2009

Deficiencies in regulations for anti-money laundering in a cyberlaundering age including COMET: Central Online AML Merchant Enforcement Tool

Brian David Schwartz
Iowa State University

Deficiencies in regulations for anti-money laundering in a cyberlaundering age including COMET: Central Online AML Merchant Enforcement Tool

by

Brian David Schwartz

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Information Assurance

Program of Study Committee:
Sree Nilakanta, Major Professor
Doug Jacobson
Rick Carter

Iowa State University

Ames, Iowa

2009

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Money laundering, an act of illegal cash washing, accounts for two to five percent of the world's gross domestic product. This alarming amount of illegal financial activity has brought national and international laws, regulations on banks, and procedures to deter money launderers. With the rise of cyber banking, digital cash, anonymous stored value cards, and advanced personal identifiable information theft, money laundering laws and regulations fail to account for the movement of illegal money in the digital world.

Discussed in this thesis is an overview of the current money laundering techniques and regulations. The objectives of this research are twofold; first, to broadly identify deficiencies within the banking and regulatory institutions regarding cyberlaundering including hypothetical cyberlaundering methods and second, to suggest a specific feasible approach to minimize and deter online laundering of illicit revenue through the application of COMET: a Central Online AML Merchant Enforcement Tool. COMET is a central database system which makes use of data mining techniques to mitigate a cyberlaundering return merchandise scheme.

CHAPTER 1. MONEY LAUNDERING OVERVIEW & TECHNIQUES

Tom Delay, the 24th United States House of Representatives Majority Leader [1] was asked to step down in October 2005 for money laundering. Benazir Bhutto, the former Pakistan prime minister was convicted in 2003 for laundering money through Swiss bank accounts [2]. Franklin Jurado, an economist from Harvard University was convicted of laundering money in the amount of $32 million for the Columbian drug lord Santacruz-Londono in 1996 [3]. Money laundering is not a new crime – it has been around since organized crime in the 1930s, and still plagues today's financial market. According to the International Monetary Fund, roughly $600 billion is laundered each year [4]. This is between 2 and 5 percent of the world's gross domestic product. With the rise of a global economy and a digital economy, money launderers are finding easier ways to use other country's banking rules and regulations to their advantage.

1.1 Introduction to Money Laundering

Money laundering is 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 [5]". The primary task is deception when looking at the heart of money laundering: deceiving the authorities by

making assets appear as if they have been obtained through legal means, with legally-earned income, or to be owned by other parties who have no relationship to the true owner.

The laws of each country that have criminalized money laundering define the activity a bit differently. This is one of the ways money laundering works – by taking advantage of the changing rules per country.

1.1.1 Stages of Money Laundering

To better carve a definition of money laundering, it is crucial to understand how laundering occurs. Money is usually laundered through a series of transactions and it typically includes three steps. To move to the next step in the process, funds need to be moved. Some of the more obscure methods are done through means of cyber-hacking.

1.1.1.1 Step one: Placement

During the first phase, the money launderer will place his/her illegal assets into the financial system. This is often done by placing funds into circulation through financial institutions, casinos, shops, currency exchange and other businesses, both domestic and international.

Some examples of this phase are:

- Breaking up large amounts of cash into smaller sums and then depositing those directly into a bank account.

- Shipping cash across borders for deposit in foreign financial institutions, or be used to buy high-value goods, such as artwork, and precious metals and stones, that can then be resold for payment by check or bank transfer.

1.1.1.2 Step two: Layering

The layering step to money laundering involves taking the proceeds and developing complex layers of financial transactions to disguise the audit trail, ownership, and source of funds. This phase can involve transactions such as:

- Transferring the deposited cash from one account to another
- Converting deposited cash into monetary instruments (e.g. e-gold on the Internet)
- Reselling high-value goods and monetary instruments
- Investing in real estate and legitimate businesses, etc.
- Using shell banks, which are typically registered in offshore areas, and wire transfers, which will be focused on later in the thesis

1.1.1.3 Step three: Integration

The third and final stage in the money laundering process involves placing the laundered proceeds back into the economy to create the perception of legitimacy. By the integration stage, it has become very difficult to distinguish legal and illegal wealth [40]. The

launderer might choose to invest the funds in real estate, luxury assets, business ventures, or other means.

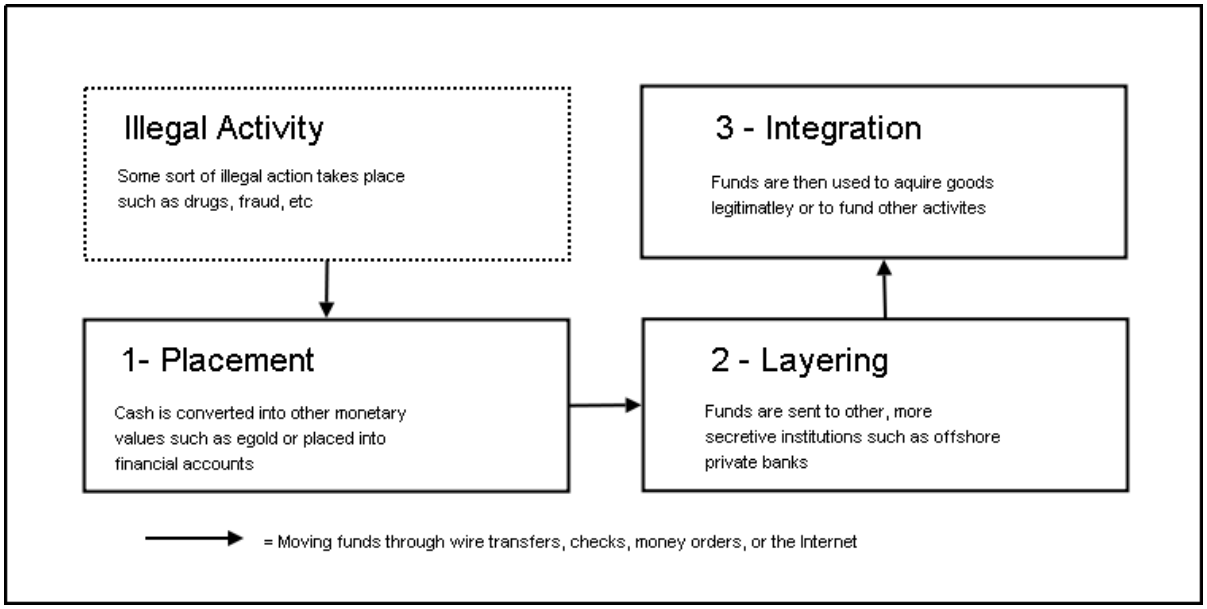

Figure 1. Stages of Money Laundering

1.1.2 Current Money Laundering Zones

Currently, there are three large money laundering "zones" associated with money laundering [5]. Below is a brief discussion of each, though I would like to introduce a new money laundering zone, "cyberlaundering", which will be discussed more in detail in the latter portion of my thesis.

1.1.2.1 Correspondent Banking

Correspondent banking is the service by which "one bank provides services to another bank to move funds, exchange currencies or carry out a variety of other transactions [5]". In some correspondent relationships, the foreign bank's local customers are permitted to conduct their own transactions, including wire transfers, through the foreign bank's U.S. correspondent account. Those accounts are known as "payable-through accounts." In other situations, a foreign bank's correspondent account in the U.S. is used by another foreign bank to conduct its own transactions, a practice called "nesting [6]."

With such direct access to the U.S. financial system, once the funds are received in the U.S. correspondent account, the foreign bank's customers or other foreign banks can move the money in or out of the U.S. with the correspondent account serving as cover. This money laundering "gateway" is termed as correspondent banking. It added that money laundering through correspondent banking "is not a new or isolated problem. It is longstanding, widespread and ongoing [5]."

This vulnerability compelled the Wolfsberg Group, an organization of large banks founded in 2000 that issue guidelines for private banking, to publish principles on correspondent banking in November 2002 [7]. These recommendations include:

- Due diligence on risk-based accounts
- Client information needs to be reviews and updated regularly

- Institutions should not offer services or products to shell banks
- An international registry of financial institutions should be created to help aid in tracking down money laundering

1.1.2.2 Private Banking

In recent years, private banking has been seen as one of the most vulnerable areas of financial activity in the money laundering field. It gives financial flexibility to people of high net worth that move billions of dollars worldwide, often secretively, and with comparatively little control.

A 1999 report released by the Permanent Subcommittee on Investigations documented these reasons as to why private banking is susceptible to money laundering [8]:

- Private banking clients may have political or economic ties
- There is generally a closer relationship between the banker and the client
- Private banking is referenced as “secret” culturally
- Money laundering controls tend to not be enforced to as great of an extent as public banks would
- There is a greater margin of profit in private banking

One concerning factor that federal regulators have is the way private bankers work. Many of them work in large banks and are given salary bonuses for new customers whom they attract to the bank.

The U.S. Office of the Comptroller of Currency (OCC) recommends that banks evaluate private banking accounts on a "risk-grade basis," determining the level of risk by type of business, geographical location and bank product or service extended [9]. It states that well formed steps to open an account are “fundamental risk controls for private banking relationships.” These procedures, which bank management should follow, should include identification of account owners, source of wealth, and identification of “normal and expected” transactions.

In order to assess these risks, the U.S. Anti-Money Laundering/Bank Secrecy Act Examination Manual, released jointly in 2005 by the federal banking regulators, states that the following factors should be considered [10]:

- Nature of the customer
- Purpose and activity of the account, product, or service
- Relationship between the bank and the client
- Location and jurisdiction of the client's home or business
- Public information about the customer that is reasonably available to the bank

In order to verify the financial and legal status of a business, the OCC states that banks should require its personnel to identify the primary owners and review articles of incorporation, partnership agreements, financial statements and other relevant documents.

It warns that customers introduced by a third party financial partnership, such as an investment advisor, may require "particular attention." Before establishing their own third party procedures, banks should confirm that the intermediary "maintains and adheres to adequate standards to verify the identity and legitimacy of its customers [10]."

1.1.2.3 Black Market Peso Exchange

The U.S. Customs Service and Colombian law enforcement officials arrested 37 individuals as a result of a 2 1/2 year undercover operation named Operation Wire Cutter in 2002 [11]. Though this case is not recent, it is worth mentioning – it was monumentally described in the 2002 National Money Laundering Strategy as a landmark case that brought down several Colombian peso brokers who were believed to have laundered money for narcotics cartels. These brokers were engaging in a form of money laundering called the Black Market Peso Exchange (BMPE). This method of money laundering is so significant that it is considered a money laundering zone.

The Black Market Peso Exchange method is, generally, a process by which money in the U.S. derived from an illegal activity is purchased by Colombian "peso brokers" from criminals in other countries and often deposited in U.S. bank accounts that the brokers have established. The brokers sell checks and wire transfers drawn on those accounts to legitimate businesses, which use them to purchase goods and services in the U.S.

For financial institutions to detect and prevent laundering by peso brokers, they must be familiar with the common laundering methods used by the brokers. The most common scheme involves multiple checking accounts opened at U.S. banks by foreign nationals [12]. Banks must also be aware of the increases in the movement of dollars in the corresponding accounts of foreign banks.

1.1.2.4 Cyberlaundering

As the physical world of money is fading, a new era of money laundering ease is evolving. The first means of laundering electronically was through wire transfers. Moving money through a wire transfer currently provides a limited amount of information regarding the parties involved. This is becoming less common however, and greater details regarding a wire transfer are to be recorded. As the privacy of wire transfers is decreasing and the record keeping regulations are increasing, money launderers need to expand their methods. This approach happens through the world of cyberspace.

As consumerism increases in the cyber world, so does the need for an effective and efficient means of financial transactions. As a result, electronic cash was created as a replacement for cash. Digital or electronic cash refers to “money or scrip which is exchanged only electronically [12]”. Although a great deal of electronic cash is traceable, a few institutions still provide a means of offline and online anonymous digital cash. This type of anonymity is of a particular interest to money launders.

The issue that arises in cyberlaundering is the deficiency of the regulations specific to electronic money laundering. Many digital banks do not fall under a specific regulatory statute, and thereby would not have to adhere to certain rules that brick and mortar banks would need to. Furthermore, there is a great deal of controversy in regards to the privacy rights – weather all electronic transactions should be monitored simply because a small percentage might be illegal.

1.2 International Crime Organizations

Local and national law-enforcement agencies have been limited to combating money laundering by the confines of geographic jurisdiction. As a result, perspective has equally been limited and crime has been a local or national issue. Money laundering, especially in the cyber world, has crossed jurisdictional boundaries and has gone global. Even though the advent of money laundering is an international threat, it is important to know the large money laundering organizations. More than 80% [13] of current money laundering is performed through a connection to these organizations. There are three main types of transnational organizations. First, there are the six large [13] transnational criminal organizations: the Italian Criminal Enterprises , the Russian Mafiya, the Japanese Yakuza, the Chinese Triads, the Columbian Cartels, and the Mexican Federation. The second main type of criminal organizations is the smaller groups which are very highly organized. These organizations have certain criminal specialties that work for the six large transnational organizations as a

smaller entity. These groups are found in Nigeria, Panama, Jamaica, the Dominican Republic, and Puerto Rico. Lastly, there are terrorist groups who deal in smuggling, contraband, narcotics, and other items as a means to finance their political objectives. The method of terrorist financing is similar to money laundering, but done differently.

1.2.1 The Big Six

The Italian Criminal Enterprises are made up of four distinct criminal groups operating primarily in Italy: the Mafia, the Camorra, the 'Ndrangheta, and the Sacra Corona Unita (Sacred Crown). These groups are generally organized on family or clans and work on a system of power known as the *sistema del potere* [13]. This system of power has expanded beyond Italy and formed alliances with transnational organizations.

The Russian Mafiya has become the world's dominant criminal organization. They are known as the rackteers in the U.S. and consist of about 5,000 to 6,000 gangs [14]. Their past skills have been slavery, human smuggling, gasoline fraud, toxic waste disposal, and telecommunications fraud. Currently, they are involved more with Internet banking fraud, credit card theft, and money laundering over the Internet. The schemes and speed at which they carry out these activities are increasing daily [14].

The Japanese Yakuza has been a part of Japan since the early 1600s and is currently a large part of legal and illegal economies. The issue was so bad that the government passed the Act for Prevention of Unlawful Activities by *boryokudon* [13]. Boryokudon or

"organized crime" groups were not allowed to make a profit on extortion, gambling, or other legitimate or illegitimate activities. Currently, the Yakuza of Japan deals a great deal with the financial sector, using laundered money to perform their activities [15].

The Chinese Triads consists of many branches of organizations based in Taiwan, Hong Kong, Macau and mainland China. The Chinese Triads can be found in the U.S. as well – particularly in San Francisco. Their activities include drug trafficking, contract murder, money laundering, gambling, prostitution, car theft, extortion, and racketeering [16]. A recent scheme that the Triads are performing is shipping goods to non-existent companies where the goods are replaced with cash. They are then marked as undeliverable, and the cash is shipped back. Returned goods are not inspected because they seem to have never been delivered.

The Columbian Drug Cartels are known to have the largest cocaine trafficking. The cocaine comes from Peru, Bolivia, and Columbia. The Cali Cartel is known for its high amount of financial crime over the other two. The other two are known as the Medellín Cartel and the Norte Del Valle Cartel. The Cali cartel invested its funds into legitimate business ventures as well as front companies to mask the influx of money it was obtaining in cocaine. In 1996, the Cartel was making 7 billion in annual revenue [41]. The cash needed to be laundered. Gilberto Rodriguez Orejuela, who was affiliated with the Cartel, was able to secure the position of Chairman of the Board, of Banco de Trabajadores. The bank was believed to be used to launder funds for the Cali cartel, as well as the Medellín Cartel.

Furthermore, Gilberto founded the First InterAmericas Bank operating out of Panama. Gilberto admitted to money being laundered through the bank, however, he stated that the process was legal. Gilberto later started the Grupo Radial Colombiano, a network of radio stations and a pharmaceutical chain which was also used to launder monetary funds.

The Mexican Federation launders approximately $7 billion annually amounting to 2.5% of the Mexican economy's value [13]. Responsible for the cocaine, heroin, and marijuana production in Mexico, the drug proceeds are placed into the financial system through Mexican banks or casas de cambio, or sent back across the border without knowledge of the true owner of the funds.

1.2.2 Other International Criminals

Nigerian Criminal Organizations are known for many different cybercrimes, and laundering money via the Internet is not any different for them. Their money laundering efforts include standard techniques such as smuggling and money-exchange houses but do things a bit differently. The Nigerian criminals will buy heroine from countries, paying for it in U.S. dollars. They then smuggle the heroine to the U.S. and Europe. After selling the drugs, consumer goods are purchased where they are sold in Nigeria on the black market. In order to then convert the proceeds of this into US dollars, the naria (Nigerian Currency) is delivered to one of the cities on the Nigerian border. These are converted in to CFA francs, a

currency promoted by France to promote trade. The receipts of the trade allow them to wire the francs to banks in England where they are then converted into U.S. dollars.

CyberCrime Inc. is an umbrella name for people who are involved with organizing criminal activity on the web. One of their largest crimes is assisting the big six with laundering money for them through methods that will be discussed later in the thesis. The biggest issue with these criminals is the speed and determination they have for conducting illicit activity on the Internet, whether it is drug trade or cleaning up dirty money.

1.3 Money Laundering Techniques and Tools

The following section talks about the more common techniques used by launderers to wash dirty money through the banking industry. Knowing these techniques can better help mitigate and understand how money laundering can occur in the cyber world.

1.3.1 Smuggling

Since 1986, the structuring method (discussed in section 1.3.2) of money laundering became a criminal offense. As a result, smuggling has been the most popular method for starting the money laundering process. Smugglers are attempting to get the cash away from the strict U.S. and into a less monitored country. The simplest way to wash cash using via smuggling is when the money travels over the border, such as from the United States to Mexico, the money is not declared on a CMIR report (CMIR reports will be discussed later

in the thesis). The launderer then turns around and declares the funds at U.S. Customs as legitimate revenue, backed up with phony receipts from Mexico. Then the cash can be placed in any U.S. bank without any suspicion, and wired to a location of choosing. The DEA and Customs estimates that roughly $50 billion is smuggled out of the U.S. every year, thus avoiding many of the money laundering reports and regulations. This is only the amount seized however – there could be much more.

