BVG Trust

J. Sci. Trans. Environ. Technov. 2016, 9(3) : 131-138

Scientific Transactions in Environment and Technovation

Money Laundering and its impact in banking industry

*S. Kannan[1] and K. Somasundaram[2]

[1]Department of Computer Science and Engineering, Karpagam University, Coimbatore, Tamilnadu 641021, India.
[2]Department of CSE, Vel Tech High Tech Dr RR and Dr SR Engineering College, Avadi, Chennai-60062, India.

Abstract

Money Laundering (ML) is a global phenomenon with political, economic and social consequences, which impact on the ability of business and societies harmfully. The existence of illegal flows creates economic distortions such as weakening the banking industry, disinvestment of licit economy, loss of attractiveness for Foreign Direct Investment (FDI), erratic use of the resources or promotion of illegal activities. In private domain, there are numerous cases of business seriously vulnerable by ML operations. This paper presents the four stages of money laundering zones such as correspondent banking, private banking, black market peso exchange and cyber laundering which are connected with the ML activities. Then, different money laundering tools and techniques are outlined. This paper explains how the ML activities occur in banking and non-banking industry. Also, some of the recent trends used in name screening and sanction screening for financial institutions are also discussed.

Keywords-Anti Money Laundering (AML), Black Market Peso Exchange, Correspondent Banking, Cyber Laundering, Private Banking, Name Screening and Sanction Screening.

INTRODUCTION

Money laundering (ML) is defined as the process of hiding the illegal source, existence, or application of income derived from criminal actions, and the subsequent hiding of the source of that income to create it appear legitimate[1, 2]. The main task is cheating when observing the heart of ML, cheating the authorities by creating assets look as if they have been acquired through legal means, with legally-earned income, or to be possessed by other parties who have no relationship to the real owner. The rules of each country which have forbidden the MLoutline the activity a bit differently. It is one of the ways money laundering works – by taking benefit of the varying rules per country[3].

ML is critical to recognize how laundering happens. Generally, money is laundered over a series of transactions and it usually includes three steps[4, 5]. Some of the more vagueprocedures are done with the help of cyber-hacking. Fig.1 shows the three stages of money laundering.

Placement – In this stage, the money launderer will place his/her illegal properties into the financial system. It is regularly done by retaining funds into circulation with the help of casinos, financial institutions, currency exchange shops, and other businesses, it can be both domestic and international.

Some examples of this stage are:

→ Breaking up huge amounts of cash into smaller sums of cash and then placing those directly into a bank account.

→ Transport cash across borders for credit in foreign financial institutions, or it can be used to buy high-value properties, such as precious metals and stones, and artwork which can then be resold for payment by bank transfer or check.

Layering–This stage involves taking the proceeds and evolving complex layers of financial transactions to mask the ownership, audit trail, and source of funds. This stage can include transactions such as:

⇒ Financing in real estate and legitimate businesses, etc.

⇒ Moving the deposited cash from one account to another

⇒Reselling high-value goods and monetary instruments

⇒Converting deposited cash into monetary instruments (example, e-gold on the Internet)

⇒ Utilizing shell banks that are generally registered in offshore areas, and wire transfers

Integration - This stage in the money laundering process contains placing the laundered incomes back into the economy to generate the perception of legitimacy. It has become very hard to differentiate legal and illegal wealth. The launderer might select to capitalize the funds in luxury assets, business ventures, real estate, or other means.

*Corresponding Author :
email: *kannan.sathasivam@citi.com*

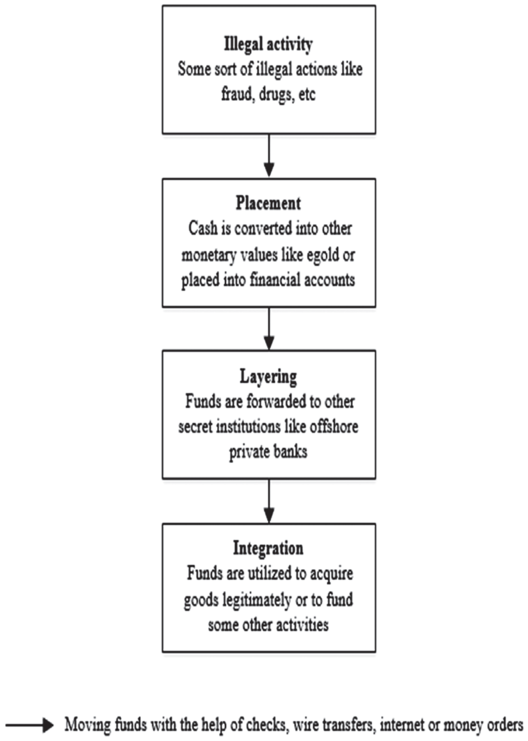
Illegal activity
Some sort of illegal actions like fraud, drugs, etc
Placement
Cash is converted into other monetary values like egold or placed into financial accounts
Layering
Funds are forwarded to other secret institutions like offshore private banks
Integration
Funds are utilized to acquire goods legitimately or to fund some other activities
Moving funds with the help of checks, wire transfers, internet or money orders

