not required to report as much information about their customers, investigation becomes more difficult or too costly for law enforcement to identify the transaction when needed. Also, the types of transactions a DTO selects must be complex enough to withstand ordinary scrutiny. Shifting funds between banks conceals the funds but not as much as moving the money through various asset types, which incur costs for buying and selling. There must be a combination of both types in order to complete the layering process. Constantly moving funds from bank to bank further obscures the audit trail and requires law enforcement to conduct a much more extensive investigation as the money is being moved. By the time investigators have fulfilled the necessary legal process to subpoena a bank, the money has usually already moved on to a different location.

Integration

The final stage of the money laundering cycle, integration, involves returning the funds to the designated recipient through legitimate means. Examples include the purchasing of big ticket items or business investments through the use of "*shell companies*" (Sullivan 2015). At this stage the dirty money is indistinguishable from legally acquired funds and can be used by the recipient to purchase whatever they desire.

Scope of the Problem

In recent years this cycle has been accommodated by the increased size of the global financial system. In 2009, the UNODC estimated that the total amount of money laundered was around $1.6 trillion or 2.7 percent of global Gross Domestic Product (GDP) in 2015, that number rose to $2 trillion or 3 percent of global GDP (UNODC 2015). This jump can be attributed to the advances in financial information, technology and communication that allow institutions to operate much more efficiently. Today, a vast array of products and services are offered to customers all over the world which creates a complex, dynamic environment in which investors, both legitimate and illegitimate, are constantly initiating multiple transactions each day. Thus, monitoring the financial system for money laundering becomes all the more difficult.

This process has proven especially true in a nation as advanced both financially and technologically as the United States. The UNODC estimated that proceeds from all forms of financial crime in the United States, excluding tax evasion, was $300 billion in 2010, or about two percent of the U.S. economy. Of this amount, $264 billion was attributed to forms of fraud while $64 billion was related to drug proceeds (UNODC 2015).

While fraud constitutes a greater dollar amount of money laundering in the U.S., the threats of Drug Trafficking Organizations (DTOs) that effectively conceal and inject their drug

profits into the financial system prove a greater threat to the US. While drug use has declined by one-third since the *"War on Drugs*" was declared, the power of the Cartels that continue to supply the drugs has not. In 2011, the National Drug Intelligence Center (NDIC) found that Mexican DTOs "dominate the supply, trafficking, and wholesale distribution of most illicit drugs in the United States (NDIC 2011)." While there are other DTOs who operate within the U.S. such as Colombia and those headquartered in South American countries, none impacts the U.S. drug trade as much as Mexican-based traffickers. Their dominance stems from their control of smuggling routes across the U.S. southwest border and their capacity to produce, transport, and distribute many forms of drugs (NDIC 2011).

The Success of DTOs can also be attributed to their ability to launder money without detection. John Cassara, a former Treasury agent and an anti-money laundering expert, explains that we should be most concerned with how few U.S. drug proceeds are captured by authorities. He writes:

> *"The Office of National Drug Control Policy estimates that Americans spend approximately $65 billion per year on illegal drugs. Yet according to the Drug Enforcement Administration (DEA), only about $1 billion is seized per year domestically by all federal agencies combined. The approximately 1.5 percent successful seizure rate is actually even more depressing because identifying bulk cash related to drugs is probably the most straight forward anti-money laundering investigation. So we can infer the seizure rate is much worse for other kinds of money laundering in the United States that collectively total in the hundreds of billions of dollars* (Cassara 2009)."

While the exact amount of drug proceeds that are allowed to flow through the financial system is unknown, The National Drug Intelligence Center estimates that Mexican and Colombian drug trafficking organizations "…annually generate, remove and launder between $18 billion and $39 billion in wholesale distribution proceeds (NDIC 2011)."