Smuggling cash out of the United States is the method of choice for many money launderers because the primary goal of the U.S. Customs Service is inbound drug monitoring more than outbound drug monitoring. Smuggling drugs into the U.S. is only one of three types of smuggling used in the laundering cycle. Outbound cash smuggling and inbound financial instrument smuggling are the other two. For example, a study in 1994 found that 85 out of 338 ports controlled by Customs had been performing outbound inspections [13]. There are 5,000 trucks that cross into the U.S. daily on average with only about 200 of those inspected (This statistic was conducted before September 11th, 2001. Inspections have increased since).

Smuggling cash is done by three different methods. Cash is shipped in bulk through the same channels that were used to bring in the narcotics. Another way is hand carrying the cash. Lastly, the cash can be converted into a monetary instrument such as a money order or a traveler's check and then mailing these to foreign banks.

1.3.2 Structuring

The term structuring describes the act of dividing large sums into smaller sums less than $10,000 each to avoid the Bank Secrecy Act Reporting requirement (discussed later in the thesis). Since 1986, this method has been listed as a crime through the banking industry. It is widely used in the cyber laundering realm as the law only applies to financial institutions. Many launderers are structuring in a method known as “smurfing” where the each deposit is not made by the same individual but rather this individual is hiring others to deposit the money in accounts in an attempt to remain anonymous. One offline case of this was the Grandma Mafia Case where a 60 year old grandmother led a group of women in depositing $25 million in various bank accounts in California.

1.3.3 Front Companies

Front Companies are a place where launderers can place and layer proceeds that are illegal. A metals company called Cirex International was used by a Colombian drug lord to deposit approximately $150 million into various U.S. bank accounts [13]. Front companies do not need to comply with any financial institution to operate. They are also difficult to detect if there is legitimate business being conducted and if the institution is not required to fill out CTRs (discussed later in the thesis).

1.3.4 Shell Corporations

Shell companies are, according to the FATF, “institutions, corporations, foundations, trusts, etc., that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located. [42]” These companies assist with the layering step of money laundering and are not complex to set up. Any lawyer will register a business for a fee and name him or herself the chairman/chairwoman. Corporate bank accounts are created at various offshore or island banks. The organizations are used when clients need to launder money and remain anonymous.

1.3.5 Dollar Discounting

Dollar discounting is where a drug dealer will auction his drug proceeds to a broker at a discount. Then the broker is assuming responsibility for laundering the money. This is done so that the money can be given to the drug dealer quickly in order to better prevent himself from being discovered by law enforcement.

1.3.6 Mirror-Image Trading

The mirror image trading scheme works in where a launderer buys contracts for one account while selling the same amount from another account. Because both accounts are controlled by the same person, there is neither profit nor loss – just new money.

1.3.7 Inflated Prices

This scheme works where false invoices are created for imported good that were never purchased or bought at high inflated prices. It is estimated that this false evaluation of the price of goods that come from overseas has cost the U.S. approximately $30 billion in taxes that are not accounted for per year [13].

1.4 Money Laundering in the Banking Industry

About 30 years ago, it was very easy for a drug dealer or a criminal to walk into a United States bank and deposit large amounts of money. Through the aggressiveness of Bank Secrecy Act regulations and the US Patriot act, the US banks are not as strong of a field for money laundering. It has become exceedingly difficult for money laundering to occur within the realms of U.S. banks. In this section, a quick overview of the banking industry will be introduced along with common money laundering techniques. This framework will help with understanding the banking laws and statues so that preventative cyber laundering measures can be discussed.

1.4.1 The United States Banking Industry

The banking industry in the United States is complex, consisting of financial industries at the federal, state, and local level. All these are regulated by federal and state agencies that at times regulate the same things. The primary banking system is the Federal

Reserve, which is run by a board of seven governors appointed by the U.S. president for 14 years. The Federal Reserve has 12 central banks, a Federal Advisory Council, and member banks. All banks of national status are members of the Federal Reserve Banking System. They are supervised by the Office of the Comptroller of Currency and must contain the word "National" in their name. If they meet these qualifications, then they can become a member of the system.

1.4.2 Offshore Banks

An offshore bank is a bank located outside the country where the depositor of financial currency resides. These "offshore banks" are generally in a low tax jurisdiction that provides financial and legal advantages. Besides the advantage of greater privacy that an offshore bank provides, there are many other reasons why a money launderer would look to an offshore bank. Some of these include:

- No mandatory reporting of suspicious activity
- The government in where the offshore bank is located is corrupt
- American dollars can be used in an offshore bank (possibly)
- Ability to use anonymous, nominee, or numbered accounts
- No effective monitoring of currency movements
- Access to free-trade zones
- Bank regulatory systems in many offshore banks do not perform well

The term “offshore” originates from the banking industry in the United Kingdom where the term “offshore” was where banks in the Channel Islands were. Offshore banks are more commonly used to represent many of the banks on small islands and even many of the stable, private banking done in Switzerland.

1.4.3 Common Money Laundering in Banks

This section will briefly discuss some of the common money laundering techniques that have been used in the banking industry. Through the Bank Secrecy Act and other Anti-Money Regulations, these have been mitigated extensively. It is helpful to better understand these methods in order to mitigate methods for cyberlaundering.

1.4.3.1 Wire Transfers

Wire transfers are simply transferring money from one bank or institution to another. Wire transfers are and will be imperative for the banking industry. This method of “layering” illicit funds is the most common tool in the banking industry for moving large amounts of capital. There are three main transfer systems used in the world for wire transfers. One is called CHIPS (The Clearing House Interbank Payment System), another is known as Fedwire, and the international wire system is known as SWIFT (Society for Worldwide Interbank Financial Telecommunication). There are approximately 700,000 wire transfers daily moving over $2 Trillion U.S. dollars [43]. A wire transfer works in this

manner. A bank sends a message to a transfer system's main computer indicating the originating bank, the amount, the receiving bank, and the specific person who is to receive payment. The computer adjusts the balances, and produces an electronic debit ticket at the original bank along with a credit ticket at the receiving bank. Once the bank receives a credit ticket, it lets the originating bank know to debit the money. If the two banks are part of the same wire transfer system, they are the only two banks in the chain. If they are not, such as in an international transfer, then transfers have to be done through a correspondent account. 80% of the transactions are not done this way however [13].

The Annunzio-Wylie act of 1994 regulated wire transfers in the following manner. The originating bank accepts a payment order and begins a wire transfer. It must verify and retain records of the identity of the individual submitting the payment order. If there is no information given, the bank still processes the order, but must make a note that there was no information provided. At the same time, the bank obtaining the transfer needs to maintain records of the recipient. Any banking system that is forwarding on the information does not need to verify records. The record-keeping and verification requirements apply to funds that are $3,000 and greater.

1.4.3.2 Money Laundering Prevention

Banks take a very strong approach in mitigating risk and preventing money laundering from occurring in their institution. Since the inception of the Bank Secrecy Act in

1970, other rules and regulations followed in order to cork any holes that came about from the rising technology and change in the banking system. As a response to the September 11th Attacks, the US Patriot Act clamped down on terrorist financing by extending the rules already in place. The one stipulation however is the need to prevent money laundering from occurring electronically.

All banks are required to have a BSA compliance program. These programs must set out a system of internal controls, designate a BSA security officer, undergo auditing, and train bank personnel. Furthermore, banks must institute a "Know Your Customer" policy in order to verify that the customer is not on any list of known fraudsters, terrorists or money launderers, such as the Office of Foreign Assets Control's Specially Designated Nationals list [44]. Other than this, the policy monitors transactions of a customer against their banking history and banking of their peers.

1.5 Money Laundering in Non-Bank Financial Institutions

The Bank Secrecy Act originally applied only to 20 "financial institutions", and was later extended to apply to all national banks. Five of these were banks, where the other 15 were known as non-bank financial institutions and included the following:

- SEC registered and other securities or brokers/dealers
- currency exchanges
- investment banks

- traveler's check and money order issuers
- redeemers
- credit card systems
- insurance companies
- travel agencies
- precious metal dealers
- pawn brokers
- finance companies
- real estate brokers
- financers
- the U.S. postal service
- casinos

Non-bank financial institutions listed are subject to the BSA reporting requirements, but generally need to only license within the state. The known money laundering cases in Non-Bank Financial Institutions are the casas de cambio, major wire companies, the wire transfer "Giro houses [37]" or neighborhood money transmitters and insurance companies.

CHAPTER 2. MONEY LAUNDERING STATUTES & LAWS

Money Laundering is an international issue. As with many laws and statues, the regulations to handle money laundering activity are addressed slightly differently by each nation. The United States has, in recent years, looked at anti money laundering regulations as a means to prevent terrorist financing due to the attacks of the World Trade Center in 2001. The U.S. will be discussed first. In order to discuss techniques mitigating cyberlaundering, a discussion of regulations in effect in other international communities will be addressed.

2.1 U.S. Rules and Statues

The U.S. Began regulating money laundering in 1970 by passing three statues. First was the Bank Secrecy Act (BSA) of 1970. This act served as the foundation of bank reporting activities. The main purpose of the act was to create a paper trail of any activity deemed "suspicious" for law enforcement to follow [46]. Section 5311 of the Bank Secrecy Act states that its purpose is "to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings [47]". This report is an IRS form 4789, more currently known as a Currency Transaction Report (CTR). Whenever an individual or someone conducting a transaction on behalf of an individual that involves $10,000 or aggregations that add up to $10,000 in one day, a CTR must be filed by the bank. These records must be retained for five years minimum. Banks with more than $1 billion in assets are examined biannually; others are done randomly to make sure that the law is being upheld.

Another major part of the BSA is the requirement for banks to fill out Currency and Monetary Instrument Reports (CMIRs) and Foreign Bank Account Reports (FBARs). CMIRs are similar to CTRs but record any coins, foreign currency, securities, traveler's checks, bearer bonds, and negotiable instruments deposited which have value greater than $10,000 [48]. FBARs are forms that deal with the deposit of $10,000 USD into a foreign bank [48].

In 1982, the BSA was modified to include other financial institution's necessity to file CTRs such as travel and insurance agencies, money exchanges, auto dealerships, and wire transfers. In 1984 the BSA again amended by the Comprehensive Crime Control Act. This act amended section 5323 of the Bank Secrecy Act that provided awards for people who could provide information into cases of money laundering where the government was able to recover more than $50,000.

In 1986, the Money Laundering Control Act came into power. This addressed the issues that launderers were performing to skirt the reporting requirements. Launderers would use casinos, use front companies, and simply smuggle money. The method most commonly used by money launderers was to structure the transactions by dividing the deposits into amounts that were less than $10,000. As discussed briefly earlier in the thesis, this is known as “smurfing”. Smurfing is a term derived from the blue smurfs where there were many small entities (many small smurfs) [49]. The Money Laundering Control Act addressed these issues by requiring CTRs be filled out if small deposits amounted to $10,000 in a day. Furthermore, casinos were required to adhere to the BSA.

In addition, the BSA provides civil money penalties for noncompliance [46]. The first case where this took place was against The Bank of Boston. The bank failed to file CTRs for 1,163 transactions valued at $1.2 billion. Other banks followed suit: Croker National Bank paid a fine of $2.25 million for not filling CTRs, the Republic Bank of Miami was fined $1.95 million.

In 1990, a group called “FinCEN” was formed. FinCEN, or The Financial Crimes Enforcement Network, is a bureau of the United States Department of the Treasury that collects and analyzes information about financial transactions in order to combat money laundering and terrorist financing.

The Annunzio-Wylie Anti-Money Laundering Act of 1992 strengthened BSA violation sanctions along with requiring Suspicious Activity Reports (SARs). SARs are similar to CTRs with the exception that SARs allowed banks and other institutions to report suspicious activity other than a deposit of $10,000. Furthermore, the verification and recordkeeping for wire transfers were put into place, and the Bank Secrecy Act Advisory Group (BSAAG) was established.

In 1994, the Money Laundering Suppression Act was established. This required banking agencies to review and enhance training, and develop anti-money laundering procedures. The Money Laundering and Financial Crimes Strategy Act in 1998 created the High Intensity Money Laundering and Related Financial Crime Area (HIFCA) Task Forces to concentrate law enforcement efforts at the federal, state and local levels in zones where money laundering is a problem.

The most interesting change to Anti-Money Regulations seemed to occur in a matter of weeks after the September 11th terrorist attack on the world trade center. The rules and regulations in anti-money laundering were for the most part domestic, but because of the attack, the regulations that were to be enforced had a global outlook. The Bank Secrecy Act originally did not include laws that were targeted to prevent terrorist financing by way of money laundering. This was done by the passing of the US Patriot Act in 2001. The act included provisions on counterfeiting, information gathering and sharing, victims, and bribery of a public official. This law also made laundering money through a foreign bank a criminal offence.

Some other provisions the act included were:

- Prohibiting the U.S. from maintaining accounts for foreign shell accounts.
- Allowing the U.S. to obtain and hold the proceeds of foreign money laundering cases that occurred in the U.S.
- Creating new offenses of the concealment of terrorists.
- Encourage cooperation amongst banks, law enforcement, and regulators to discourage and prevent money laundering. This included sharing information about individuals engaged in suspicious activity.
- Including certain compute fraud crimes associated with money laundering, export control violations, firearms offenses, and foreign corruption offenses.

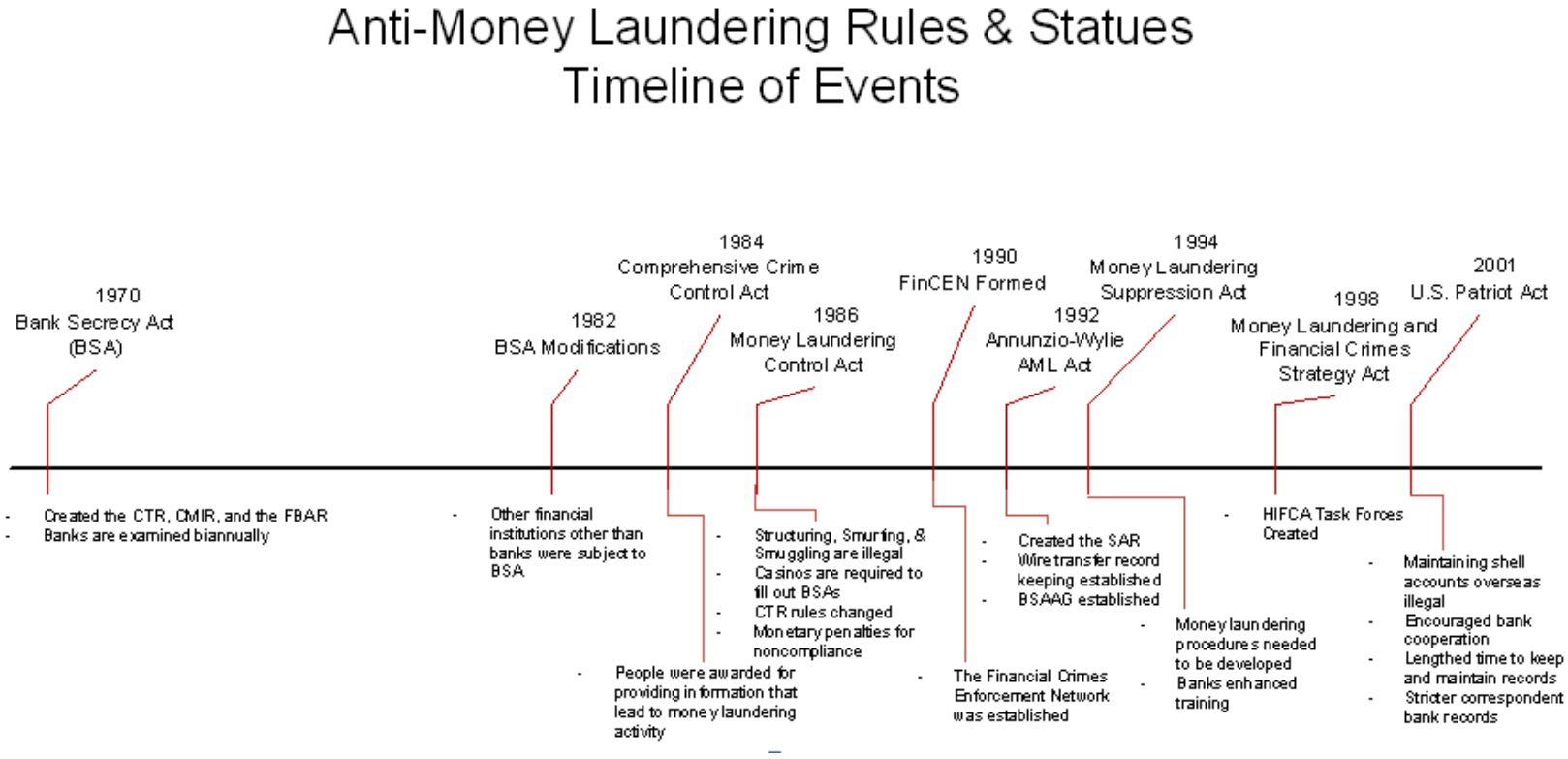

Figure 2. Timeline of AML Acts and Statue

Furthermore, the act covers certain aspects of record keeping. The US financial institution must now maintain additional records for any bank. The US financial institution must maintain additional records for any correspondent bank account it holds for a foreign bank. These records must include details of the owner(s) of the foreign financial institution and the name and address of a US resident authorized by the foreign bank to accept service of legal process for records regarding the correspondent account. According to the law, this information must be provided to the US authorities within seven days. Furthermore, the Secretary of the Treasury of the Attorney General may issue a summons of a subpoena to any foreign financial institution that maintains a correspondent account in the US, and request any records relating to an account. If a foreign financial institution fails to comply with the subpoena, the Secretary of the Treasury or the attorney general can issue a written notice to the US financial institution ordering it to terminate the correspondent banking relationship within ten days.

2.2 International Regulation Development

Due to the increase of money laundering at the international level, trans-national organizations have been formed to address this issue. Many countries are very open to the idea, and those that are not are discovering that their economic development is negatively affected due to a lack of cooperation. Many countries prohibit working with countries whose rules and regulations towards combating money laundering are considered inadequate. A list

of countries that do not cooperate with international money laundering strategies is issued by the Financial Action Task Force (FATF) – an international organization formed to prevent global money laundering. The FATF is an independent international body established in 1989. Its main purpose "is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing [28]".