Fig.1. Stages of Money Laundering

I. CURRENT MONEY LAUNDERING ZONES

There are four large money laundering zones connected with money laundering[6]. They are detailed as follows:

A) Correspondent banking

Correspondent banking is the service by which one bank offers services to other bank to transfer funds, which interchange currencies or carry out a multiplicity of other transactions[6]. In some correspondent associations, the foreign bank's local clients are allowed to conduct their own transactions, such as wired transfers, with the help of foreign bank's correspondent account. Those type of accounts are called as payable-through accounts. In other circumstances, a foreign bank's correspondent account is used by another foreign bank to perform its own transactions. This practice is named as nesting.

With such direct access to foreign financial system, once the funds are received in the same correspondent account, the foreign bank's customers or other foreign banks can move the money in or out of the correspondent account location with the correspondent account serving as hiding place. This money laundering gateway is called as correspondent banking. This susceptibility required the Wolfsberg Group, which issue guidelines for private banking, to distribute principles on correspondent banking in November 2002[7]. These endorsements include:

→ Client data require to be analyze and update regularly

→ Institutions should not provide services or products to shell banks

→ Due diligence on risk-based accounts

→ An international registry of financial institutions must be generated to help aid in tracking down money laundering.

B) Private banking

Nowadays, private banking has been seen as one of the most exposed areas of financial activity in the money laundering domain. It facilitates financial flexibility to people of high net worth which move billions of dollars global, often secretively, and with moderately little control.

A report released on 1999 by the Permanent Subcommittee on Investigations renowned these explanations as to why private banking is vulnerable to money laundering [8]:

→ There is usually a closer relationship between the banker and the client

→ Private banking customers may have economic or political ties

→ Private banking is referenced as "secret" socially

→ There is a better margin of profit in private banking

→ Money laundering controls incline to not be imposed to as great of an extent as public banks.

One regarding factor that federal regulators take the way private bankers effort. Many of them work in large banks and they offer salary bonuses for new clients whom they attract to the bank.

The Office of the Comptroller of Currency (OCC) endorses that banks estimate private banking accounts depends on "risk-grade basis," estimating the level of risk by geographical location, type of business, and service extended or bank product[9]. It states that well-rounded stages to open an account are central risk controls for private banking associations. These measures, which bank management should follow, should include account owners identification, identification of normal and expected transactions and source of wealth.

Anti-Money Laundering (AML) and Bank Secrecy Act Examination Manual, released jointly in 2005 by the federal banking regulators to evaluate these risks. It states that the following features must be considered[10]:

→ Nature of the customer

→ Relationship between the bank and the client

→ Activity and purposed of the account, service or product

→ Public information about the customer which is practically available to the bank

→ Location and authority of the client's business or home

C) Black market peso exchange

The Black Market Peso Exchange method is defined as the process by which money in the U.S. derived from aprohibited activity is purchased by Colombian "peso brokers" from prisoners in other countries and regularly dropped in U.S. bank accounts that the brokers have recognized. They trade wire transfers and checks drawn on those financial records to legitimate businesses. They use them to purchase properties and services in the U.S.

On behalf of financial institutions to prevent and detect laundering by peso brokers, they should be aware with the shared laundering methods used by the brokers. The most standard scheme includes multiple checking accounts released at U.S. banks through foreign nationals[11]. Banks also should be alert of the growths in the movement of dollars in the consistent accounts of foreign banks.