Methods

Bulk-Currency Smuggling

To launder such a large amount of money, DTOs employ a variety of laundering methods, most common of which is the act of bulk currency smuggling. This method is most closely associated with the placement phase. Before funds can be injected into the financial system they must be consolidated under one cash house so that deposits can be made either in the U.S. or in some other foreign country. Specifically, bulk currency smuggling involves physically moving hidden amounts of cash and monetary instruments in excess of $10,000 into or out of the United States without filing a Report of International Transportation of Currency or Monetary Instruments (CMIR) with U.S. Customs and Border Protection (CBP) (Sullivan 2015). In a paper by Celina Realuyo, a professor of practice at the National Defense University, she stated, "Cash remains the preferred payment method by criminal enterprises across the globe, including the Mexican cartels." This form of money laundering is necessary not only to obtain profits (ultimate goal of DTO's) but also to move operating funds (their source of power and impunity) (Realuyo 2012) .

It helps to consider the drug trade as a pipeline that flows from South America (where drugs are made), through Central America and Mexico then ultimately into the United States. Along this pipeline are smaller feeder lines that inject cash profits from illicit activities south towards the kingpins who run the entire organization. In return, the pipeline distributes a portion of funds for operating expenses in the form of physical currency to various employees or third parties along the way.

While the concept seems simple, the actual techniques employed by DTO's are anything but. In Sylvia Longmire's book, *Cartel,* she said, "If there's one thing in Mexico's drug war that is constant, it's change (Longmire 2015)." This statement holds especially true for money laundering. The smuggling of bulk currency centers on the adaptation of current investigative techniques to avoid seizure at the border or certain storage facilities. Revisiting the pipeline example, authorities try to establish a cutoff point or "bottle-neck" to stem the flow of both drugs and funds (Farah 2011). The genius of the DTO's is their ability to redirect their pipeline at will in order to keep the organization flowing.

In a paper on the Merida Initiative by the Woodrow Wilson International Center for Scholars, the entire process of smuggling bulk currency is described in detail. First, DTO's consolidate their illicit funds, in the form of cash, to one of the several regional cash houses in major cities. As stated earlier, the money is converted from smaller bills into $100 or $50 bills to reduce the size of the currency needed to transport. The cash is then vacuum sealed in plastic bags and distributed into hidden compartments used as "*crossing vehicles*." These vehicles are constantly rotated and carry only a finite amount (usually around $100,00 or $50,000) in-case they are seized by authorities during transport. They are redesigned specifically for concealing large amounts of currency within compartments throughout the car. At the border, the schedule of crossing is dictated by the amount of traffic or security at a particular crossing point. Those in charge of this schedule are known commonly as *halcones* or hawks. *Halcones* are distributed across the entire border employing a vast array of satellite technology, voice over Internet Protocol, and encrypted messages to communicate with their associates. Authorities have reported cases in which the technology of these individuals is more advanced than the equipment of border patrol agents (Farah 2011). This is just one example of DTO's knowing what to invest

in to stay a step ahead of law enforcement. Meanwhile, authorities at this point have the task of inspecting traffic and personnel both entering and exiting the U.S.

Transportation screening, as defined by the Department of Homeland Security, is determined by the process of “risk management.” Because of the massive amount of vehicular border crossings per day, almost 700,000 according to CBP, resources can only promote a finite amount of searches at a given location. This percentage usually falls around 10% of vehicles crossing, and is dictated by the cars and areas authorities believe present the greatest risk. Knowing there is a lack of security along the border, *halcones* communicate to the transportation teams the areas with the least amount of risk each day in order to prevent their vehicles from falling within that 10% criteria. In the risk of capture, many drivers will either try to turn their cars around or simply walk out to blend in with the crowd on foot. A border patrol agent has said that DTOs are willing to lose 2 out of every 10 cars. The $100,000 to $200,000 lost as a result is simply an operating expense and does little to affect the organization (Farah 2011).