Four tools have been established as requirements for effective action against money laundering:

- The criminal justice system within a country must be able to enforce the tracing, halting, and acquisition of the money involved in criminal activity.
- Enactment and implementation of legislation to criminalize and prevent money laundering must be present
- Due to the international drug trade and money laundering schemes, there must be an enhanced level of international cooperation to assist with the capturing of money launderers
- Legislation and regulations need to be put in place to assist with the criminal justice system

When discussing the international action against money laundering, specific mechanisms existed for the prevention and control of the crime. One of the first groups to get involved was the European Union (EU). The EU issued three orders on the Prevention of

the money laundering through the financial system. The first order was established in 1991 and required all member states to change their national laws to be able to prevent their banks from a money laundering exploitation. The second order came about from the limitations of the first order and was established in 2001 [50]. Within this order existed two major proposals. The first was to enhance the control of drug trafficking and other crime, including tax evasion. The second proposal was to bring terms to the non-financial sector. This brought various objections from different groups, but eventually settled with the following bodies involved in the order:

- Estate agents
- External accountants, auditors, and tax advisors
- Auctioneers where payment were in cash and for amounts of €15,000 and over
- Dealers in high-value, such as precious stones or metals, or works of art
- Independent legal professions specializing in specific functions

The third order was adopted by the EU in 2007. This order contained more details in regards to due diligence for customers with regards to three cases:

- Where there is no face-to-face contact with the customer
- Banking relationships overseas
- Relationships with people of political power

Furthermore, the order did not include a specific industry but stated “other natural or legal persons trading in goods, only to the extent that payments are made in cash in an amount of €15,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked [29]”

In 1988, the United Nations held a conference for the Adoption of a Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances [51]. Four obligations for parties participating in the Convention were created:

- Money laundering became a criminal offense
- Measures for the proceeds of drug trafficking were created
- Measures to permit international assistance in order to combat money laundering
- Ability for courts to order that financial records be available to law enforcement disregarding bank secrecy laws.

In 2002, the Palermo Convention was ordered by the General Assembly of the United Nations who adopted the United Nations Convention against Trans-national Organized Crime [52]. The convention was legally bound by the UN and created a treaty, which was signed by 184 countries. The treaty established laws against obstruction of justice, corruption, money laundering, and participation in organized crime. Furthermore, the

convention assisted countries on issues such as mutual legal assistance, extradition, transfer of proceedings, and joint investigations [52].

In 1974, a committee by the name of the Basel Committee was established. This committee was made up of the central banks from ten different countries: Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the UK and the USA. The committee set forth as statement of principles, titled the "Basel Principles" and has proved over the years a large step forward in the prevention of money laundering. In 2001, the committee issued customer due diligence for financial institutions addressing customer verification standards called "Know Your Customer" (KYC) which was later revised by the Financial Action Task Force (FATF). The Basel Committee formed The Offshore Group of Banking Supervisors (OGBS) to help define and implement international standards for cross-border banking.

The Financial Stability Forum (FSF) was created in 1999 to bring together senior officials from banks and supervisory committees in order to reform many of the auditing issues in offshore centers [53]. Many of the wealthier offshore financial centers had a better compliance then those of lower income. An assessment program was put into place to insure compliance from all offshore financial centers.

In 2002, the International Monetary Fund (IMF) and the World Bank began a one year program to assess the international money laundering standards conducted with the FATF and OGBS [54]. Following the program, the World Bank and IMF responded to over

100 countries who were asking for help in building a program to help fight money laundering and terrorist financing. The assistance focused on how countries could up their regulations to standards found in the international realm as well as improving coordination between governmental departments.

In the late 1990s, the international scene became concerned that private banks were not involved enough with combating money laundering. As a result, a group called the Wolfsberg Group which consisted of 12 global banks produced and published Anti-Money Laundering Principles for Private Banks. In 2002, the Wolfsberg Group produced a statement on the financing of terrorism and in 2003 a statement on monitoring, screening, and searching. These principals are voluntary but there are very strong reasons for institutions involved with private banking to adhere to the principles.

The Egmont Group created a meeting of the Financial Investigation Units (FIUs) of many FATF countries in 1995 in order to improve and increase communication between the parties. According to the group an FIU is "a central national agency responsible for receiving, analyzing and disseminating to the competent authorities disclosures of financial information concerning suspected proceeds of crime, or required by national legislation or regulation in order to combat money laundering [55]". Furthermore, the group founded a Memorandum of Understanding which information could be shared more easily between the FIUs.

These groups and summits have been pinnacle in the mitigation of money laundering. However, the main international force has become the Financial Action Task Force (FATF) and its forty recommendations which have been the cornerstone for most national anti-money laundering laws throughout the globe [13]. When the attack on the World Trade Center occurred, the FATF issued an additional Nine Special Recommendations to prevent terrorist financing.

To become a member of FATF, the minimum criterion needs to be followed:

- Commitment to prevent money laundering at the political level
- All Recommendations must be implemented within three years
- Annual self-assessment exercises and two rounds of mutual evaluations must be administered
- Must be an active participant in the regional FATF body
- Must be a country that is strategically important
- Money laundering and drug trafficking must be a criminal offence in your country
- Financial institutions must identify their customers and be able to report suspicious transactions

The FATF fulfills other roles, including assisting those countries who are a part of FATF to implement anti-money laundering guidelines, follow case studies, and promote anti-

money laundering measures. The Forty Recommendations published by FATF are targeted towards governments and financial institutions forming a comprehensive statement against money laundering at the global level. In 2000, the FATF drew up criteria to create a list of Countries that did not follow FATF's Forty Recommendations. In 2000, the list was at 23 countries, and currently has only two – Myanmar and Nigeria.

FATF has been a driving force in combating global money laundering, identifying many of the trends and methods associated with money laundering. As the world enters an age where the use of computer technology begins to aide in transferring money globally, the FATF will need to be responsive and adjust its combat in the world of money laundering.

2.3 U.S. Bank Regulatory Forms

The Bank Secrecy Act outlines five major reports and an IRS form (8300) that banks are required to file in the U.S. In addition to these reports, banks must maintain certain records as well – this section will briefly cover the six reporting forms in order to explain what information is being reported to FinCEN.

2.3.1 Currency Transaction Report (CTR)

Since the beginning of the Bank Secrecy Act till 1992, the CTR was the primary form to evaluate and determine if money laundering was an issue in a financial institution. The filing of this form was required if transactions of an individual would amount to $10,000 or

more in a given day. Since 1992, the CTRs have been enhanced by Suspicious Activity Reports (discussed in section 2.3.6). The reason why CTRs are not the only form of compliance: the IRS estimates that 30 to 40% of CTR filings are simply routine legitimate deposits. Furthermore, each CTR is costing approximately $3 to $15 to report totaling $130 million per year. For federal agencies, the cost to report and process the data is approximately $2 per CTR. Banks are also heavily fined for insufficiently filing CTRs.

2.3.2 Currency Transaction Reports by Casinos (CTRC)

Since 1985, casinos with revenue greater than $1 million must fill out CTRCs. During 1996, casinos filed 150,000 CTRCs which totaled approximately $3.2 billion. In 1997 these forms were simplified by the Treasury Department to state that every deposit, withdrawal, exchange of currency or tokens/gambling chips that involve $10,000 or more must be included.

2.3.3 Currency and Monetary Instrument Report (CMIR)

The Currency and Monetary Instrument Report, or also known as the "Report of International Transportation of Currency or Monetary Instruments" was created by the BSA in 1970 [46]. This form required any person who transports inventory greater than $10,000 in or out of the U.S. to declare this on a CMIR. This is different than a CTR in where a CTR is the responsibility of a bank and a CMIR is on the responsibility of an individual.

The most interesting case involving a CMIR happened in 1988 with Raoul Arvizo-Morales, who at the time was employed by a money exchange in Juarez, Mexico. He was asked by his brother, who was the owner of a money exchange business at that time to transport $172,081.04 in checks and cash to the Texas Commerce Bank in El Paso, TX. A CMIR was filled out for that transaction. Just before he was about to leave, his brother asked Raoul to stuff a little over $20,000 into a brown paper bag, which he did not claim. At the border crossing, the CMIR was given to the customs officer who asked to see the money. Raoul produced two paper bags with money in them. When the customs officer asked if all the money was going to the Texas Commerce Bank, he said yes except for one of the paper bags. Arvizo-Morales asked if he could add the contents to the CMIR form as it was a mistake. The officer declined and seized all of his money. The Court of Appeals for the Fifth Circuit allowed the entire sum to be forfeited, but were displeased with the harshness of the statue [13].

2.3.4 Foreign Bank Account Report (FBAR)

Every person, banks, or financial institution who has an interest with a financial institution overseas who deposit more than $10,000 in aggregate must report that relationship with the U.S. Treasury yearly. There are a few exceptions to the rule:

- U.S. military banking facilities operated by a United States financial institution are not considered foreign, and therefore an FBAR is not required.

- An officer or employee of a bank who is under supervision of the OCC, the Board of Governors of the Federal Reserve System, the OTS, or the FDIC, is not required to report having signature or other authority over a foreign account if the officer or employee has no personal interest in the account.
- An officer or employee of a domestic corporation whose equity assets exceed $10 million and 500 or more shareholders is not required to file an FBAR if the person has no personal financial interest in the account.

2.3.5 Form 8300

The IRS form 8300 is a mirror image to the CTR. The form needs to be filled out and submitted by someone who is involved in trade, business, or transactions that involve cash or the equivalent over $10,000. Until February 1992, businesses were only required to fill out receipts on cash over $10,000 received in a 12 month period. Since that time, the rule has been amended to report other forms of instruments that have financial value [56].

This business reporting was quite insufficient pre-1990. The IRS stepped up and began assessing heavy penalties to those industries that were not submitting reports. The largest case to date was against five car dealerships in the New York, which failed to file an IRS 8300. Cars and the bank accounts of the dealers were seized, with fifteen people pleading to money laundering, structuring, and not reporting certain bank deposits [13].

2.3.6 Suspicious Activity Report (SAR)

Since its inception in 1992, the SAR has been the most important form to mitigate money laundering. Whenever a financial institution's employee "knows, suspects, or has reason to suspect" that a transaction have been processed that seemed suspicious, an SAR needs to be filled out. There are over 23,000 institutions in the U.S. that are required to fill out an SAR: basically, almost every financial institution in the U.S. is required to comply.

The term "suspicious activity" is said to include any activity that "has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction".

A financial institution is required to file an SAR within 30 days of any suspicious activity. Failure to file an SAR will expose the bank and those responsible to action resulting in fines and monetary penalties. Since the inception of the system, over 125,000 SARs have been filed, with over 40% of them involving possible money laundering. The only issue with SARs is that there is a bit of discretion that is left in the hands of those who are required to file. What is "suspicious" to one bank teller might not be "suspicious" to another. The FATF has even admitted that countries do not have mandatory reporting requirements but only requirements to file an SAR where "suspicious activity" is involved. This "hole" is one

that is of concern – many launderers are finding other ways to smurf money, such as the utilization of the Internet.

2.4 Law Enforcement Tools

This section discusses the current tools and operations law enforcement currently uses to track down drug traffickers and uncover money laundering schemes. Though the OCC, OTS, Federal Reserve, and IRS all play a role in mitigating money laundering through the rules and regulations by way of forms and audit trails, it is the DEA and Customs Service, with help from the FBI and international groups such as the MI-5 and MI-6 from Britain, who are at the front line of the war on money laundering and drug trafficking [13].

In order to target money transmitters, the Bank Secrecy Act and U.S. Patriot Act has a way to require any United States domestic financial institutions to target transactions between specific geographical locations of high criminal activity of greater than a specified value. These are through Geographic Target Orders (GTOs) and last for 180 days [57]. In 1997, the first GTO was targeted at money remitters in New York who were wiring money to Columbia. These GTOs resulted in a find of $500 million being wired through this line every year – most of the money was drug money. Due to the GTOs, laundering of money went back to smuggling the cash which in turn accounted for an increase in cash seizures [57].

The Office of National Drug Control Policy is the administration of the High Intensity Drug Trafficking Areas (HIDTA) Program. This program is designed to locate areas in the U.S. with the greatest drug trafficking problem. The key priorities of the program are [58]:

- Evaluate drug threats in the region's drug threat
- Design policies to focus efforts that combat drug trafficking threats
- Develop and finance programs to implement strategies to mitigate drug trafficking
- Improve the effectiveness of drug control effort
- Reduce and eliminate drug trafficking

2.5 Conducting Investigations

When conducting a money laundering investigation, there are four steps in the process: identify the unlawful activity, identify and track the financial transactions, perform a financial analysis of the target, and freeze/confiscate assets. This section will explore each of the steps.

2.5.1 Identify the Unlawful Activity – Step 1

The majority of money laundering investigations start as a result of previous investigations into a person's illegal activity of narcotics, gambling, smuggling, etc. The investigators need to make sure that the unlawful activity that they are looking into is one of "specified unlawful activities" that could potentially be a money laundering scheme. Under sections 1956 and 1957 of the BSA, the government must be able to show that the funds came from one of the over 200 "specified unlawful activities [46]". The most common ones in money laundering cases are drug trafficking, crimes on the environment, banks violations and drug trafficking.

2.5.2 Identify and Track the Financial Transaction – Step 2

This is the step in where the money is revealed. As stated in step one, most money laundering investigations occur as a result of an investigation in narcotics, for example, by the same person. Investigations track the finances from the target using the following:

- Documents obtained when a search warrant was issued. Things like money receipts, brokerage statements or their address, wire transfer receipts, automobile records, etc.
- Law enforcement databases. For example, FinCEN's database that holds SARs, CTRs, CMIRs, etc. should be the starting point of the investigation.

- Databases that come from the commercial sector. Documents such as credit reports and court dockets which may give a great deal of information about the target.
- Public records such as corporate information, social security, information about any bankruptcy activity
- Places that distribute licenses such as the Bureau of Motor Vehicles, marriage licenses, and any public notary records [13].

2.5.3 Financial Analysis of the Target – Step 3

Two tools are used to in investigate a target's financial situation and determine if the spending habits they have reflect those of a launderer or one whose financial activity is normal. The first is called a "net worth analysis" and is used when the assets of a targeted individual are noticeable, and the other is labeled a "source and application of funds analysis" which is used where the spending habits are noticeable.

2.5.3.1 Net Worth Analysis

Net worth analysis is a tool that determines if a suspect has acquired assets at a rate that is over the rate of income from sources where she obtains it legitimately. This is much more easily done when the suspect acquires and disposes of tangible assets or the spending

habits are more transient and the lifestyle is "luxurious" in nature. The case *United States v. Sorentino*, the court called attention to this analysis method and stated it like this:

"The government makes out a prima facie case ... if it establishes the defendant's opening net worth ... with reasonable certainty and then shows increases in his/her net worth for each year in question with which, added to his/her non-deductable expenditures and excluding his/her known non-taxable receipts for the year, exceed his/her reported taxable income by a substantial amount…. The jury may infer that the defendant's excess net worth increases represent unreported taxable income if the government either shows a likely source, … or negates all possible non-taxable sources."

2.5.3.2 Source and Application of Funds Analysis

The source and application of funds analysis is a toll that is used to discover if someone that is accused of money laundering has obtained assets at a rate larger than his legitimate income level. This works quite well when the target is hyper spending and living over his or her normal means.

The analysis is quite simple – the cash that is not identified is equal to the total cash expenditures minus the total income of cash. This works when a person's income is known and has been reported or not known and not reported.

2.5.4 Freeze and Confiscate Assets – Step 4

Seizure and freezing the money is important to a laundering investigation. Though this topic of how the confiscation occurs is outside the realm of this thesis, it is important to note this step and understand that the timing of this step is of the upmost importance. Most money launderers will gather a large amount of money over a period of time and then send out the money in allocated blocks. It would not make much sense if the accounts were frozen after a large withdrawal was performed.

CHAPTER 3. CYBERLAUNDERING

The board of the International Monetary Fund in November of 2001 decided to "intensify fund activities in the international fight against money laundering, to expand these efforts to include anti-terrorist financing activities [17]". The plan recognizes that "funds are recycled in the financial system through a variety of layering techniques which take advantage of regulatory and supervisory weaknesses." In 2002, the U.S. laid out a National Money Laundering Strategy acknowledging the difficulty of estimating just how large the issue with money laundering is. The percentage of recorded GDP that is laundered money is worsened by the ease of cyberlaundering [43].

As of 2008, over 1.5 billion people worldwide are connected and use the Internet [18]. This access to information is a facilitator for world trade at speeds unheard of not too long ago. Because of this, the Internet is abundant with crime and criminal alliances. Financial value can be transported as anonymous, tax-free, and unregulated across borders and jurisdictions. This has been putting a great deal of burden on regulations, law enforcement, and legal systems; especially in developing countries where these systems are weak to begin with.

Cybercrime has experienced high growth from 2001 to 2007 – attacks on computer servers have risen by 1343% [21]. This trend is partially caused by software weaknesses, operating system hole exposures, and network vulnerabilities. Furthermore, this growing number represents attacks on the financial sector. The International Data Corporation reported that over 57% of all attacks from last year have been initiated on the financial sector

[45]. FINCEN's Suspicious Activity Reports for Computer Intrusions have topped a 500% increase over the past year. This amounts to about $222 billion dollars of money laundered annually through the Internet [45].

Due to the Internet's speed and expediency, financial transaction costs and float time are greatly reduced. These attributes are even more attractive to criminally oriented entities as it decreases disclosure and risk. For example, within fifteen minutes after the slammer worm of 2003 was introduced into the Internet, 27 million people in South Korea had no cell phone nor Internet access, five of the Internet's 13 root servers crashed, and Continental Airlines had to suspend flights due to absence of online access [63]. The ability to disrupt operations of businesses globally and quickly is an issue. Currently we do not have the policy or regulations to combat it.

There is no standard law or regulations that set up guidelines on how to discover and bring online money laundering to justice. This chapter will define and discuss what is known about cyberlaundering.

3.1 Cyberbanking

To be able to understand money laundering as a cyber crime, cyber banking needs to be explained. The Financial Crimes Enforcement Network has placed cyberbanking as a high priority by creating an e-Money council to assess how well the regulations and law enforcement system is doing with regards to electronic banking and online payment systems.