D) Cyber laundering

Initially, money laundering is done electronically with the help of wire transfers. Transferring money through a wire transfer presently offers a limited amount of information about the parties involved. It is becoming less corporate and more details about a wire transfer are to be documented. As the privacy of wire transfers is reducing and the record protection regulations are growing, money launderers want to expand their methods. This method occurs through the world of cyberspace.

As consumerism rises in the cyber world, so does the need for an efficient and effective means of financial transactions. As a result, electronic cash was generated as a replacement for cash. Electronic or digital cash refers to scrip or money exchanged only by electronic means[11]. Though a great deal of electronic cash is noticeable, still a few institutions offer a means of online and offline unidentified digital cash. This kind of secrecy is of a particular interest to money launders.

The problems arises in cyber laundering is the lack of the regulations precise to the electronic money laundering. Most of the digital banks do not fall under a particular regulatory statute, and so would not have to follow to certain rules. Moreover, there is a great deal of argument in regards to the privacy rights that whether all the electronic transactions should be observed simply because a minor percentage might be illegal.

II.MONEY LAUNDERING TOOLS AND TECHNIQUES

This section presents the more common techniques used by money launderers to wash dirty money with the help of banking industry. Knowing these techniques can better prevent from ML and understand how ML can happen in the cyber world.

A) Smuggling

The structuring method of ML became anillegal offense since 1986. As a consequence, smuggling has been the most widespread method for establishing the ML process. Smugglers are trying to get the cash away from the strict country and into a less supervised country. An easy way to wash cash through smuggling is when the money moves over the margin, such as from the United States to Mexico, the money is not acknowledged on a CMIR report.

Smuggling cash is prepared by three diverse methods:

1. Cash is transported in bulk through the same channels which is used to carry in the narcotics.

2. Hand carrying the cash.

3. Cash can be transformed into a monetary instrument such as a traveler's check or a money order and then emailing these to foreign banks.

B) Structuring

Structuring is defined as the act of separating large sums into smaller sums less than $10,000 in order to avoid the Bank Secrecy Act Reporting condition. In 1986, this technique has been registered as a crime through the banking industry. It is extensively used in the cyber laundering realm as the rule only relates to financial institutions. Most of the money launderers are structuring in an approach known as "smurfing" where each deposit is not complete by the same individual but somewhat this individual is hiring others to credit the money in accounts in an effort to remain unidentified. Example, one offline case of this was the Grandma Mafia Incident where a 60 year old grandmasteered a group of women indepositing $25 million in numerous bank accounts in California.

C) Mirror image trading

The mirror image trading system works in where a money launderer buys agreements for one account but selling the same amount from some other account. Since both accounts are measured by the same person, there is neither profit nor loss – it just fresh money.

D) Shell corporations

Shell companies are according to the trusts, institutions, foundations, corporations, etc. They do not conduct any manufacturing or commercial business or any other form of commercial process in the country where their registered office is situated[12]. These companies support with the layering stage of ML and they are not complex to format. Any lawyer will list a business for a name and him or herself the chairman/chairwoman. The corporate bank accounts are created at severalisland or offshore banks. The organizations are utilized when clients requisite to launder money and remain unidentified.

E) Front companies

Front Companies are a place in which the money launderers can place and layer profits that are illegal. They do not require to fulfill with any financial institution to activate. They are also problematic to detect if there is genuine business being conducted and if the organization is not necessary to fill out CTRs.

F) Inflated prices

Inflated prices works where false invoices are generated for imported good which were never bought or purchased at high inflated prices.

G) Dollar discounting

Dollar discounting is where a drug dealer will sale his drug proceeds to a broker at a reduction price. Then, the broker takes the responsibility for laundering the money. Then the money can be easily given to the drug dealer in order to better prevent himself from being exposed by law enforcement.

III. MONEY LAUNDERING IN BANKING INDUSTRY

Near 30 years ago, it was very simple and easy for a criminal or a drug dealer to deposit huge amounts of money. Through the fierceness of Bank Secrecy Act (BSA) principles and the Patriot act, the banks are not as robust for ML field. It has become very problematic for ML to occur within the realms of banks. This section presents a quick outline of the banking industry along with the usual money laundering techniques. This section will aid with understanding the banking statues and laws so that preemptive cyber laundering actions can be measured.