Stored-Value

While the transportation of bulk currency will always be a concern, the increasingly popular use of stored value is becoming more prevalent. Stored value involves the use of any item that contains a liquid amount such as credit cards, gift cards, or traveler’s checks. Currently, there are no cross border requirements in regards to stored value items. This lack of regulation not only means that smugglers can cross with unlimited amounts of stored value cards but they are also not subject to the same $10,000 limit that is reported for cash. Another use of these cards is their ability to transfer currency from dollars to pesos with relative ease. For example, a

smuggler could purchase a debit card in the U.S. for cash, carry that card across the border and simply withdrawal pesos from the nearest ATM once in Mexico.

Money-Service Businesses

The final bulk currency smuggling method used by DTOs involves the exploitation of Money Service Businesses (MSBs). MSBs are institutions outside of banks who offer cash related services such as check cashing, issuing traveler's checks, or transmitting money. These services can come in the form of wire, fax, draft, check, or courier, and exist expressly for the purpose of allowing people who are unable to use the traditional financial institutions as a means to transfer money. Examples of such businesses include the U.S. Postal Service, Western Union, American Express, Travelers Express, and MoneyGram. However, unlike stored value items, MSBs are fairly regulated. The following two regulations, according to the U.S. Treasury, limit the ability to use MSBs for large cash transactions:

- *For transactions conducted at a money service business, a $2,000 ceiling applies.*
- *For transactions conducted by issuers of money orders from a review of clearance records of orders sold or processed, a ceiling of $5,000 applies.*

While MSBs are rarely used to launder large amounts of currency they remain a common tool for low level employees. These employees usually conduct operations within the reporting thresholds and view MSBs as a very useful way to withdraw cash when needed.

These types of institutions also exist outside of the U.S. *Casas de Cambrios* are Mexican exchange facilities that enable the remittance of international payments to individuals or companies. The difference between MSBs in the U.S. and Casas de Cambrios is the amount of

federal regulation imposed by the Mexican government. Mexican regulators do not impose as strict reporting requirements and thus are used more often by DTOs.

Banking System

More complex than laundering bulk currency, and more popularly reported on, are techniques which exploit the financial system. After the placement phase, funds are ready to be layered so that they are further distanced from their origin. Layering is most commonly done by shuffling currency through services or products offered by financial institutions such as banks or MSBs. The National Money Laundering Risk Assessment (NMLRA) estimates that almost half of all proceeds from drug trafficking are placed into the financial system.

U.S. banks serves as favorable vessel to inject funds into the financial system without detection. There are almost 13,000 U.S. depository institutions that operate within a diverse variety of business models of which almost half are banks. U.S. banks are most susceptible to risk due to the amount of dollar, denominated deposits they conduct daily. Because of the soundness of the dollar it is a preferred method of payment not only to DTOs but to businesses across the world, making it very feasible for business transactions. The Federal Reserve System's real-time gross settlement system, Fedwire, which is used to clear and settle payments with immediate finality, processed an average of $3.5 trillion in daily funds transfers in 2014. (Fedwire 2014).

Correspondent Banks

Much of the funds that are transferred throughout the financial system are done so through the use of correspondent banks. These banks establish relationships with "respondent

banks," which are foreign banks with no physical presence in the host country of the correspondent bank. These relationships are essential to the function of the U.S. and international financial system, facilitating everything from remittances, trade finance, and economic development. However, because of the complexity of correspondent account relationships, multiple intermediary financial institutions may be involved in a single funds transfer transaction. Correspondent Banks in the U.S. for example interact with thousands of different respondent banks across the globe. In order to offer customers services that involve their host country, these banks engage in business with the correspondent bank. Many of these respondent banks are in countries with little global presence or a weak economy such as Mexico or other South American states.

Correspondent banks are required to verify the anti-money laundering programs of respondent banks, but they are not always able to verify their customers. As stated earlier, respondent banks are many times located in countries with weak economic growth. Because economic growth is not thriving in these parts of the world, banks are not heavily inclined to deny customers when presented with the chance of doing business; even if it means they must forgo conducting the accurate background checks.