The money we traditionally use is easy, acceptable, and anonymous. It is generally limited to a small amount and the country that issued the currency. In a cyberbanking

system, traditional currency is eradicated. Rather than paying with a tangible object, cyberpayments facilitate the transfer of financial value through online bank accounts, smart cards, or Electronic Benefits Transfer (EBT) cards [19]. This cyberpayment system has the good qualities of traditional currency with added benefits such as widespread acceptability, security, and anonymity. The transfer velocity of cyberbanking is what allows the movement of large amount of dollars as fast as the computer can transfer the funds. The primary issue lies in whether cyberbanking should be and continue to be anonymous and as a result immune to banking regulations and law enforcement.

Many world organizations have created facets to quickly and safely buy and sell goods over the Internet. As an example, Secure Electronic Transaction (SET) was created in 1997 based on x.509 certification as a means to secure credit card transactions over insecure networks. SET introduced duel signature which links two messages that are intended for two different receivers. The customer wants to send her order information to the merchant and the payment information to the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know information concerning the customer's order. The link proves that the payment is intended for this order. SET failed simply due to the responsibility of the user providing a valid certificate. If malware was placed on a user's machine, this certificate could be compromised and the responsible party would be the unknowing customer.

Cyberbanks are not typical banks as one would expect. They do not offer deposit services but act as financial intermediaries for financial transactions. Cyberbanks can be unregulated [59] and work in an environment where anonymous transactions take place

instantaneously. Cyberbanks can also operate anywhere in the world and avoid detection by using forwarding systems electronically.

The Treasury's Department's Office of Thrift Supervision (OTS) is responsible for granting approval to companies looking to offer secure regulated U.S. banking services on the Internet (the OTS is the primary regulator of all federal and state chartered thrift institutions).

The OTS has granted approval to only two U.S. thrift holding companies to offer electronic banking services over the Internet. The first approval was granted on in 1995 with Cardinal Bancshares Inc. The second grant was given to Atlanta Internet Banks in 1997. AIB is the first approved and regulated bank that is exclusive to Internet transactions. AIB is required to adhere to the guidelines that were set out in the OTS "Statement on retail on-line personal computer banking" [13].

3.1.1 Cyberbanking Data Encryption

Online banking services need to provide strong data encryption. In 1993, the federal government created the National Information Infrastructure Forum to create a universal banking encryption standard for financial transactions on the Internet. They proposed the Clipper Chip, an 80 bit encryption system which contained a key that would enable the government to have access if they needed it. Many electronic rights organizations were against the Clipper chip, disputing that it would have the effect of not only possible illegal government surveillance, but also the design was secret, and therefore businesses might be forced to adopt an insecure system placing more risk on their computer structure [60].

Furthermore, better security standards such as PGP (pretty good privacy) were sprouting, pointing the attention of cyber banking in another direction.

Today, most online financial banking makes use of the Transport Layer Security (TLS) protocol. This protocol prevents eavesdropping, forgery, and creates non-repudiation. The issue that arises is that the government no longer has a "back door" and therefore cyberbanking payments may be immune to anti money laundering efforts (anonymous and untraceable). TLS makes use of the SHA-1 algorithm which has been recently hacked [20] complicating the use of TLS as a cyberbanking method even further.

3.1.2 Stored Value Cards

Stored value cards are similar to debit cards with the exception that the card is loaded with money. The use of the card is completely untraceable and the financial limits on the cards are unbounded [45]. Visa cash, Mondex Cards, and FeliCa are the currently the largest producers of stored value cards. A launderer with the proper software may be able to transfer billions of dollars on stored value card(s) out of the country. Currently, these cards lack the adequate controls to prevent this type of money laundering [45].

3.2 Cyberpayments

Cyberpayment systems are an international work in progress. Due to the speed of technology, issues cannot be addresses as progress moves forward. Many different systems are in development, but two dominant generic systems have undergone development, testing, and operation. The first is stored value smart cards, and the other is Internet based payment

systems known as electronic cash or “e-cash”. These two technologies are beginning to converge thus creating one large cyberpayment infrastructure.

Technical and commercial standards in the cyberpayment industry have been a progressing issue in international financial activity. This has led to a system-level control to discourage any single country from abusing the system. The beneficial factor in cyberpayment systems is their ability to take advantage of the deployment of network technology. This system allows for a peer to peer value transferring, payer anonymity for the customer, and a greater ability to conduct purchases internationally.

In discussing the cyberpayment-money laundering realm, it should be noted that the same technologies underlying cyberpayment products can be used as information gathering tools by law enforcement and payment system regulators. The privacy implications of the enhanced government surveillance of information is an issue often criticized as infringing on the right of privacy, but is essential to battling criminal activity. For law enforcement, his thesis takes into consideration the Freedom of Information Act of 2007 and the Privacy Act of 1974.

3.2.1 Cyberpayment System Models

Cyberpayment systems currently are structured in four standard ways – the merchant issuer model, the bank issuer model, the non-bank issuer model, and the peer to peer model.

3.2.1.1 The Merchant Issuer Model

The simplest of the four models, this system is where the smart card issuer and seller of the service or good is the same. A good example is where a user will place cash onto a

smart card that only is redeemable for a particular merchant and will not work with other merchants such as the Washington D.C. metro system.

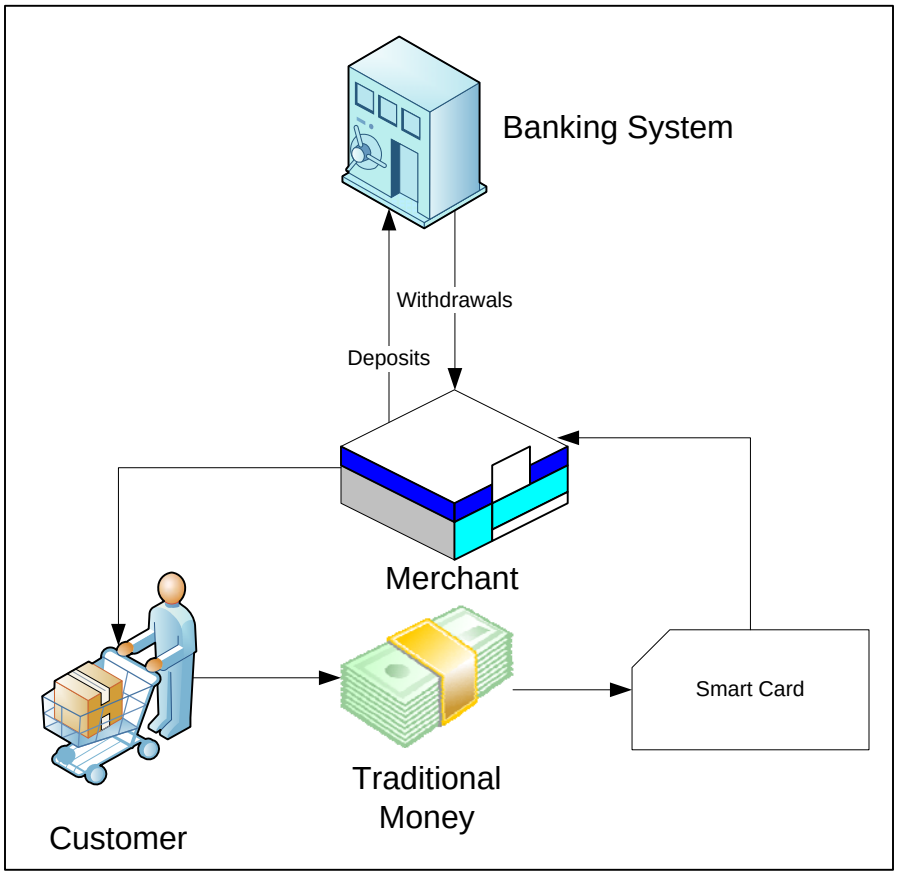

Figure 3. Merchant-Issuer Model

3.2.1.2 The Bank Issuer Model

This model is where the merchant and issuers of the smart cards are different entities. This is where the customer loads money onto a card handled by an issuing bank, and then uses it with a merchant who interacts with a different bank. The two banks report to a clearinghouse to transfer the balance. Preloaded credit cards by Visa, debit cards, and proton cards in Belgium are examples.

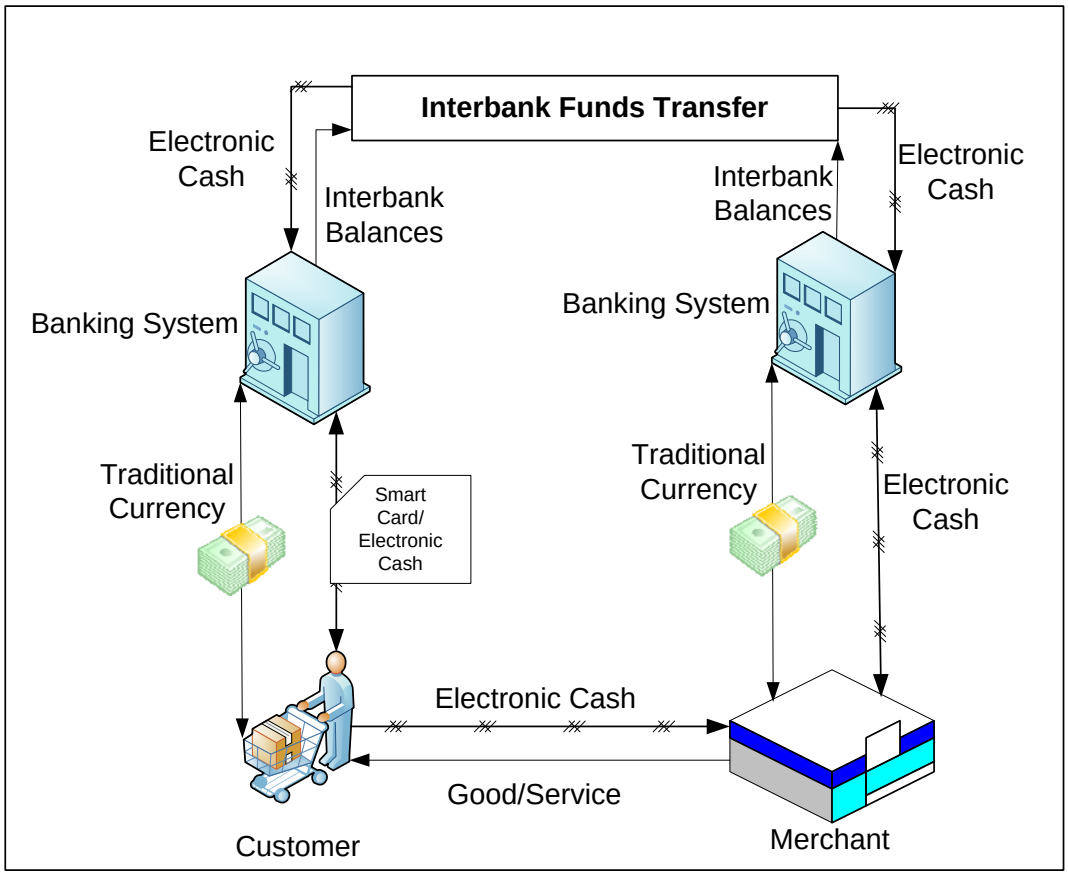

Figure 4. Bank-Issuer Model

3.2.1.3 The Non-Bank Issuer Model

This model is where users will buy electronic cash with traditional money and use it at participating merchants who accept that particular electronic cash.

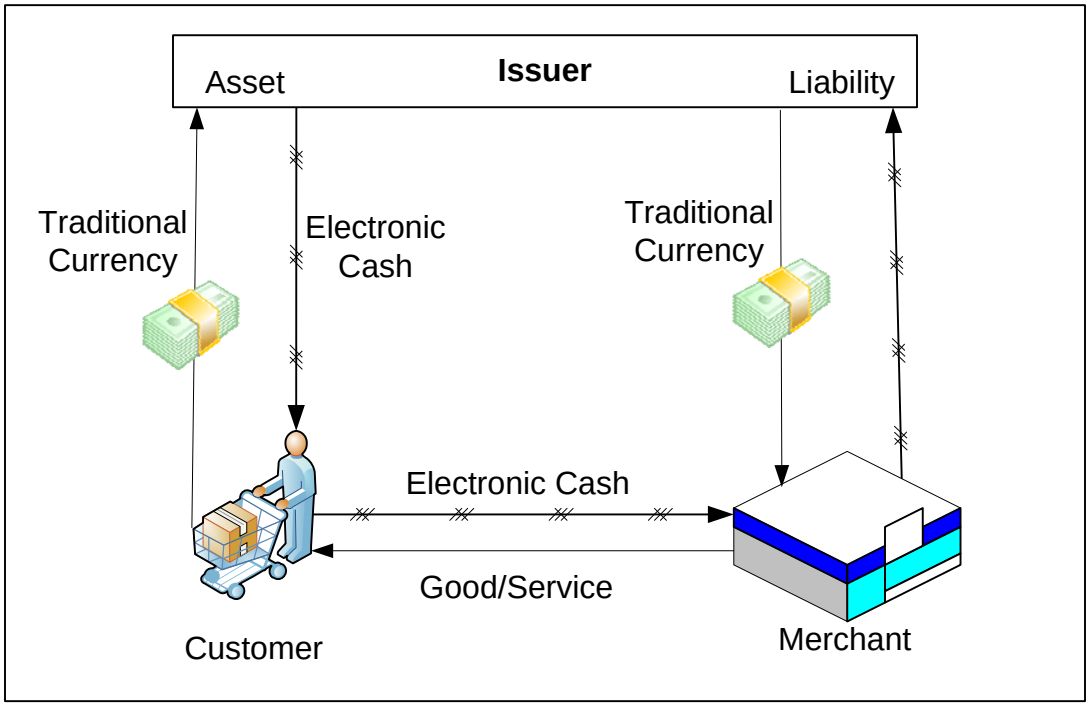

Figure 5. Non Bank Issuer Model

3.2.1.4 Peer to Peer Model

Electronic cash issued from banks or an entity that is not a bank can be transferred between users. The only time contact is established is during the conversion of traditional money to electronic cash and vice versa (during redemption). This sort of model is most susceptible to money laundering as there is no bank involved and conversions can bounce from person to person rapidly.

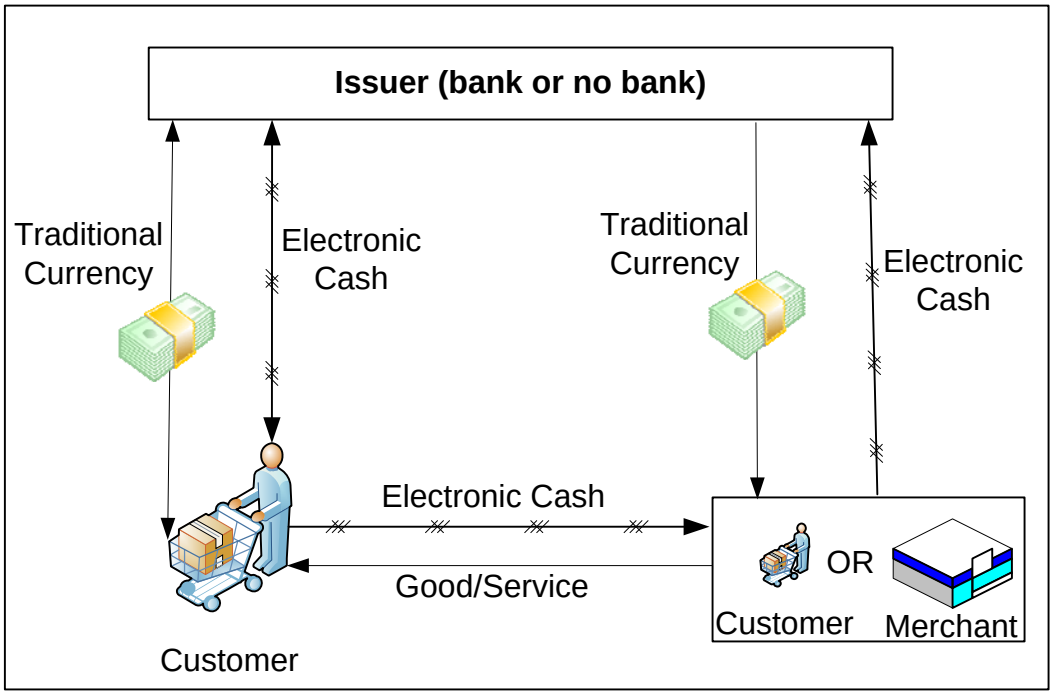

Figure 6. Peer to Peer Model

3.2.2 Developments in Cyberpayment Systems

Different areas of the world have been launching small projects through joint ventures with the credit card industry. Many of these have been value stored smart cards and online payment abilities. This will create an infrastructure with many different types of payment products.

Credit cards have been the dominant form of online payment for many years. The security in credit cards is performed through signatures, photos and Card Verification Value (CVV) numbers. Since credit cards are used more for illicit use of one's payment account, they are not the primary system for cyberlaundering. Ten years ago, the use of DigiCash by

David Chum was the primary method for laundering money by means of electronic currency [24]. DigiCash provided true anonymity by introducing a number of cryptographic protocols. DigiCash declared bankruptcy in 1998, and was acquired by InfoSpace in 2002 [24]. Currently, there are five electronic payment systems that are the front runners in electronic currency.

3.2.2.1 Virtual Wallet Systems

The major player in a virtual wallet system is PayPal. PayPal is a money transfer system that was launched for customer-to-customer transaction but has now taken on business to customer accounts at well. PayPal acts as an unbiased mediator offering low risk to both seller and buyer of the money. PayPal accepts money from the purchaser by charging the purchaser's credit card for any transactions, debiting a checking account for any payments, or having PayPal debit the purchaser's PayPal account that has a positive balance for the purchase. The personal information required to start a PayPal account is a name, e-mail address, credit card information, and billing address for a credit card. One interesting service that PayPal provides merchants is the ability upload a file with e-mail addresses and amounts, and pays the recipients in bulk. This PayPal tool could potentially be used for smurfing. Other virtual wallet services are PNC Virtual Wallet and Microsoft's Virtual Wallet.

3.2.2.2 Smart Cards and Stored Value Cards

German Geldkarte is a credit card sized plastic card with a computer chip embedded in the card. Payment information in the form of currency value is stored on this chip and can

be retrieved with card readers designed especially for the card. This feature makes smart cards independent from central servers and allowing anonymous transactions. Smart cards can store up to 80 times more information than magnetic stripe stored value cards [25]. Another major player in Smart Cards is Mondex. Mondex is an electronic cash system that has received ITSEC level E6 (Information Technology Security Evaluation Criteria's highest rating of security) [22]. It is known to be one the most secure alternatives to traditional currency. Mondex is a joint venture between Wells Fargo, MasterCard, AT&T Universal card Services, Discover card, Michigan National Bank, Chase Manhattan Bank, and First Chicago [23]. Stored value cards and smart cards are referred to interchangeably for the remainder of the thesis.