A) The banking industry

The banking industry is complex, comprising of financial industries at the state, federal, and local level.These are controlled by state and federal agencies that at times control the same things. The chief banking system is the Federal Reserve that was run by a board of seven governors selected by the president for 14 years. The Federal Reserve consists of 12 central banks, a Federal Advisory Council, and member banks. Every banks of national position are members of the Federal Reserve Banking System. They are administered by the Office of the Comptroller of Currency and should include the word “National” in their name. If they attain these qualifications, then they can become a member of the system.

B) Offshore banks

An offshore bank is a bank situated outside the country where the investor of financial currency resides. Generally, these are in a low tax authority and facilitates legal and financial gains. Besides the benefit of greater privacy that an offshore bank offers, there are many other causes why a money launderer would look to an offshore bank. Some of these comprises as follows:

→ The government in where the offshore bank is situated is corrupt

→ No mandatory reporting of malicious activity

→ Bank regulatory systems in many of the offshore banks do not perform well

→ American dollars can be possibly used in an offshore bank

→ No active monitoring of currency movements

→ Capability to use nominee, anonymous, or numbered accounts

→ Access to free-trade zones

→ The word offshore originates from the banking industry in the United Kingdom where the word offshore was where banks in the Channel Islands. They are commonly used to denote many of the banks on minor islands and even many of the steady, private banking done in Switzerland.

C) Common money laundering in banks

This section outline some of the common money laundering methods that have been used in the banking industry.

1) Wire transfers

Wire transfers are just moving money from one bank or institution to another one. Wire transfers will be imperative for the banking industry. This way of layering illegal funds is the most usual tool in the banking industry for transferring large amounts of investment. There are three central transfer systems used for wire transfers in the world.

1. The Clearing House Interbank Payment System (CHIPS),

2. Fedwire, and

3. International wire system is called as Society for Worldwide Interbank Financial Telecommunication (SWIFT). There are around 700,000 wire transfers daily transferring over $2 Trillion U.S. dollars[13].

A wire transfer works done in the following manner:

A bank directs a message to a transfer system's main computer, which representing the initiating bank, the receiving bank, the amount, and the particular person who is to collect the payment. The system regulates the balances, and yields an electronic debit voucher at the original bank along with a credit voucher at the receiving bank. Once the bank accepts a credit voucher, it rents the originating bank know to withdrawal the money. If two banks are measure of the same wire transfer system, they are the only two banks in the series. If they are not, it is such as in an international transfer, then transfers have to be completed with the help of correspondent account. However, 80% of the transactions are not done this way[14].

2) Money laundering prevention

Banks applies a very strong approach to prevent the money laundering and mitigate the risk from occurring in their institution. Hence, BSA is introduced in 1970 in order to cover any holes which came about from the growing technology and change in the banking system. As a result of September 11th Attacks, the Patriot Act closed down on terrorist financing by spreading the rules already in place [15, 16].

All banks are compulsorily have a BSA compliance program. It should set out a system of internal controls, elect a BSA security officer, train bank personnel and undergo auditing. Moreover, banks should institute a "Know Your Customer" policy in order to prove that the customer is not on any list of known money launders, fraudsters, or terrorists. Other than this, the policy observes transactions of a customer over their banking history and banking of their peers.

D) Money laundering in non-bank financial institutions

The BSA formerly applied only to 20 financial institutions, and it was late extended to relate to all national banks[17]. Among five of them are banks, where the other 15 are known as non-bank financial institutions and they are given as follows:

→ SEC registered and other securities or brokers/dealers

→ investment banks

→ redeemers

→ pawn brokers

→ precious metal dealers

→ real estate brokers

→ the postal service

→ currency exchanges

→ credit card systems

→ insurance companies

→ casinos

→ financers

→ traveler's check and money order issuers

→ travel agencies

→ finance companies

IV. RECENT TRENDS IN SCREENING

Nowadays, it is a real challenge to block and identify the malicious transactions while processing huge volumes of legitimate transactions with better accuracy. Generally, financial institutions spend more money, time, and resources for examining the false positives, as money transfer activity and transaction volume increases. This can be reduced with the help of name screening and session screening methods.