One of the many services these banks offer are wire transfers. Wire transfers are an electronic fund transfer from one person or entity to another. In the context of money laundering, these transactions most commonly involve the transfer of funds between financial institutions. Because the conduction of wire transfers are almost immediate, they are much more desirable for DTOs than the transportation of bulk currency. Many times DTOs will conduct wire transfers from a U.S. bank, where they have structured funds, to a foreign bank account. The country in which funds are sent will most likely be one with very few bank secrecy laws. These "offshore"

accounts are very difficult to track since banks do not have to report as much as those in the U.S. Once DTOs believe the audit trail of the funds are misconstrued enough, the funds need to be transported to their ultimate destination.

Shell Corporations

Key institutions used for the integration phase are shell companies. A shell company is a legal entity that is state registered but has not been used for any profit generating function. Shell companies can serve legitimate purposes; for example, holding property rights or financial assets. Most companies technically begin as shell companies until they are put to operational use. Shell companies can also be used to conceal the source, ownership, and control of illegal proceeds. Specifically, they conceal the identity of the beneficial owner of the funds.

Thus, the records of transactions are often more difficult for law enforcement to access because they are offshore or held by professionals who claim secrecy, and the professionals who run the company act on instructions remotely and anonymously (Sullivan 2015). For example, in 2007, two men in Colorado, who were charged with drug trafficking allegedly opened bank accounts, made structured cash deposits to the accounts, and used nominees to facilitate large purchases. According to the indictment, the defendants regularly brought cocaine into the United States from Mexico for distribution in Colorado, Texas, Georgia and elsewhere, earning more than $15 million. The defendants used straw buyers in Denver to acquire cars and applied for home loans listing a co-conspirator’s business as their employer on the mortgage applications (NMLRA 2015).

Trade Based Money Laundering

A third major money laundering technique is known as Trade-based money laundering (TBML). TBML is defined by the Financial Action Task Force as follows:

> *The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity, or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail* (FATF 2005).*"*

TBML is a less known money laundering technique that authorities are still trying analyze. Because the actual process has not been systematically examined on a global scale, the amount of money laundered through the commerce system is unknown. However, some experts argue that it is the largest money laundering method used in the United States today (Cassara 2009).

In simple terms TBML involves the purchase of goods through a legitimate supplier to disguise currency as products of value. These goods can then be shipped across borders and act as payment to complicit businesses or resold back into usable currency. The benefit is the simple explanation to authorities when crossing the border. Shipments of legitimate goods beyond the border pose less suspicion to the authorities since there are no laws broken within the most crucial portion of the process.

One of the key aspects of TBML, is the over and under invoicing of goods for profit. This involves the falsification of documents related to the goods so that their value is either increased or decreased relative to their actual price. For example, a money laundering facilitator can value exported goods as $200,000 when they are actually worth $100,000. The recipient of those goods will then pay $200,000 to the sender which includes a $100,000 payment to the sender on top of the goods' actual value. Such a transaction allows for the settling of debts between those engaged in illicit activities. The same can be done in reverse by under-invoicing the true value of the

traded good. If one party sends $500,000 worth of a commodity but lists the value at $200,000 on the invoice and is paid that amount by the recipient, they have effectively transferred $300,000 to the recipient (U.S. Senate 2013) . .

Another version of TBML is the Black Market Peso Exchange (BMPE). The BMPE is used more by Columbian drug traffickers but its growth through the years has led to fears that it will be permanently adopted by their Mexican counterparts. For years the BMPE has allowed DTOs who operate within U.S. borders to pay suppliers in Columbia. It was originally invented to avoid high tariffs between the two countries but has since been adopted to conduct money laundering operations. An example of how the BMPE works is when a money broker in the United States accepts the drug dollars from a U.S.-based agent and then provides Colombian pesos to the supplier in Colombia through Colombian merchants seeking to import U.S. goods. The agent then uses the drug dollars to purchase those goods and ships them back to Colombia.