3.2.2.3 Escrow Services

Escrow.com, auctionchex.com, docdata.com, and iloxx.de are all major companies who partake in escrow. These are also known as "Customer to Customer Contracts" These services allow buyers and sellers to set certain stipulations online. After both parties agree to these rules, the escrow service emails the buyer, asking him to pay the amount for the service. The payment can be made via credit card, personal or business check, money order, cashier's check or wire transfer. This is kept in an escrow account, and the seller is informed via email to enter the site to get the shipping details. After the goods are received, inspected and approved by the buyer, the seller is paid by the escrow service for the goods. If the buyer is dissatisfied and returns the goods, the seller will also be given time to inspect and accept the goods as returned. In this case, the escrow service returns the money to the buyer. Based

on research, it seems that the level of security of escrow service is higher than smart cards and virtual wallet systems.

3.2.2.4 Direct Billing

Some systems use software that allows the user to make purchases, which are later billed through the Internet Service Provider or a phone bill. Most prominently are eCharge Phone, which is a web front end to the 800/900-premium rate telephone billing network. eCharge now also participates in creating virtual credit, debit and value storage allowing customers to make online purchases without releasing private financial information.

3.2.2.5 Micropayments

Micropayments are a means to transfer small amounts of money over the Internet. These payments are so small that credit cards or other electronic processing methods would be impractical to use for each payment. As a result, small businesses sprang up where users can deposit small sums of money ranging from a dollar and up, to be used on participating websites. The participating websites will extract small amounts of currency based on what the user is purchasing, and the micropayment company will perform larger debits from the customer.

3.3 Methods of Cyberlaundering

This section provides an overview for the methods of online money laundering that have been identified in literary review. According to these methods, network-based cyberbanking and stored value type smart cards have provided opportunities for money

launderers to conceal the movement of illicit funds. Identifying methods in which cyberpayment tools are used by launderers can help to draw a clearer picture for abuse within cyberpayment networks. These examples, along with the examples discussed in the next chapter, will help to determine the rules and regulations that need to be put in place in order to start mitigating cyberlaundering.

3.3.1 Electronic Currency

Non-fiat currency on the World Wide Web, such as digital gold currency (DGC) has been under scrutiny for proving to be a method to launder money electronically. DGC is a type of electronic currency that is based on gold ounces. This is very similar to the U.S. paper gold certificate was exchangeable for gold before 1933 [61]. DGC is not regulated – it is based on trust. As of April 2008, DGC providers held over 9.6 tons of gold as reserves to back up their currency [26]. This was 47% increase since January 2007 and worth approximately $280 million.

DGC offers global world currency as precious metals have international currency codes [27].

3.3.2 Online Casinos

Online casinos are defined as “the provision of opportunities to play games of chance or obtain access to sports of race bookmaking via computer networks”. While these networks are used for entertainment purposes, they have also provided a way to launder money quickly. The dirty money is played at the casinos, and the payment of clean money returned to the launderer. These transactions are done almost instantaneously and can be

done from home. Because the Internet is global, many of these online casinos do not fall under any particular jurisdiction. According to Forrester Research roughly 1,400 online gambling sites are in existence [32].

CHAPTER 4. HYPOTHETICAL CYBERLAUNDERING METHODS

Based on the research conducted on the methods of money laundering and the regulations imposed on them, along with the current cyberlaundering methods previously discussed, I have determined additional cyberlaundering methods that have not been yet mentioned. These methods become additional facets through which criminals can wash their money without jurisdiction or uncovering their identity.

According to John Wagner, the BSA/AML Compliance Officer for the Office of the Comptroller of Currency, one of the largest threats to money laundering currently is the use of stored value cards. As stated earlier, stored value cards represents money on deposit with the issuer, and are similar to debit cards. The difference between stored value cards and debit cards is that debit cards are usually issued to an individual account holder under name issuance, while stored value cards are anonymous. The first three hypothetical cyberlaundering methods involve using stored value cards. The remaining seven discuss other methods of cyberlaundering.

4.1 Stored Value Payments for Drugs

Drugs can be sold to users in exchange for disposable smart cards denominated in amounts typically associated with street drug transactions rather than normal money typically used in buying drugs. These smart cards would then be pooled by the street dealer where they could be then taken to a merchant. For a standard fee, the merchant would then upload the electronic value from the cards to a financial institution. Once the funds have entered a legitimate payment system, they are sent to a domestic or offshore account. This follows the

same process as the placement, layering, and integration phases of traditional money laundering.

4.2 Transferring Value through Cyberpayments

One practical way drug trafficking proceeds can be stored is through smart cards of high value. Some smart cards and stored value cards can hold fiat currency in the upwards of thousands of dollars allowing the trade of illicit funds to not only be anonymous but also allow easy transfer of large amounts of currency. These cards are smaller and weigh less than traditional currency, providing an incentive for drug traffickers. The cards are then disposed of through depositing the funds from the smart cards into an offshore bank.

A second way of transporting value beyond the reach of law enforcement authorities could be to transfer stored value over a telephone system or electronic online system that works with the monetary value on smart cards. Such products offer criminals a rapid and effective means for transferring and consolidating a stream of illicit funds. Once funds enter the payment system it is impossible to distinguish the illegal money from legal funds.

4.3 Transferring Value through Network Based Systems

Smart cards with a low balance have the ability to transfer their value onto personal computers, which would then transfer that value over the Internet, using increasingly available anonymous remailers to conceal the points of origin of illicit funds. Recipients could then pull the funding together and reintegrate the value into the payment system.

The ability to use the Internet in this fashion is troublesome – smart cards of small values generally are not seen as a threat. A launderer would keep the values low – perhaps

under $100 to prevent any sort of detection of the structuring scheme. These values could then be smurfed into accounts offshore where AML regulation is not as strict or in a financial institution where privacy of customer accounts are enforced.

4.4 Payments via the World Wide Web

This example of Cyberpayment system misuse involves a fraudulent not for profit business that only accepts electronic value as a means for donations. Funds collected for an apparently legitimate charity can be in actuality dirty money obtained by drug trafficking. These funds can be uploaded from virtual wallets, and then redistributed from one financial institution to another individual or group someplace else on the globe.

4.5 Blended Phishing

Phishing is not a new technique for the cyber world. Phishing is a criminally fraudulent process of attempting to acquire sensitive information by looking like a trustworthy entity [62]. Many of the old tactics of phishing are no longer working due to the increased awareness of this crime. As a result, criminals are becoming more devious in their phishing attempts. Not only will they use a familiar front to deceive someone, (such as mocking up a illegitimate website to seem legitimate) but perhaps use various techniques such as email, websites, and VOIP (Voice over IP) to mask the drop point of legitimate money.

A launderer, under this method, is looking for individuals to assist with smurfing illegal funds into an account. The launderer has an account with illicit funds that need to be moved to another account inconspicuously and without any flags. In order to do this, a

launderer will send out an email asking participants to deposit a certain amount of money into their accounts and move it to another account. The email can be spoofed to represent a different bank instead of the one that the money is coming from – the location of where the money is coming from can be fronted by a website, and with the use of voice over IP (VoIP), a launderer can also easily set up a number that users can inquire more about this "activity" to further enhance their trust in this process.

The assistant will then be asked to go to the banks site, and withdraw "x" sum of currency. This currency should be deposited into their account, and within a certain time frame, the currency should then be deposited or wired to a different account less a percentage. Since the assistant is obtaining a portion of the dirty money without knowing that the money is in fact illegitimate, there is not much incentive to report this activity.

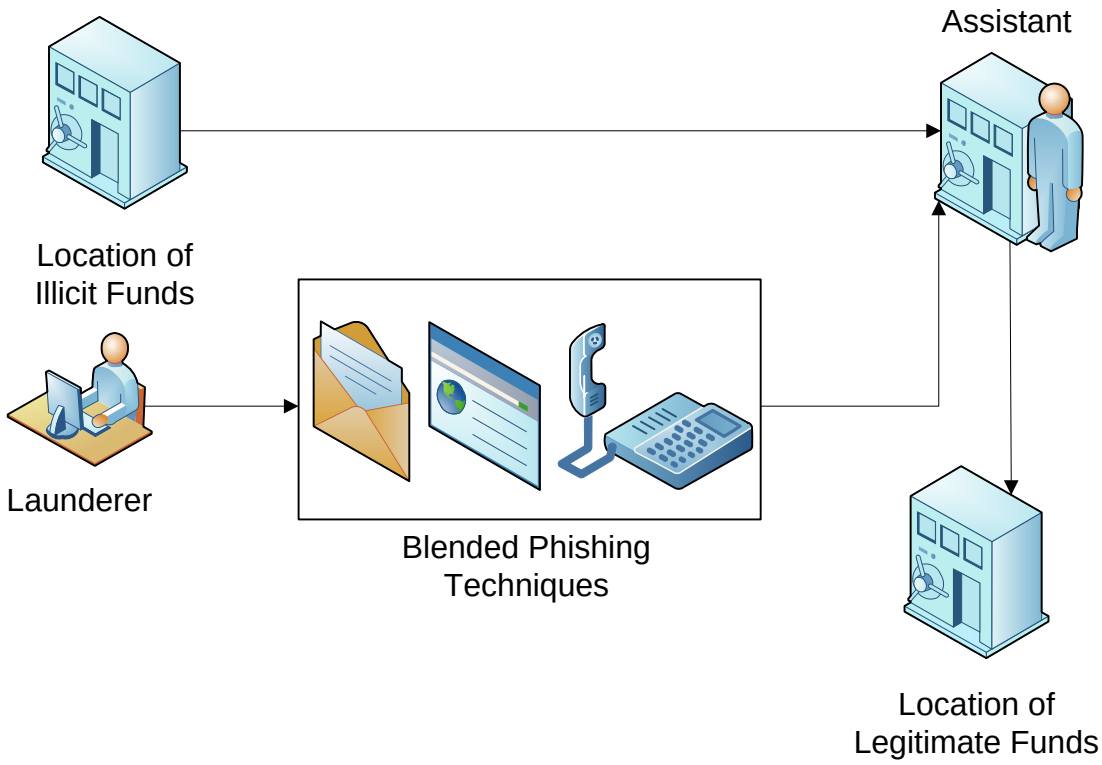

Figure 7. Blended Phishing Technique

Blended phishing works by spoofing phone, email, and websites in an attempt to fool a user into believing that funds from the launderer are coming from a location that they truly are not. In regards to VoIP, the launderer will spoof a caller ID, perhaps using the phone number of a bank they are pretending to represent, in an attempt to trick the assistant.

ANI, or the Automatic Number Identification, is a system in the United States used by telephone companies to determine the number of the calling party. Some VoIP companies will allow you to run your own Private Branch Exchange (PBX) which houses the ANI system. Configuring the files on the PBX will allow you to spoof any number to a caller.

Some of the current companies that support running a private PBX are VoicePulse and Nufone [31].

Email spoofing works by using telnet to access an exchange server running the sending mail transfer protocol (SMTP). Once a launderer discovers how to access a bank's exchange server, the launderer will send out an email that contains legitimate headers acting as a bank's email. Since many mass mailing emails do not encourage mailing back, correspondence can be done over the spoofed VoIP service rather than through email.

Web phishing, to a trusting user, can fool someone into accessing an illegitimate site to further prove the validity of the funds. A launderer could set up a phishing site to perhaps lead an individual into believing that funds are coming from a particular bank. This can be done through content theft of a legitimate site, and setting up a URL with a similar name. Another method would be to perform content theft of a legitimate site, and then poison the DNS Cache in an attempt to relay the IP address of where the attacker's fake site is to a valid domain name.

With careful planning and structuring the use of different phishing entities, social engineering is a harmful threat in acquiring an individual to participate in a money laundering scheme. If a launderer can utilize participants only once, then banks do not file SARs for moving money from one financial institution to another under the amount of $3,000 USD [13]. Furthermore, a launderer can set up shell companies and have the money deposited into an online bank not regulated by the United States. The deposits would look like legitimate income for the shell company.

4.6 Botnets

Botnets are group of software robots that run autonomously and automatically. The robots or bots are generally running without the computer owner's knowledge. These bots can be downloaded through malicious email, malformed images, embedded in additional software, or just downloaded and executed through a computer.

Botnets are controlled by a "bot herder" or an individual/group who knows how to command the bots to perform certain activities on infected computers. Bots can do anything from send spam to delete files off of your computer. In this scenario, the bots can be used to launder money through ones banking system in an attempt to obtain clean money.

In 2004, a bot was discovered to be transmitting the keystrokes of infected computers to a chat room on the Internet Relay Chat [30]. These bots can be used to compromise username and log in information of an infected person's machine into their online banking system. As a result, a bot herder would then be able to access the bank account of the infected user, and wire money into a compromised machine's account and then out to their account. To the user, it will just look like a mistaken withdrawal and corrective deposit.

One of the more popular bots that enable traffic sniffing and keystroke logging is Agobot. Agobot is written in C++ and released under a GPL license. Due to its high modular structure, creating new functions for the bot is easy to do. Agobot in this scenario would be created with a keystroke logger and record all instances of a key stroke. It would be supplied within an Internet Relay Chat server and channel information to relay the logged keystrokes back to the bot master. The channel is secured, and a list of authorized users is provided (the names of the users who can control the bots).

To infect a computer, the launderer could simply exploit the vulnerability of an operating system or service. Malformed HTML files that exploit Internet Explorer vulnerabilities, or Peer to Peer Direct Client to Client file exchange can be used as well. Once a bot is installed, the first thing that it will do is update the registry key found at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ in order to start with Windows. From there, the bot would connect to the IRC server and begin sending keystrokes out to a channel. When a user types in a common website URL to a bank, this information will be transferred to the launderer.

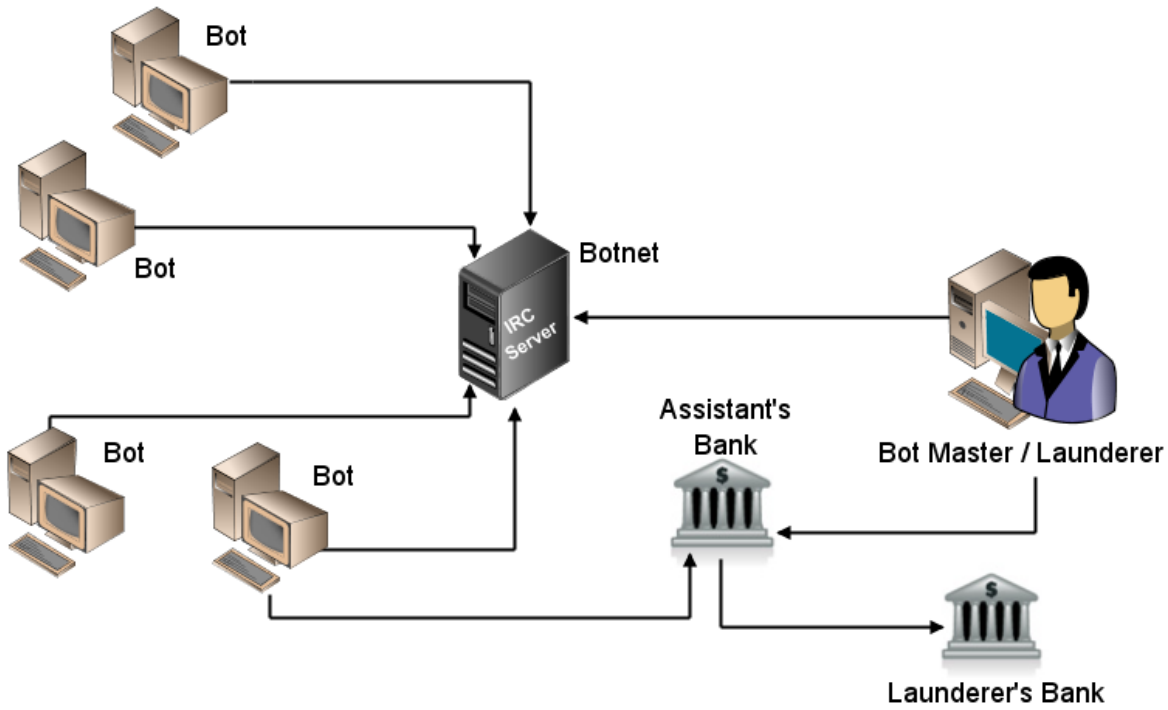

Figure 8. Botnet Laundering

Having access to an online bank account, the launderer could then deposit funds into the user's bank account and then transfer them out as a payment to a shell account. The online deposit and withdrawal of funds can be quick and small, which might not even tip off a bank. Furthermore, if a deposit is made into an account, and the same amount is then withdrawn, the owner of the account used to launder money is likely to assume the deposit was simply an error and not inform the bank concerning the activity.

4.7 Micropayment Smurfing

The placement stage of money laundering is the most important stage. If the placement aspect is done quickly, as this is the argument for the dangerousness of cyberlaundering, the layering and integration stages will become more difficult to discover as well.

With this in mind, one area that money launderers might exploit is the area of micro-payments and micro-loans. Micropayments refer to low-value electronic financial transactions, ranging from a fraction of a cent to a few dollars [33]. Amazon.com has a patented one click payment system as a service to smaller websites. Visitors to these sites can donate to the website host by clicking through Amazon's service. Amazon in return will take a percentage of the donation and a service fee [34]. Micropayments on the Internet make far more sense in a medium where margin costs are minimal. This has unleashed focus by programmers and web site designers. Initially micropayments became Internet phenomena when websites and companies would pay affiliates, other websites that offered a hyperlink and/or banner ad to the paying website. Often these payments were fractional per actual click

through. For example, company X pays company Y a few dollars for every one thousand visitors that are funneled from company Y's website to company X's site.

The new phenomenon are companies who allow a user to set up an uninsured bank account on line to pay for small finances such as buying points for an application on an online system such as facebook for a dollar or less. Such a system could work by a launderer setting up an account or multiple accounts with a micropayment system, and then creating

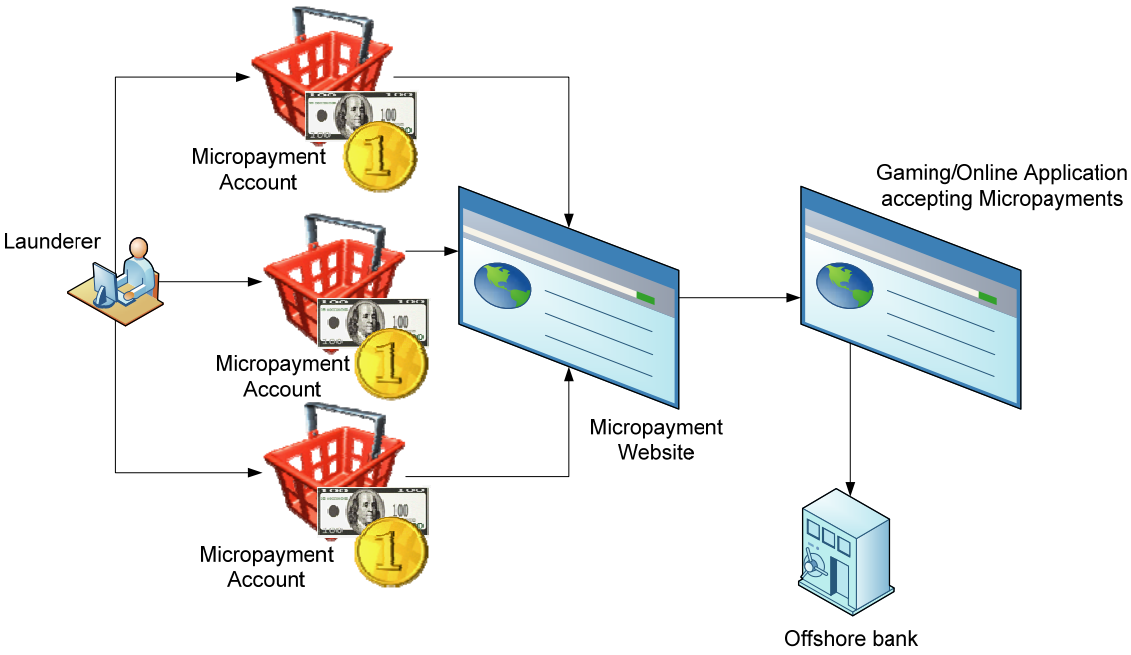

Figure 9. Micropayment Smurfing

some application on line where the illicit funds could be used. A launderer could create an application that would accept these micropayments and therefore provide legitimate receipt for the funds. Furthermore, the system could drastically reduce the ability of law enforcement to conduct Geographically Targeted Orders (GTO).

4.9 Return Merchandise Scheme

As of last year, 875 million consumers have shopped online. The number of Internet shoppers is up 40% in two years [35]. Billions of dollars are exchanged for goods and services per year solely off the Internet and that number is rapidly growing as people obtain and rely on the Internet more frequently. The majority of these online stores allow returning merchandise and herein lies an illicit way to launder money. As stated earlier in the thesis, legislation to prevent money laundering is placed at many of the "large purchase" corporations – real estate, casinos, and precious metal dealers. Making small purchases to launder money was not beneficial to a launderer, and therefore legislation had no need to place this legislation on companies who sell items valued around $500 or less.

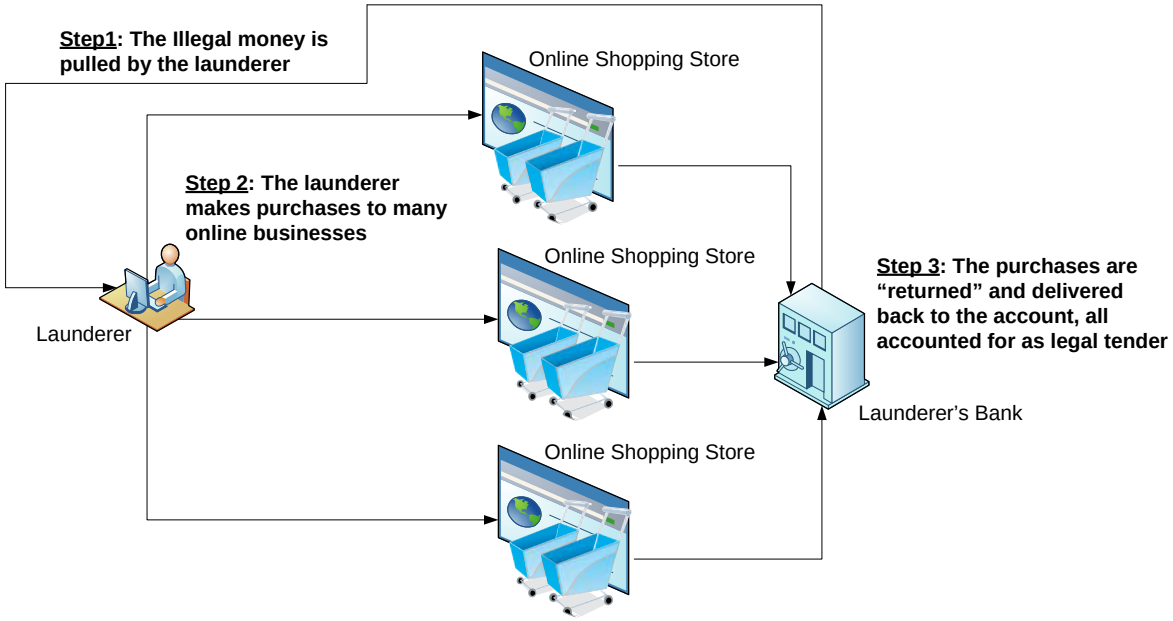

Figure 10. Return Merchandise Scheme

With the advent of the Internet, a launderer can structure smaller amounts of money through legitimate online businesses quickly. For example, a launderer would make a purchase of 25 toys at an online toy store of $20.00 each. This payment of $500.00 could be done at 100 different stores around the globe, allowing a launderer to place $50,000 of illicit funds into the system. The launderer could then ask for a return on the merchandise, integrating the funds into legal tender. This sort of movement would be too difficult for a launderer to do without the Internet – he/she would need to physically visit each shop. This would raise suspicion as well as the activity would be too time consuming.

In chapter 6, a suggested tool is briefly introduced to mitigate this method of cyberlaundering. It would require merchants by law to participate in a money laundering detection system. The system would not create much overhead for the businesses. Rather, it will provide extra security for an online business to not fall into facilitating cyberlaundering.

4.10 Online Stock Trading

Online stock trading is becoming a bigger phenomenon each year. Companies such as Ameritrade, E*Trade, Scott Trade, and Trade King are providing ways for their customers to purchase Initial Public Offerings and other stock options without the need for a personal broker. These online methods of purchasing stock leave out a great deal of human interaction that once was a part of buying and selling stock. As a result, the buying of stock with illegal money and selling for legal funds is a valid method for online money laundering.

A launderer will place funds into multiple accounts with an online trading company. This money will then be used to buy stock which is the layering portion of the laundering scheme. Once the money has been used to purchase the shares, the launder will sell the shares thereby obtaining legal currency. From there, the funds can be withdrawn from the online stock company and placed into an account offshore, where the money is not subject to anti money laundering regulation and is seen as legitimate cash from selling stock online.

CHAPTER 5. CYBERLAUNDERING LEGISLATION

Title III of the US Patriot act has provided a higher level of enforcement for facilitating the prevention, detection and prosecution of international money laundering at the level of banking regulations, record keeping, smuggling and counterfeiting currency. Furthermore, all regulations such as the Money Laundering Control act of 1986 and the Bank Secrecy Act of 1970 are in place to mitigate and enforce money laundering primarily at the banking level. To date, there is not much legislation on money laundering at the cyber level. When dealing with creating rules and regulations at the cyber level, issues such as intellectual property, privacy, freedom of expression and jurisdiction all take part in money laundering over a computer system. The FATF has begun to focus their recommendations to include a more cyber crime centered approach, but has not fully deduced solid legislation on how to mitigate, deter and bring justice to those who launder money through the use of a connected computer system.

This chapter talks about three issues that impact the cyberpayment and cyberlaundering system. From there, I will discuss other policies and suggestions for cyberlaundering legislation.

5.1 Law Enforcement Issues

There are two areas that make up the law enforcement issues dealing with cyberlaundering. The first is the value of cyberpayment tools to a cyberlaunderer and other parties who are trying to hide financial activity from government oversight. The second area is the response that law enforcement should have towards those abusing cyberpayment

systems for cyberlaundering and how computer investigative techniques will be used to find patterns of abuse. Furthermore, issues such as law enforcement jurisdiction, privacy, and collaboration with other agencies all are a part of this section.

To be fully successful in enforcing cyberlaundering, the federal or state government must have access to the cyberpayment transaction information. The current rules that oversee wiretapping and auditing of financial records from regulated AML institutions can provide a "hook" for additional law enforcement regulation. Due to the fact that cyberpayment systems are a key system in modern society, they should have a higher transparency and accessibility to the law enforcement agency. As online currency is equivalent to traditional currency, those who issue cyberpayments must have the same level of supervision from the government as do the brick and mortar banks. Furthermore, those conducting illegal money laundering online should bear the same repercussions as those doing it physically.

From a perspective of enforcing law, there needs to be a specific pattern of collaboration with financial institutions through a rewrite of policy that includes the new system characteristics of Cyberpayment networks. As discussed in section 2.5.1, sections 1956 and 1957 of the BSA outline over 20 unlawful money laundering activities. This section should be amended to include cyberlaundering activity. A good interpretation of legal and regulatory procedures on how government would have access to the cyberpayment system and the records of financial activity should be created and modified as cyberpayment systems evolve. The issue that can been seen is the approach of enforcing law reactively, and perhaps this can be mitigated by any new cyberpayment system to comply with base

requirements of providing information to the government on how to access information out of the cyberpayment system, how best to detect fraud, and how to monitor internationally transferred funds.

The law enforcement practice that is mentioned in this section raises major issues for consumer privacy and what investigative practices are acceptable under the current constitution. There should be specific policies in place for monitoring a particular cyberpayment system. If the monitoring is more invasive than what current law allows in order to fully prevent cyberlaundering, then customers of the system should be notified of this within the terms of service. Targeted investigations could be done similarly to how Finsen completes GTOs (Geographic Targeting Orders) to carry out current money laundering investigations. These investigations would hone in on individuals records and therefore provide better evidence that cyberlaundering is taking place. This will be talked about more in section 5.4.

5.2 Issues in Regulation

The regulatory issues in cyberbanking to prevent cyberlaundering can be easily mitigated if many of the existing rules that are imposed on banks such as compliance with the Bank Secrecy Act and the current U.S. Patriot Act laws were also imposed on cyberpayment systems and many of the large online businesses. If online businesses need to comply with the anti money laundering laws, they could explore the idea of providing their customers the online currency.

When talking about regulations of cyberpayment systems to mitigate cyberlaundering, there are two main subjects. The first is coordination on an international front that would have the oversight of all cyberpayment systems. This might be an extension of the FATF that creates regulations, or perhaps an official body in conjunction with Interpol, but its main role would be law enforcement and auditing. The second is the legal understanding that cyberpayments play as an important contender as an addition to the economy.

As far as those who have the legal authority to issue cyberpayments, this should rest on a mix of public and private partnerships. In order to better mitigate cyberpayment misuse the number of entities that could issue cyberpayment values should be limited. Perhaps only banks and Money Services Businesses (MSBs) should be able to participate. An alternative to this would be to allow only financial institutions who are regulated tightly with law enforcement (BSA/AML regulations, etc.) be able to issue cyberpayments.

I find that there are four areas in cyberpayment systems that should be regulated by the government in an attempt to mitigate cyberlaundering. First, is the frequency and size of transfers of above a certain value from one person to another. Though many wire transfer companies already mitigate this, there is no regulation from government that caps the amount of money and number of transfers that can be sent from one entity to another. Second are the records of transactions. Under the U.S. Patriot act, brick and mortar banks must hold records of an account for seven years after the removal of their last account. This policy has proven to be helpful in locating money laundering operations and terrorist financing. If this policy was in place for cyberpayment systems and audited in a similar fashion as what the Bank

Secrecy Act calls for, then the misuse of cyberpayment systems can be mitigated as well. Third is limiting the monetary value of stored value cards. If the value of these cards is minimized to only allow values comparable to the efficiency of the business that they are intended for, then this would minimize the ability for drug dealers and money launderers to utilize this anonymous cash as a way to perform their illicit activities. Fourth, would be the number of transactions that would be able to take place on a cyberpayment system such as a smart card. For example, if a user of a smart card adds or deletes currency more than three times in a given day, then the card will no longer work unless approved by an official of the cyberpayment system. This would not only mitigate the use of the card by the consumer, but would allow a system or an official of the system to place a suspicious flag on the card or even submit an electronic SAR on a user of the smart card when the customer tries to exceed the number of uses.

Furthermore, there are four outlying areas that need to be addressed when creating regulations on the cyberpayment systems. One is how the confidentiality and privacy of the consumer will be adhered to. If there is not a targeting order on an account, then there need to be rules and regulations against the ability of enforcement to open and review logs of a cyberpayment system. Furthermore, the second area that needs to be regulated is the necessity for limitations on law enforcement's access to information in a cyberpayment system. This will prohibit unreasonable surveillance and intrusion of privacy. Third, the cyberpayment system's stability needs to be regulated including its ability to be purchased by another entity if needed (the liquidity of the corporation). Lastly, there needs to be regulation that protects the consumers of the cyberpayment system. It needs to be documented and

understood that the features of the cyberpayment system will not disclose possibilities of information access.

5.3 International Coordination with Policy

Due to the nature of online cyberpayment systems, in order to implement a successful anti money laundering policy, there needs to be a high level of cooperation internationally. Most cyberpayment systems are designed to be international, and therefore long term regulations that are imposed on them should be international as well. If there is to be a commonality of cyberpayment system policy, then there would have to be a convergence on technical and operational standards. These standards should be similar and under the same sort of rules that currently govern anti-abuse and fraud. Because there has been a lean towards equal trade rules for the import and export of goods and services, there should be equal rules to the cyberpayment systems as well. The international standardization of the trade rules has created economic growth. This provides solid rationalization for the government to create an international cyberpayment system.

The issue however is that when the government intervenes in the system as to enforce the laws, this is a defensive approach and can hurt the business of cyberpayments as far as competition is involved. To mitigate this, there should be room for creating individual compliance – much like the structure of the current Bank Secrecy Act. This way, there could be more room for innovation in the cyberpayment industry as long as certain evaluations are performed such as bi-annual audits from an international working group.

5.4 Suggestions for Mitigating Cyberlaundering

Law enforcement, regulation, and international coordination are the three major issues that need to be addressed when establishing cyberlaundering policy. This section will discuss some suggestions to mitigate cyberlaundering cohesively.

5.4.1 Keeping Records

The most major component to mitigate cyberlaundering is keeping records of who is buying and using stored valued cards, making online purchases and returning the merchandise, and who is using micropayment systems and other cyberpayment services. The first suggestion to tackling this issue is that all cyberpayment systems and merchants who provide a consumer with the ability to purchase merchandise valued at more than $3,000 USD in a period of two weeks should be required to develop and maintain a "Know Your Customer (KYC)" policy. This policy should be synonymous with the KYC policy in place for financial banks in the U.S. Within KYC, a Customer Identification Program (CIP) should be required. The CIP program must be developed with a clear understanding of all the possible money laundering facilities within that system. For example a CIP program would include information on the customer such as the type of account that is being offered, how the accounts are being set up, and other information that can identify customers to the best ability. This information in a cyberpayment system could be the following:

- Information on the ISP that the account was set up through including the IP address
- Information on the ISPs where the account was used (where the accounts are being logged into to make transactions, etc.) including the IP address

- If the cyberpayment allows for account maintenance through the use of a phone service (such as customer service), tracking the location of where the phone calls are made.

One other suggestion for mitigating cyberpayment systems online is to only allow customers whose ISP has a relationship with the cyberpayment system to use the cyberpayment system. This does limit the client base of a cyberpayment company, but may be necessary to better mitigate illicit activity such as laundering electronic currency. A relationship such as this could mitigate anonymous use of the cyberpayment system such as launderers trying to use a proxy to hide their location and provide false information. Furthermore, ISP relationships could assist with record keeping. An ISP who would want to provide a more secure cyberpayment system would be required to maintain a registry of subscribers with appropriate identification information, maintain a log of traffic information with the IP address, maintain these logs for a certain period of time, and also provide this information to the cyberpayment system when needed to match logs to detect and flag suspicious activity.

5.4.2 Authentication

One of the largest issues in the cyberlaundering is how to prevent the misuse of credit systems such as smart cards or stored value cards. One possibility is to introduce the use of a biometrics system into the smart card. The biometric system could provide an alternative measure to locating the origin of the currency. Furthermore, the currency may not be able to be used until another biometric scan is performed. Such a system may fall under privacy

scrutiny and would not be adapted to the fullest extent. An alternative that might work better as a commercial cyberpayment system is to re-introduce an authentic mechanism of anonymous cash where the anonymity has the ability for revocation.

The e-gold electronic banking system provided electronic currency, but the only information necessary to open an account was an email address [36] which ultimately led the company to be indicted by a federal grand jury for laundering. Since this incident, along with the bankruptcy of DigiCash run by David Chum, the notion of anonymous digital cash has not been clearly defined. However, it is still a valid possibility of implementation if regulations, law enforcement, and other attributes explained in this thesis are implemented. E-cash should not be confused with digital money that provides a paper trail. This currency however can only work if the bank issuing the currency is also the same bank where the currency can be deposited. This way, if the cash is used to make illegal purchases, then the bank can trace where the money came from. Furthermore, if the depositor tries to structure the funds by depositing the currency into separate accounts, the depositor can be identified. The idea to this method is to provide an algorithm that would provide anonymity when one customer is transferring the currency to another customer. Anonymity of the source of the currency (if the depositor is using the funds illicitly) and anonymity of the depositor is kept if the initial withdrawer is using the funds anonymously.