Anti-Money Laundering

To counteract the preceding methods the U.S. government promotes multiple federal resources towards anti-money laundering tactics. Anti-money laundering is centered on two motives, prevention and investigation. Prevention is a combined effort between the federal government and financial institutions s to deter money laundering practices in the U.S, while investigators ensure that companies are complicit with current regulation and also build evidence for anti-money laundering cases.

Regulation

Bank Secrecy Act

The first and most effective piece of legislation to counteract money laundering in the U.S. was the Bank Secrecy Act of 1970 (BSA). The BSA requires all banks and financial institutions to keep records ensuring the details of financial transactions that could be traced by investigators if needed (BSA 1970). As mentioned earlier, this act also requires the reporting of any cash transaction in excess of $10,000 to be reported in a Currency Transaction Report (CTR). A CTR is filed with the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) and must be kept on file for a minimum of five years. Examples of financial institutions listed within the act aside from banks include; brokers, dealers, MSBs, and Casinos.

Aside from the $10,000 filing requirement, these institutions are also required to implement an anti-money laundering program (AMLP) within all financial facets of their operations. Section 1010 states,

> *"A covered financial institution shall establish a due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to enable the covered financial institution to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by such covered financial institution in the United States for a foreign financial institution.*(BSA 1970*)"*

Other specific duties required by the BSA include the designation of a compliance officer, an employee training program, and independent audits of the AML to ensure efficiency.

FinCEN

FinCEN was created in 1990 to support federal, state, local, and international law enforcement by analyzing the information required under the Bank Secrecy Act (BSA),Their mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial

intelligence and strategic use of financial authorities. They are modeled most closely after the Financial Action Task Force, which set the tone for anti-money laundering standards in Europe for decades. The creation of an organization centered around the investigation of money laundering proved the seriousness of the issue and the commitment the U.S. is willing to make in the fight against these forms of crime.

Patriot Act of 2001

The Patriot Act of 2001 was created in response to the terror attacks of 9/11. The main goal of this act was to deter and punish terrorist acts in the United States and around the world, and to enhance the capabilities of law enforcement investigatory tools. While the act was designed to combat terrorist financing, there are portions of the act that apply to preventing laundering by DTOs as well. This portion of the Patriot Act is known as the "International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001." Important sections that pertain to the regulation of financial institutions include the following:

Section 311: *Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern*

This section gave the Secretary of the Treasury the power to "require any domestic financial institution or domestic financial agency to maintain records, file reports, or both, concerning the aggregate amount of transactions, or concerning each transaction… for such period of time, as the Secretary shall determine." Now customers are more easily identified through their accounts within correspondent banks (USA Patriot Act 2001)

Section 312: *Special Due Diligence for Correspondent Accounts and Private Banking Accounts*

Similar to section 311 this section also imposed stricter regulation on bank's management of correspondent accounts. Specifically banks must exercise "due diligence" in identifying the owners or operators of a foreign bank account before doing business with such banks(USA Patriot Act 2001).

<u>Section 313:</u> *Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks*

As stated earlier shell banks remain "the vehicle of choice for money launderers, bribe givers and takers, sanctions busters, tax evaders and financers of terrorism." This section prohibited financial institutions from "…establishing, maintaining, administering, or managing a correspondent account in the United States for, or on behalf of, a foreign bank that does not have a physical presence in any country." In order to establish a physical presence the shell company must be maintained by a foreign bank, reside at a fixed address, and employ at least one full-time worker who maintains operating records related to banking activities. While this act is important in deterring the use of electronic shell companies as vessels for fund transmittals it is important to note that this act does not require the listing of the beneficial owners involved in a such a company. This omission means that the operator of a shell company does not have to be listed in order to conduct legal transactions (USA Patriot Act 2001).

<u>Section 352:</u> *Anti-Money Laundering Programs*

This section requires financial institutions to establish anti-money laundering programs, which at a minimum must include: the development of internal policies, procedures and controls; designation of a compliance officer; an ongoing employee training program; and an independent audit function to test programs (USA Patriot Act 2001).