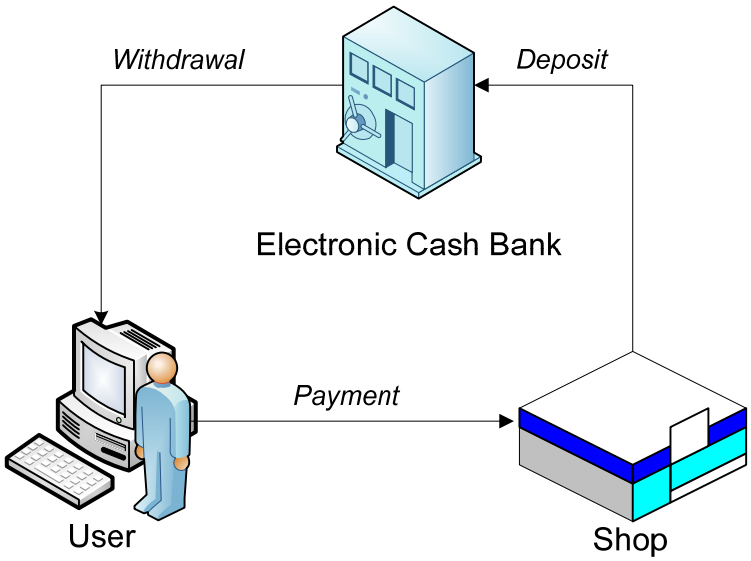

Figure 11. Simple Electronic Cash Arrangement

The three major money wire transfer systems (SWIFT, CHIPS and Fedwire) for the banking industry use heavily authenticated protocols to securely transfer currency from one financial institution to another. The methods are known as Financial Cryptology (FC) and incorporate blind signatures as well as strong RSA encryption. Similar methods can be applied to authenticate users for a cyberpayment system. The use of Kerberos, certificates, and digital signature algorithms can all play a part in authentication. Certain open source modifications to the Kerberos system can be installed on a machine that wishes to use cyberpayment system. This could provide a higher level of authentication to prevent illicit misuse of the cyberpayment system.

5.4.3 Tracking & Trigger Systems

In order to mitigate cyberlaundering, it is imperative that a cyberlaundering system houses classifier systems along with data mining tools that utilize artificial intelligence algorithms to raise flags in the event of suspicious activity. In order to preserve the anonymity of cyberpayment system users and stored value card users, data that is running through these systems shall not be disclosed unless a flag is raised. With the use of good artificial intelligence systems, suspicious activity can be detected early in a cyberlaundering scheme.

There is a necessity for an online banking system to prove due diligence of compliance with the international cyberlaundering laws. This can be enforced by proving to federal auditors that a cyberpayment system runs such a system by means of a continuing or random audit. The way that this can be done is by artificial intelligence (AI) to match activity into a chain and compare it to historical information in the same account along with comparing it to other cyberpayment accounts in the same group. When locating suspicious chronological transactions, the ability to target fraudulency is much easier than targeting one's user account. A deposit of $7,000 may not be suspicious but a multitude of $7,000 deposits may. Furthermore, by comparing the transaction chain with historical data, it may be feasible to locate suspicious activity by the trend in transactions rather than setting human thresholds, such as $3,000 to $10,000 USD (Which are thresholds for CTRs and SARs in the brick and mortar banking industry). A further advantage to instigate AML AI is that the data mining methods can uncover laundering techniques such as structuring and patterns of

laundering activities. In chapter 6, elaboration on specific data mining tools that could be used will be discussed.

One suggestion for tracing currency through a cyberpayment system is to create the ability for an international law enforcement group to order the tracking of a computer network system. This would be exclusive to a particular system or group of cyberpayment systems in proximity of each other. This order would be very similar to Geographic Targeting Orders (GTOs) issued by the U.S. Department of Treasury. GTOs would fall under laws such as the Bank Secrecy Act here in the U.S. The capability would be built into the cyberpayment system as a "traceable" protocol if there are means to do so. For example, a stored value card could contain a log listing of recent activity and the values on the card. This activity would be tagged onto the card itself and contain other information such as the time that transfers occurred, and the identity of the receiver of the value. Within a cybersystem, a tagging infrastructure would occur that contains the flow of funds, and the recipients and originator of the cybervalue system. In addition to tagging stored value cards and E-cash as funds move through a cyberpayment system, Internet protocol (IP) tunneling techniques such as IPSec protocols or VPN could be utilized to not only provide enhanced security of the cyberpayment system, but also provide law enforcement with a simpler method of tracing funds that might be associated with cyberlaundering. A suggestion would be that tags would be placed on the transfer messages. The two IP addresses (sender and receiver) would create a link. Any severs that use TCP/IP with the tagging function would maintain logs for law enforcement. This information could be sent directly to a secure central server where other tests could be run such as AI algorithm checks. The action of

checking the traffic could only be implemented under rules clearly laid out in the Bank Security Act regulations.

5.4.4 International Database for Financial Intelligence

As stated earlier, coordination from all nations is imperative to effectively mitigate cyberlaundering. One strategy that an international group can implement is establishing a database housing suspicious activity from cyberpayment systems in an effort to follow illicit users on a global scale. The database would need heightened security due to the sensitivity of such a central system. This can be done by only allowing authenticated authorized users into the system and providing layered security to keep criminal activity away.

An aspect of the "Know Your Customer Policy" at financial institutions is to verify that a customer is not on money laundering list or other illicit activity list such as the Office of Foreign Assets Control's Specially Designated Nationals [44]. This list contains thousands of entries and is updated at least monthly. An easy step to mitigating cyberlaundering is requiring cyberpayment systems to check this list as a part of a cyberpayment system's KYC policy.

The cohesiveness of such a system will play a vital role in creating an environment where cyber currency can exist, while maintaining low risks of illicit activity. The following chapter presents a specific tool that can be used to detect a return merchandise scheme. It relies on a central database system protected by government. This sudo-black box system will raise flags and only allow information to be monitored when needed.

CHAPTER 6. CENTRAL ONLINE AML MERCHANT ENFORCEMENT TOOL (COMET)

COMET, a **C**entral **O**nline AML **M**erchant **E**nforcement **T**ool is a hypothetical system that mitigates and flags suspicious cyberlaundering activity that utilizes the buying and selling of merchandise from online realtors. As mentioned in section 4.9, the return merchandise scheme would provide a method of structuring illicit revenue online through the use of online stores. By creating a secure international record keeping system, this method of cyberlaundering would be better mitigated.

6.1 Overview

COMET is a data collection system that houses the transactions of customers who buy goods online. When any purchase greater than $500 is established at an online store currently participating in the COMET system, information about the transaction and the account to which it was created is sent to the COMET system. Furthermore, any transaction where the merchandise is returned by the customer is sent to COMET as well. This is done in all participating online merchant systems to detect possible structuring by a cyberlaunderer.

Sequence matching and other data mining techniques are performed as regularly as possible to locate any trigger activity that relates to cyberlaundering. Once a flag is raised, the system sends the appropriate information to law enforcement that can then begin to monitor a customer who may be involved with cyberlaundering. This tool solely cannot be

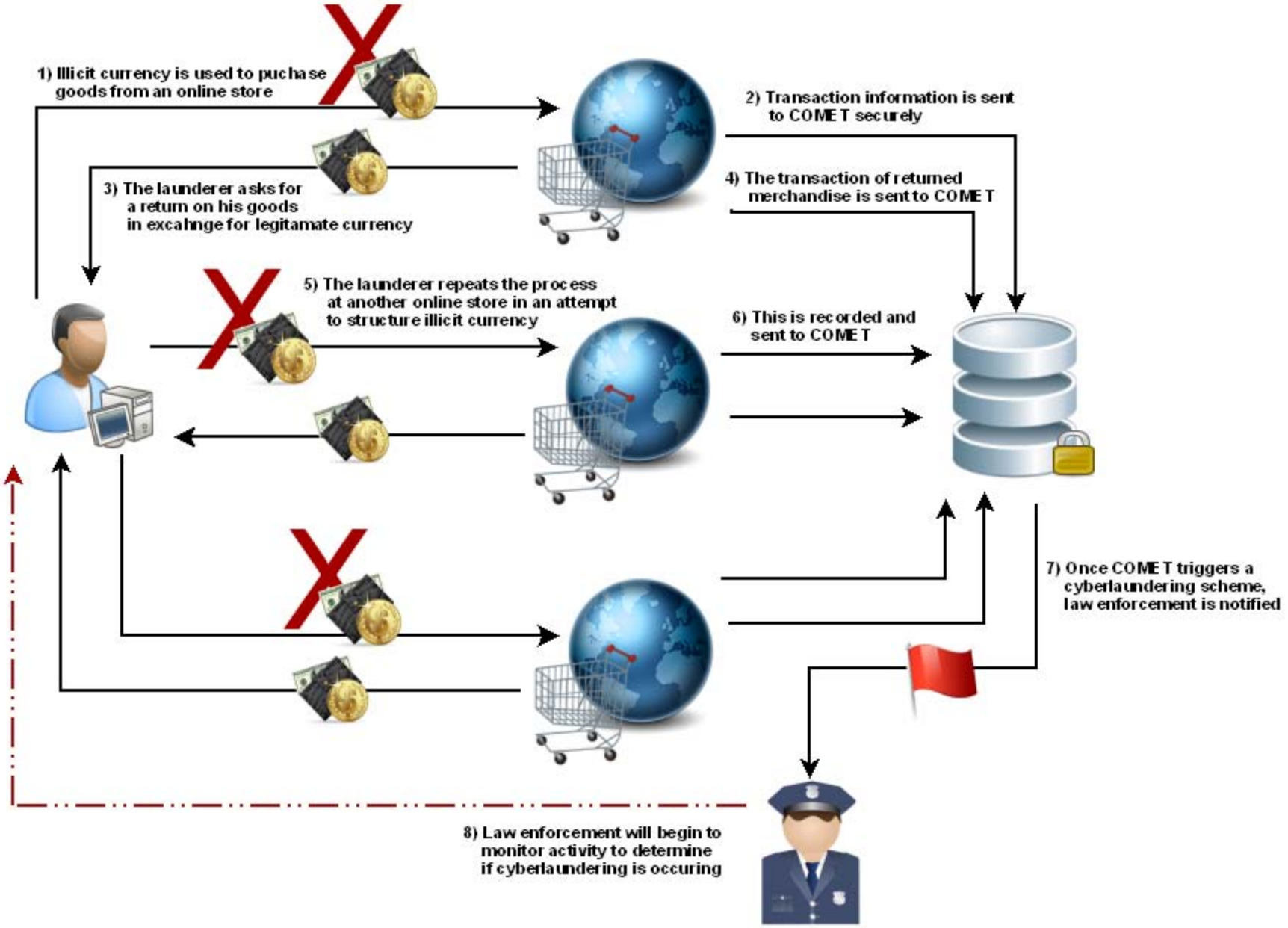

Figure 12. Overview of the COMET system

used to directly locate and persecute a launderer or a laundering group, but rather as another piece of evidence to locate and persecute those who engage in cyberlaundering.

6.2 Design Specifications

In order for COMET to work properly, it is essential that the cyberlaundering behavioral patterns and the network's structural features perform as accurately as possible, limiting the amount of false positives found by the system. Currently, many of the large Financial Money Laundering Software in the industry such as "Fiserv" uses various artificial intelligence mechanisms to automatically generate Suspicious Activity Reports. Furthermore, network intrusion systems such as SNORT and RealSecure Guard by IBM use artificial intelligence as well to detect malicious packet activity. The same artificial intelligence algorithms that exist within these programs, decision tree and Bayesian inference, can be utilized to locate and rank cyberlaundering based on probability computations. Furthermore, the design should be able to perform link analysis in order to identify groups of members along with group interaction patterns. Additionally, regression and case-based reasoning could be included which would reveal possible leads and trends timelier. Support vector machine (SVM) mining technology may be used for the system as SVM helps with mining highly assorted data sets [38].

In order to recognize cyberlaundering activity, data preparation is necessary. This step in the process involves collecting data, pre-processing data, and restructuring the database. Data is created by comparing the transaction records of unusual activity to those that merit normal behavior. The use of support vector machine learning theory can be used

as an alternative to the rule based data filtering system that has been implemented in AML software created for the banking industry. Furthermore, data is often noisy and may require database restructuring to allow for better identification of entities along with finding links and structure hidden in the transactions.

6.2.1 Data Collected

Traditionally, money laundering software at banks generally collect suspect information such as name, address, social security number, state identification (such as a drivers license), relationship to the financial institution, date of suspicious activity, dollar amount, and a summary characterization of the activity. In a cyberlaundering system such as COMET, those materials other than driver's license and social security number can be sent to the database system since most online merchants have no need to collect this information. If a company did ask for it, that might discourage a user from making purchases with that company. Other information should be included for the tracking of a person laundering money using this online method such as IP address information, customer account information, purchased goods, monetary value of the purchased goods, what denomination the money was in, how the goods were purchased (e.g. E-cash, credit, or direct banking withdrawal), and geography.

6.3 Security of COMET

COMET's security can be discussed in two areas. One is securing the transmission between an online merchant and COMET. The other is prevention of a data breach by not

only unauthorized users but also law enforcement using the system to mitigate cyberlaundering.

When a merchant signs on to participate in the COMET system, they are verified with an international anti-cyberlaundering working group as a legitimate business. Physical location and evidence of legitimate activity is required. Once this is confirmed, the merchant is set up with a virtual private network account making use of IP tunneling protocols. Certificate validation is performed, and the tunnel will stay open unless requested by the merchant to close for explained purposes. Requested information from the merchant is sent to COMET as part of the transaction process, and a response from COMET that the information has been received is sent back. If for any reason the transmission fails COMET technicians will be notified, and the request for the information will be asked from the merchant at a later time. The suggested method of encryption is the use of Pretty Good Privacy (PGP) to sign the information sent to COMET. As of 2009, there is no known method for effectively breaking PGP or performing man-in-the-middle attacks once the certificates were exchanged.

The COMET database will be housed at one central location. Replication of the system will be performed for disaster recovery purposes and will not be active in mining for data relating to cyberlaundering. The database is set up as close to a black box as those working with it and law enforcement that does the investigations do not know the data mining algorithms COMET uses to raise triggers. COMET only accepts input from merchant authentication, and relays cyberlaundering triggers to those who are responsible for carrying out investigations on cyberlaunderers.

6.4 Investigative Triggers

Laundering money through the use of online business entities is rarely performed under the same labeled account from multiple online merchants. Rather there is a behavioral pattern that occurs over time involving sets of real world entities.

Traditionally, anti money laundering detection had two categories: usual legal activity and unusual illegal activity. The issue with this was when two different people were engaged in a similar transaction, one person might be found guilty of money laundering while the other was not. This is because money laundering is a motive of wrongdoing rather than an actual criminal activity. "Usual" and "unusual" activity is a relational choice based on behavioral activity where "suspicious" activity is a varying judgment call based on the legitimacy of a transaction. The idea of COMET is to not only associate rules of triggers based on the customer, accounts, products, geography and time, but to use artificial intelligence to better determine suspicious activity based on records of merchandise bought and returned.

Because expert rules cannot effectively determine the probability of a suspicious transaction, each suspicion indicator needs to be weighed, scored, and ranked in order of severity. The uniqueness of COMET is that the perspective of raising a flag is subject oriented rather than transaction oriented. Customer due diligence should focus on finding and determining behavior patterns rather than learning from simple background knowledge. To improve on locating these behavior patterns, COMET will not only look at transactions made to trigger an investigation but also to accounts and users in where abstractions pulled from data consolidation where similar information is used to create clusters.

6.4.1 Network Forensics

Once an account has been flagged and enforcement has been notified, methods used in network forensics make it feasible to trace and physically locate a launderer. As discussed earlier in the thesis, better cooperation between law enforcement and Internet Service Providers will help in tracking down where users are located in a cyberpayment scheme. ISPs will also assist with perhaps other transaction data that could link more than one party together who is involved in a particular cyberpayment scheme. Future development of IP traceback methods will help to uncover where cyberlaundering activity is happening. Bloom filters could also be used to determine the location of an IP as long as the routers of which the traffic is coming through support it.

6.4.2 Burden of Proof

COMET is a system simply to assist law enforcement in tracking cyberlaundering activity where the return merchandise scheme is performed. The burden of proof for the system relies on law enforcement and not on COMET solely. Though the system is designed to minimize the false positives, there is a percentage of risk associated with any data mining system where the flags could inaccurately locate activity and mark it as suspicious. The law and regulations under COMET should allow for proving a person guilty of cyberlaundering to rest in the hands of law enforcement along with additional evidence surrounding the convicted not obtained by COMET but by other methods.

6.5 Ongoing Investigation

Once COMET alerts authorities of a red flag, criminal persecution should not go underway immediately. In the banking industry, FinCEN recommends that any suspicious activity not be immediately shut down, but rather allowed to continue in an attempt to gather better information and real time activity [39]. COMET should be modeled after this line of thought. Law enforcement, once notified of suspicious activity by COMET, should begin monitoring activity by this user or group of users. This will allow authorities to perhaps witness cyberlaundering taking place assisting in judicial punishment. Furthermore, allowing a laundering group to structure additional electronic money could assist in locating and tracking other people involved in the same illicit activity.

6.6 Merchant Participation

In order for COMET to effectively work, two major stipulations must be met. One, all online merchants who allow purchases of greater than $500 USD must participate. This will allow COMET to effectively locate laundering activity that might be structured. Furthermore, if a group of merchants do not participate, then COMET will not work as effectively. Information on what systems is not a part of COMET will eventually become public knowledge. This will simply move laundering activity to those merchants who are not participating so the illicit activity will go undiscovered. In order for cyberlaundering to be mitigated properly, COMET must be an internationally run system and therefore every global merchant must participate in the system. Any merchant who unlawfully does not participate

will face monetary penalty. The cyberlaundering law enforcement working group will be responsible for locating and penalizing any merchants who does not participate.

As there is no value added to the merchant to participate, the system should be internationally funded by the overseeing government body. The merchant must configure their system to connect with COMET. There is not much overhead in cost after this is performed. Furthermore, merchants must be audited bi-annually to assure the international working group that they are truly sending all transaction activity. This can be performed by showing the company's account ledgers and matching this to the activity logged in COMET.

6.7 Privacy Issues

COMET is a tool which falls under privacy scrutiny from merchants who are sending all account activity including monetary value and gain to a third party. Furthermore, the public will raise concern for allowing account information and buying trends to be sent to an international database. In order to mitigate these issues of privacy, merchants and customers need to be aware of COMET's security and what information law enforcement is allow to recover and what is not recoverable.

COMET's use is for cyberlaundering only and can only be used to obtain records that have been flagged by COMET as suspicious money laundering activity. Records of activity that are deemed “usual” by COMET cannot be obtained by law enforcement. Those responsible for training COMET's artificial intelligence component cannot take part in any law enforcement activities as this would be a conflict of interest. Law enforcement can use records to help investigate any laundering activity. After any investigation is completed, any

account information used by law enforcement external to COMET must be destroyed. Moreover, law enforcement may not in any fashion have financial interest in online merchants as the group will have confidential access to merchant activity.

CHAPTER 7. CONCLUSION

Money laundering is an illicit activity that has been around since the early 1900's, but is and has been an ongoing issue. Due to the advent of free-trade such as the North American Free Trade Agreement (NAFTA), India and China's boom in commercialization and capitalism, and especially the creation of the World Wide Web in 1990, the world is becoming smaller and money laundering has now become an issue at the international level. Federal agencies estimate that about $300 billion is annually laundered worldwide [37]. Understanding the stages of money laundering along with aspects or banking “zones” help mitigate money laundering. Learning the techniques and tools that launderers use to clean illicit funds through the banking industry along with other methods has allowed law enforcement to mitigate and prevent money laundering. However, money laundering associated with cyberbanking and other electronic currency has not been clearly understood and defined. Current working groups have yet to fully decide how cyberlaundering should be mitigated and enforced.

Many rules and regulations have been created in an attempt to plug holes where laundering at a traditional bank takes place. Historically, money laundering has been a game of cat and mouse enforcement – starting with the Bank Secrecy Act in 1970 that required banks to submit information on deposits greater than $10,000. Launderers would skirt this by structuring deposits into smaller amounts or smuggling in illicit revenue, and as a result, the Money Laundering Control Act of 1986 was formed to prevent these activities from occurring. To further mitigate money laundering, the US Patriot Act of 2001 was created.

This act focused more on preventing terrorist financing, but also put stricter rules on the banks to combat money laundering. Through the tools, forms, and audits, a fairly successful program for preventing money laundering at the brick and mortar banking level was developed. However, new methods of monetary housing, distribution, and storing were and are developing in the cyber realm. These methods have introduced new ways to launder money on an international level, and quicker than ever before.

In order to fully understand the threat, we must know the tool that is creating the threat, and that is cyberbanking and cyberpayment system. Understanding these system models along with the trends and developments in the cyberpayment realm can help to determine mitigation methods of cyberlaundering. The systems are generally either affiliated with the World Wide Web or other electronic non-bank transfer systems and stored value cards. Furthermore, hypothetical cyberlaundering methods were introduced in order to help understand methods that could be used to launder money electronically.

Once a solid understanding of current methods for cyberlaundering were discussed along with other methods of illicit use in an electronic financial system then suggestions, concerns and possible policy was discussed to help mitigate the new methods of laundering money. The cyberlaundering policy discussed in the thesis closely modeled the current anti-money laundering regulations but included additional requirements due to the nature of cyberpayment systems.

Though money laundering has traditionally been alleviated by legislation and compliance, using artificial intelligent systems to detect cyberlaundering can assist in providing additional evidence of illicit activity. Moreover, data mining applications are the

only way to attempt at locating cyberlaundering as quickly as possible in order to mitigate the amount of illicit activity. The creation of an international tracking database system, COMET, that mitigates the ability for launderers to clean currency by buying and selling goods is one step in the future of cyberlaundering mitigation.

Money laundering still is an ongoing issue, and with the invention of an international means of transferring financial currency electronically, new law enforcement from the international level can create policy and guidelines similar or the same as ones suggested in this paper to prevent this crime. By slowing down or even stopping the means of laundering money electronically, many illicit activities could be thwarted and detected more easily making the world that we all live in safer, and more financially sound.

APPENDIX A

The following table lists the advantages and disadvantages to each of the hypothetical cyberlaundering methods outlined in chapter 4. The advantages and disadvantages are from the perspective of the launderer considering utilizing the methods as a route for laundering money electronically.

Methods of Cyberlaundering	Advantages	Disadvantages
Stored Value Payment for Drugs	Anonymous, lightweight cards	Use of a particular card system
Transferring Value Through Cyberpayments	Lightweight, High value, Anonymous	Need to use established smart card system(s)
Transferring Value Through Network Based Systems	Small balances prevents detection	Placement may be more traceable
Payments via the World Wide Web	Structuring and Layering is done very quickly	Discovery of the launderer could be found by the individual who originally set up the paypal account or other virtual wallet system
Blended Phishing	Assistant participation incentive, very good layering	Meticulous upfront work
Botnets	Bots are easy to deploy, no need to involve an assistant, damage is minimal to the assistant	Requires bot-herding and bot installation. Creates a footprint in the assistant's account
Micropayment Smurfing	Small amounts of money moves through the system	Small amounts of money moves through the system
Online Stock Trading	Quick turnover of opening an account, buying, selling, and then closing the account	Necessity to open up a trading account that is more heavily mitigated
Return Merchandise Scheme	Quick method to wash money in an industry that has no requirement to maintain customer information	Monetary instruments are part of the process – they must be shipped and physically returned

BIBLIOGRAPHY

[1] Wikipedia, "Tom Delay," *wikipedia.org*, Jan. 13, 2009. [Online]. Available: http://en.wikipedia.org/wiki/Tom_DeLay [Accessed: Jan. 21, 2009]

[2] Wikipedia, "Benazir Bhutto," *wikipedia.org*, Jan. 16, 2009. [Online]. Available: http://en.wikipedia.org/wiki/Benazir_Bhutto [Accessed: Jan. 22, 2009]

[3] UN General Assembly, "World Drug Problem," *un.org*, June 8, 1998. [Online]. Available: http://www.un.org/ga/20special/featur/launder.htm [Accessed: Jan. 23, 2009]

[4] International Monetary Fund, "Data & Statistics," *imf.org*, January 16, 2009. [Online]. Available: http://www.imf.org/external/data.htm [Accessed: Jan. 23, 2009]

[5] Moneylaundering.com, "AML Basics," *moneylaundering.com*, January 17, 2009. [Online]. Available: http://www.moneylaundering.com/subscribers/amlbasics/mlintro.aspx [Accessed: Jan. 23, 2009]

[6] Congressional Testimony, "Statement by Michael Morehart," *fbi.gov*, May 18, 2006. [Online]. Available: http://www.fbi.gov/congress/congress06/morehart051806.htm [Accessed: Jan. 23, 2009]

[7] "The Wolfsberg Trade Finance Principles" May 2002. [Online]. Available: http://www.wolfsberg-principles.com/pdf/WG_Trade_Finance_Principles_Final_(Jan_09).pdf. [Accessed: Jan 23, 2009].

[8] "Minority Staff Report for Permanent Subcommittee on Investigations Hearing on Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities"

November 9, 1999. [Online]. Available: http://muneeb.org/lumsblog/files/MINORITY_REPORT.pdf. [Accessed: Jan 25, 2009].

[9] “Money Laundering: a banker’s guide to avoiding problems” December 2002. [Online]. Available: http://www.occ.treas.gov/moneylaundering2002.pdf. [Accessed: Jan 25, 2009].

[10] “FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual” June 23, 2005. [Online]. Available: http://www.occ.treas.gov/handbook/bsa-amlintro-overview.pdf. [Accessed: Jan 25, 2009].

[11] "Operation Wire Cutter" Dismantles Network of Major Colombian Money Launderers,” Department of Homeland Security, January 16, 2002. [Online]. Available: http://cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/12002/01162002_3.xml. [Accessed: Jan 25, 2009].

[12] Wikipedia, “Electronic Money,” *wikipedia.org*, Jan. 13, 2009. [Online]. Available: http://en.wikipedia.org/wiki/Electronic_money [Accessed: Jan. 27, 2009]

[13] J. R. Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering*. CRC Press LLC, 1999.

[14] “Global Organized Crime,”*american.edu*, [Online]. Available: http://www.american.edu/ted/hpages/crime/Russian.htm [Accessed: Feb. 06, 2009]

[15] “Yakuza stalk Japanese markets as organized crime opens new front,” *business.timesonline.co.uk*, Aug. 28, 2008. [Online]. Available: http://business.timesonline.co.uk/tol/business/industry_sectors/banking_and_finance/article4621950.ece [Accessed: Feb. 06, 2009]

[16] Wikipedia, “Triad,” *wikipedia.org*, Feb. 4, 2009. [Online]. Available: http://en.wikipedia.org/wiki/Triad_society [Accessed: Feb 5, 2009]

[17] “The IMF and the Fight against Money Laundering and the Financing of Terrorism,” *www.imf.org*, [Online]. Available: http://www.imf.org/external/np/exr/facts/aml.htm [Accessed: Feb. 06, 2009]

[18] “World Internet Users and Population Stats,” *www.internetworldstats.com*, [Online]. Available: http://www.internetworldstats.com/stats.htm [Accessed: Feb. 06, 2009]

[19] “Electronic Benefit Transfer,” *wikipedia.org*, [Online]. Available: http://en.wikipedia.org/wiki/Electronic_Benefit_Transfer [Accessed: Feb. 09, 2009]

[20] “Chinese Professor Cracks Fifth Data Security Algorithm,” *epochtimes.com*, Jan. 11, 2007. [Online]. Available: http://en.epochtimes.com/news/7-1-11/50336.html [Accessed: Feb. 09, 2009]

[21] “2007 Internet Crime Report,” *ic3.gov*, 2007. [Online]. Available: http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf [Accessed: Feb. 09, 2009]

[22] “Mondex,” *wikipedia.org*, 2008. [Online]. Available: http://en.wikipedia.org/wiki/Mondex [Accessed: Feb. 14, 2009]

[23] Roger C. Molander, B. David Mussington, Peter A. Wilson, *Cyberpayments and Money Laundering: Problems and Promise*. RAND reports, 1998.

[24] “DigiCash,” *wikipedia.org*, 2008. [Online]. Available: http://en.wikipedia.org/wiki/Digicash [Accessed: Feb. 14, 2009]

[25] N. Behling, *Cyberpayments - Credit Cards Are Here to Stay*. [Online]. Available: http://www.jurpc.de/aufsatz/20010016.htm [Accessed: Feb. 09, 2009]

[26] “Digital gold currency,” *wikipedia.org*, 2008. [Online]. Available: http://en.wikipedia.org/wiki/Digital_gold_currency [Accessed: Feb. 14, 2009]

[27] “ISO 4217 currency names and code elements,” *iso.org*, 2009. [Online]. Available: http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/currency_codes/currency_codes_list-1.htm [Accessed: Feb. 14, 2009]

[28] “About the FATF” *fatf-gafi.org*, 2009. [Online]. Available: http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html [Accessed: Feb. 20, 2009]

[29] “Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance)” *eur-lex.europa.eu*, 2007. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML [Accessed: Feb. 21, 2009]

[30] “bot net [sic] with key logger” *sans.org*, 2009. [Online]. Available: http://lists.sans.org/pipermail/unisog/2004-April/023018.html [Accessed: Mar. 11, 2009]

[31] “ANI Spoofing” *asteriskvoipnews.com*, 2009. [Online]. Available: http://www.asteriskvoipnews.com/asterisk_news/cidani_spoofing_on_voip_using_asterisk.html [Accessed: Mar. 11, 2009]

[32] “The Future of Online Gambling” *ecommercetimes.com*, 2003. [Online]. Available: http://www.ecommercetimes.com/story/31962.html?wlc=1236920468 [Accessed: Mar. 11, 2009]

[33] C. Schmidt, R. Muller, “A Framework for Micropayment Evaluation,” Netnomics, Springer, vol. 1(2), pages 187-200, October.

[34] “Of pineapples, barbecues, and the Amazon honor system.” Computer Shopper., June 2001, Pg 24.

[35] “World statistics on the number of internet [sic] shoppers” *www.multilingual-search.com*, 2008. [Online]. Available: http://www.multilingual-search.com/world-statistics-on-the-number-of-internet-shoppers/28/01/2008 [Accessed: Mar. 17, 2009]

[36] U.S. Department of Justice – National Drug Intelligence Center, “Money Laundering in Digital Currencies,” Product No. 2008-R0709-003, June 2008.

[37] Information Technologies for Control of Money Laundering, “Electronic Money Laundering,” [Online]. Available: http://www.princeton.edu/~ota/disk1/1995/9529/952903.PDF [Accessed: Mar. 26, 2009]

[38] DTREG, “Introduction to Support Vector Machine (SVM) Models,” [Online]. Available: http://www.dtreg.com/svm.htm [Accessed: Mar. 27, 2009]

[39] United States General Accounting Office, “Money Laundering - FinCEN’s Law Enforcement Support Role Is Evolving,” GGD-98-117, June 1998.

[40] Billy’s Money Laundering Information Website, “Money Laundering - Stages of the Process,” *laundryman.u-net.com*, 2006. [Online]. Available: http://www.laundryman.u-net.com/page5_mlstgs.html [Accessed: Apr. 5, 2009]

[41] “Cali Cartel,” *wikipedia.org*, 2008. [Online]. Available: http://en.wikipedia.org/wiki/Cali_Cartel [Accessed: Apr. 5, 2009]

[42] R. Grosse, *Drugs and money: laundering Latin America's cocaine dollars*. Greenwood Publishing Group, 2001, p. 214.

[43] R. Bortner, “Cyberlaundering: Anonymous Digital Cash and Money Laundering,” *osaka.law.miami.edu*, 1996. [Online]. Available: http://osaka.law.miami.edu/~froomkin/seminar/papers/bortner.htm [Accessed: Apr. 5, 2009]

[44] “Know your customer,” *wikipedia.org*, 2009. [Online]. Available: http://en.wikipedia.org/wiki/Know_your_customer [Accessed: Apr. 5, 2009]

[45] The World Bank Financial Sector Working Paper, “Money Laundering in Cyberspace,” *cybrinth.com*, 2004. [Online]. Available: http://cybrinth.com/uploads/Money%20Laundering%20in%20Cyberspace.pdf [Accessed: Apr. 5, 2009]

[46] “Bank Secrecy Act,” *wikipedia.org*, 2009. [Online]. Available: http://en.wikipedia.org/wiki/Bank_Secrecy_Act [Accessed: Apr. 5, 2009]

[47] “US Code,” *gpoaccess.gov*, 2009. [Online]. Available: http://bit.ly/bsa_5311 [Accessed: Apr. 5, 2009]

[48] “FAQs Regarding Report of Foreign Bank and Financial Accounts (FBAR),” *irs.gov*, 2009. [Online]. Available: http://www.irs.gov/businesses/small/article/0,,id=148845,00.html [Accessed: Apr. 5, 2009]

[49] “Smurf (crime),” *economicexpert.com*, 2009. [Online]. Available: http://www.economicexpert.com/a/Smurf:crime.htm [Accessed: Apr. 5, 2009]

[50] "EU satisfied with money laundering prevention activities," *wordpress.com*, 2008. [Online]. Available: http://brilliantfixer.wordpress.com/2008/12/24/eu-satisfied-with-money-laundering-prevention-activities/ [Accessed: Apr. 5, 2009]

[51] "United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances," *un.org*, 1988. [Online]. Available: http://untreaty.un.org/English/TreatyEvent2003/Texts/treaty7E.pdf [Accessed: Apr. 5, 2009]

[52] "United Nations Convention against Transnational Organized Crime," *uncjin.org*, 2000. [Online]. Available: http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf [Accessed: Apr. 5, 2009]

[53] Bank for International Settlements, "Financial Stability Forum establishes working groups," *bis.org*, 1999. [Online]. Available: http://www.bis.org/press/p991119.htm [Accessed: Apr. 5, 2009]

[54] International Monetary Fund and World Bank, "Proposals To Assess A Global Standard And To Prepare ROSCs," July 2002. [Online]. http://www.docstoc.com/docs/4370602/INTERNATIONAL-MONETARY-FUND-AND-WORLD-BANK-ANTI-MONEY-LAUNDERING [Accessed: Apr. 5, 2009]

[55] International Monetary Fund, "Financial Intelligence Units: An Overview," *imf.org*, 2004. [Online]. Available: http://www.imf.org/external/pubs/ft/FIU/fiu.pdf [Accessed: Apr. 5, 2009]

[56] "Form 8300," *irs.gov*, March 2008. [Online]. Available: http://www.irs.gov/pub/irs-pdf/f8300.pdf [Accessed: Apr. 5, 2009]

[57] G. Cook “Bank Secrecy Act (BSA) Regulations - Money Laundering Schemes,” *cookco.us*, 2008. [Online]. Available: http://www.cookco.us/financial/money_laundering.htm [Accessed: Apr. 5, 2009]

[58] Office of National Drug Control Policy, “The High-Intensity Drug Trafficking Area Program: An Overview,” *whitehousedrugpolicy.gov*, 2008. [Online]. Available: http://www.whitehousedrugpolicy.gov/HIDTA/overview.html [Accessed: Apr. 5, 2009]

[59] K. Rijock, “From a Different Angle,” *world-check.com*, January 2007. [Online]. Available: http://www.world-check.com/articles/2007/01/11/will-5-new-unregulated-virtual-banks-become-money-/ [Accessed: Apr. 5, 2009]

[60] Electronic Privacy Information Center, “The Clipper Chip,” *epic.org*, 2009. [Online]. Available: http://epic.org/crypto/clipper/ [Accessed: Apr. 5, 2009]

[61] “Gold certificate,” *en.wikipedia.org*, 2009. [Online]. Available: http://en.wikipedia.org/wiki/Gold_certificate [Accessed: Apr. 5, 2009]

[62] “Phishing,” *en.wikipedia.org*, 2009. [Online]. Available: http://en.wikipedia.org/wiki/Phishing [Accessed: Apr. 5, 2009]

[63] “Slammer worm slows; no new reports of problems,” *computerworld.com*, January 2003. [Online]. Available: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=77918 [Accessed: Apr. 5, 2009]

ACKNOWLEDGEMENTS

I would like to take this opportunity to thank those who assisted me through this thesis and my graduate career. First, Dr. Sree Nilakanta for his guidance, advice, and support for not only this thesis, but also for the questions, concerns, and help on my graduate journey. Second, I would like to thank Dr. Doug Jacobson who chose me to be the recipient of the National Science Foundation Cyber Corps Scholarship thereby funding my education, taught many of my core classes, and mentored me through various other career development concerns. He too assisted me in the formulation of this thesis. Third, Dr. Carter for his support and appearance on my committee. Fourth, my father who valued education enough to get me where I am today. Fifth, my mother for always questioning my position on my thesis. Sixth, my dog Sandy, who has taught me that the present is the most important time in one's life. Lastly, my beautiful fiancé Inna, who is the half to my whole and supported me through the nights of research and typing.