Financial Institutions and AML Programs

As stated earlier, regulatory agencies within the federal government are not the only ones who play a role in the prevention of money laundering. Because financial institutions are themselves used as vessels for concealing funds within the financial system they are required to implement measures to deter the use of their products and services for such illicit gains.

The AML program within a financial institution is commonly referred to as the compliance or risk department. The main mission of this portion of the company is to prevent and deter money laundering as well as terrorist financing. By interpreting the policies required through the Patriot Act, these institutions establish procedures while simultaneously coordinating with law enforcement to identify any potential suspicious activity.

Section 352 of the Patriot act requires the implementation of an anti-money laundering program for specific financial institutions and at a minimum these programs must provide what are commonly referred to as the four pillars of an AML program:

- Training
- Designated Compliance officer (DCO)
- Independent audit function
- Internal policies and procedures

(USA Patriot Act 2001). A company's AML program is only valid so long as it is followed by its employees. This reality requires the education and training for all company employees in modern money laundering tactics as well as the actual details of the AML program

that a company has instilled within its policies. A company's employees should know what to do if potentially suspicious activity is identified and how to handle it.

This training should be overseen by the DCO that companies are required to have. A DCO must ensure the company abides by its own policies as well as the policies required by federal regulation. The DCO must be knowledgeable in all aspects of the BSA and possess sufficient authority to enact the requirements of such an act.

The DCO should ensure that a company is abiding by these policies with an independent audit function. The success of an AML program must be properly assessed either internally or outsourced to a third party. Many companies conduct this audit along with their financial statement and control audit required by Sarbanes Oxley.

The final and most important part of an AML program encompasses its stated policies and procedures. The three aforementioned portions of an AML program essentially revolve around whatever policies a company has decided to implement. Here, a financial institution lists all the products, locations, and customers that have exposure to money laundering vulnerabilities. Thus, the policies will differ among companies depending on size, location, and services. These policies should be in written form so that investigators and customers alike can be sure that a corporation is conducting itself within the federal anti-money laundering regulation. Much like the investment branch of a corporation this list is quantified based on the notion of risk. The policies and procedures must address these risks and provide solutions on how the company will identify, analyze, manage, and review any specific transactions that would include suspicious activity.

Once analyzed, a corporation should direct its AML resources to the areas perceived to contain the most risk. This can be done by using a risk matrix; in which a weight is given to a particular ranking of risk and then multiplied by whatever score that particular sample is given (Sullivan 2015). As stated earlier the matrix should focus on three aspects of the company: products, locations, and customers.

Both product and location considerations are rather simple. Financial institutions should have a vast knowledge of their own products as well as what countries do businesses with them. Thus, because they have so much information on these aspects of the business an accurate risk matrix can be formed.

The hardest part of any AML program, and the most essential, is quantifying the risk associated with one's customer. Due to the vast array of customers to whom many large financial institutions provide services, there is very rarely any customer relationships upon which a bank could intimately report. Very few banks have the resources to accurately keep track of all customers and their behavior. Thus, the asymmetric information that revolves around a bank and many of its customers makes knowing their business intentions quite difficult

This has led many businesses to install what is known as a Know Your Customer program (KYC) as a part of their AML criteria (Sullivan 2015). KYC programs focus on customer identification, due diligence, and when necessary, enhanced due diligence.

Customer identification begins at the onset of the relationship. When a transaction or potential transaction is about to begin, a financial institution must record and identify proper information associated with the customer. Much of this information is the same information a

company would require for a transaction in the first place; name, address, date of birth, identification number etc.

Once a company has acquired the basic information about a customer, they should begin a preliminary background check. This check is known as conducting due diligence, and is a requirement listed within section 352 of the Patriot Act. When gathering intelligence on a customer, a company does not have to identify that the information found is accurate but rather obtain certain that the identity of the customer is reasonable ensured.

Finally, a company should perform enhanced due diligence when there is a trigger event that is deemed suspicious. When a trigger event occurs, a company must decide to either further investigate the issue or close the account and identify the authorities.

Investigation

The investigation of money laundering requires coordination among both federal law enforcement and financial institutions. Both groups must assemble sufficient data to show that a transaction was conducted to hide illicit funds and then trace those funds to the original depositor as well as the source. As stated earlier, enhanced due diligence is performed after the onset of a suspicious event. This suspicion can arise from a multitude of factors. Most importantly, the use of the risk matrix described above should alert a company of any out of the ordinary transactions. The specific action that companies must take is the filing of a Suspicious Action Report (SAR) with the authorities.

A SAR alerts law enforcement of potential money laundering activity and is the initial starting point for their investigating process. Kevin Sullivan, former head of the FBI's Financial Crimes Division in Manhattan, stated that he and his team were in the "…unique capacity to

read, examine, and analyze SARs from every financial institution…almost 4,000 SARs each month." He also says that "Writing a complete and throughout SAR becomes one of the most important functions that a financial institution can perform. A SAR should be clear and provide any information that pertains to the subject; even if may not seem useful (Sullivan 2015) ."

After being filed, SARs are sent directly to FinCEN which categorizes and reviews the data to create a statistical database for law enforcement. This way, law enforcement can draw from the database the specific information they need to build cases against potential money laundering criminals.

Once law enforcement decides that a particular SAR is of interest to them, they will begin their due diligence. To obtain evidence, investigating officials will order a subpoena or summonses. These documents order the relevant financial institutions to provide information to investigators regarding the case. It is important to note that this process can be somewhat difficult in countries with many bank secrecy laws. If a country does not require companies to hand over information, they may be reluctant to do so. Another obstacle for investigators is the time it takes to fulfill the legal process of securing a subpoena. The average turnaround time from the date of a request to the date the information is sent is usually somewhere between two to six weeks depending upon the size and scope of the financial institution and the requested information. Once this information is collected, it is given to either state or federal prosecutors so that case may be filed against the either the individuals, organizations or financial institutions who are engaged in the facilitation of money laundering.

When it comes to DTO's law enforcement can also take a more direct approach to fighting organized crime. Most cases involve the collection of evidence insinuating there has

been involvement within money laundering or other illicit activities. However, both U.S. and Mexican law enforcement officials have enacted programs designed specifically to disrupt the flow of funds for drug cartels and their leaders.

One of the primary examples of an act that specifically targeted DTOs was the MeridaIinitiative. The Merida initiative was a $1.7 billion dollar joint program launched by the U.S. and Mexico in 2007. The four goals were to 1)disrupt organized crime groups 2)institutionalize reforms to sustain the rule of law and protect human rights 3) create a twenty first century border and 4) build a strong and resilient community capable of deterring involvement of its citizens in DTOs. Other specific aspects of the program involved training to strengthen the institutions of justice, helping to vet new police force members, creating new offices to handle citizen complaints and promote professional responsibility, and establishing witness protection programs. The program has also supported efforts to reduce the demand for drugs, fight corruption, and enhance Mexico's ability to the border.

Proposed changes

While the framework described above makes the process of money laundering more difficult and costly, there are still gaps that need to be addressed. In an attempt to address these vulnerabilities the following changes should be considered.

Regulatory and Financial Institutions

As discussed earlier, DTOs are increasingly using items of stored value to transport their funds from the U.S. into Mexico. To combat this threat, regulatory agencies should institute a cross border requirement for items of stored value. This requirement should be set at the $10,000

dollar limit to reduce the ability of DTOs to transport currency using extremely liquid and transportable objects.

Regulatory agencies should also enact heavier requirements for shell corporations. Before these companies can conduct business with U.S. financial institutions, they should have to report the beneficiaries or contributors of any profits earned or transactions that are conducted. This would make the investigation process much easier while also increasing the effectiveness of KYC programs.

These agencies should also enact more research for less understood money laundering methods such as TBML or the use of virtual currency. Because of the rapid advancements in technology DTOs are constantly searching for the most efficient and discreet way of laundering money. In order to most effectively neutralize the threat of money laundering, modern methods must be understood, measured, and analyzed .

As for financial institutions, their goal should be increased focus on KYC programs as well as filing more detailed SARs. Companies should adapt the due diligence aspects of their KYC programs to the potential amount of risk within their business environment. Many companies use methods suggested by the government which either do not pertain to their customers or do not encompass the full scope of risk that their company is involved in. This also applies to the use of SARs when enacting due diligence upon customers. Any portion of specific activity that would be useful to law enforcement should be included rather than filling out the bare minimum.

Finally, management must be held accountable for the effectiveness of their AML programs. Much like the imposition of Sarbanes Oxley, any company found not in compliance

with the Patriot Act or relevant regulation should be submitted not only to financial recompense but also possible criminal charges brought against managers who turned a blind eye to gaps within their AML programs.

Investigation

Currently, there is not a measurement process in place to quantify the success of investigation programs against DTOs. In order for regulatory agencies to accurately assess whether or not programs have a direct effect on performance indicators law enforcement must have a consistent measurement tool that can be compared for each investigative initiative. This means focusing on outcome-based measures rather than just output measures. This would allow both the U.S. and Mexico to assess what changes should be made to programs such as the Merida initiative.

Conclusion

So long as there are people in the U.S. willing to do drugs there will exist an environment in which DTOs are able to profit. Once earned, this money will be used to either further develop the operations of DTOs or contribute to the wealth of cartel kingpins. The main methods employed to conceal these funds from detection by the U.S. and Mexican governments include; forms of bulk currency smuggling, exploitation of financial institutions and trade based money laundering. The detection of all of these methods are made more difficult because of the size and sophistication of the U.S. financial system. Thus. there must be a coordinated effort by regulatory agencies, financial institutions and law enforcement to continuously improve their anti-money laundering policies to identify and prevent money laundering by DTOs. While their

capabilities can never be eliminated while drug use flourishes in the U.S. it can be mitigated by securing gaps within the financial system.

References

Association of Certified Anti-Money Laundering Specialists Exam Preparation Guide. (2003).

Bank Secrecy Act 1970, §§ 31-5311-5322 (United States Government Publishing Office 1970).

The Buck Stops Here, S., United States Senate Caucus on International Narcotics Control Cong. (2013).

Casserra, J. (2009, March 5). Back to Basics. Retrieved from http://www.johncassara.com/index.php?option=com_content&view=article&id=10:back-tobasics&catid=2:articles&Itemid=8

Farah, D. (2011). *Money Laundering and Bulk Cash Smuggling: Challenges for the Merida Initiative* (Rep.). Washington, DC: Woodrow Wilson Society for International Scholars.

Fedwire® Funds Service - Monthly Statistics. (n.d.). Retrieved from https://www.frbservices.org/operations/fedwire/fedwire_funds_services_statistics.html

FinCEN recognizing and reporting suspicious activity relating to financial crimes. (2003). Washington, D.C.: Financial Crimes Enforcement Network.

France, Financial Action Task Force. (2005). *Trade-Based Money Laundering*.

Longmire, S. (2011). *Cartel: The coming invasion of Mexico's drug wars*. New York: Palgrave Macmillan.

National drug threat assessment. (2011). Johnstown, PA: National Drug Intelligence Center.

National money laundering risk assessment 2015. (2015). Washington, DC: United States Department of the Treasury.

Pietschmann, T., & Walker, J. (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes: Research report*. Vienna, Austria: UNODC, United Nations Office of Drugs and Crime.

Sullivan, K. (2015). *Anti-Money Laundering in a Nutshell* (Rep.).

United States Efforts to Combat Money Laundering and Terrorist Financing, United States Senate Caucus on International Narcotics Control Cong. (2004) (testimony of Karen P. Tandy).

USA Patriot ACT, §§ 311-362 (United States Government Publishing Office 2001).