A) Name Screening

In 90s, electronic name screening was introduced to block the transactions for drug traffickers. The sanction list hardly consists of hundreds of names. In the 21st century, sanction programs are enhanced to identify the money laundering and terror funding. Names are recognized as not just any string of text, it has a typology and structure which are influenced by many regional and cultural factors. Humans can easily recognize English, Arabic, Chinese or French names. But teaching this cultural variation to the machine is very difficult. *Simple algorithms* are introduced to manage name matching on statistics to estimate linear and similarities thresholds to trigger alerts or not. These approaches are sometimes fails to provide accurate results and may result many false positives. More sophisticated approaches utilize algorithms based on machine learning and linguistic techniques to confirm that no relevant hits are missed. Algorithms based on linguistic comprises of transliteration and translation. Transliteration is the capability to compare name of different alphabets. Translation is used to store dissimilarities which mean the same thing in different languages like "John", "Juan" and "Jean" or

"Allemagne", "Deutchland" and "Germany". The screening hubs should be capable of providing a reliable result and processing checks in milliseconds. The solutions are designed at the heart of the financial organizations. Some of the technologies used for name screening are described as follows:

1) Watch List Filtering

Watch-list filtering solutions aid financial organizations keep ahead of supervisory changes and they eliminate the risk of fines and reputational disclosure. They filter the transactions and customers against sanctions. It was designed to identify the matches over each part of the name. The screening criteria is used by banks to recognize name variations and misspellings and it should be based on the level of OFAC risk related with the particular product or type of transaction.

2) SDN List

SDN incorporates a list of individuals, entities subject and groups to economic sanctions by the Office of Foreign Assets Control (OFAC) and the U.S. Treasury. The SDN list is regularly updated and covers:

→ Foreign terrorist administrations.

→ Companies, banks, vessels and individuals at first glance, may not appear to be related to the sanction targets they represent.

→ Individuals and entities situated anywhere in the world that they are controlled or owned by, or acting with respect to the government of a sanctioned country.

→ Individuals identified as involved in the proliferation of weapons of mass destruction.

→ Specially-designated global terrorists/narcotics traffickers.

3) Name matching Technology

The efficiency of matching technology is defined by how powerful the algorithms are working. Useful algorithms have commanding routines which are particularly considered to compare names, strings and partial strings, business names, spelling errors, addresses, tax ID numbers, postal codes, data that sounds analogous (such as "John" and "Jon") etc. The filtering abilities range from simple name checking algorithms to complex algorithms which can search and format/unformat data from multiple expense and messaging systems with a high degree of accuracy.

4) Rules-Based Matching Technology

Rule-based matching technology uses an integration of algorithms and business rules to estimate when two or more records match through unique iden-tifiers like passport/SSN/TIN numbers. It accurately matches on definite common fields; it creates links based on number of individual identifiers which match among the available datasets. This is the quickest and easiest linking strategy. Still, deterministic matching systems have a comparatively lower degree of accuracy when compared with probabilistic matching. It suits applica-tions where the number of records is comparatively small (less than two million).

5) Probabilistic Matching Technology

It refers to comparing different field values among two records, and allocating each field with a weight that specifies how closely the two field values can match. The sum of the individual fields' weights specifies the likelihood of a match among two records. This technology makes statistical analysis on the data and estimates the frequency of items. Then, it applies the analysis to weight the match, which is similar to the way that the user can weight the significance of each row.

6) Fuzzy Matching

Fuzzy matching technology is the execution of algo-rithmic processes (fuzzy logic) to calculate the similarity between elements of data such as personal name, business name, or address information. The fuzzy logic feature permits the algorithm to notice and calculate near matches rather than necessitate exact matching. Based on the algorithm, it may use alternate nicknames, such as Mickey" or "Mike". Names would be simple to match if they were consistent; however, money launderers use various techniques to bypass filter detection.

7) Phonetic Matching

It is the process of matching data using functions/algorithms which have been produced and focus on how a word is pronounced rather than how it is spelled. This algorithm matches two dissimilar words with same pronun-ciation to the same code that allows phonetic similarity-based word set indexing and comparison. There are words which have diverse spellings but similar pronunciation and must be matched, such as Reynold and Renauld / Sofia and Sophia etc. Therefore, a matching engine is compulsory to construct connections based on diverse phonetic transformationrules. Soundex, metaphone and double metaphone are the generally used techniques while executing phonetic-based matching.

B) Sanction Screening

Most of the financial institutions depends on the third party screening systems to perform sanctions screening. The problem for financial institutions is to identify the right balance between being capable to identify the

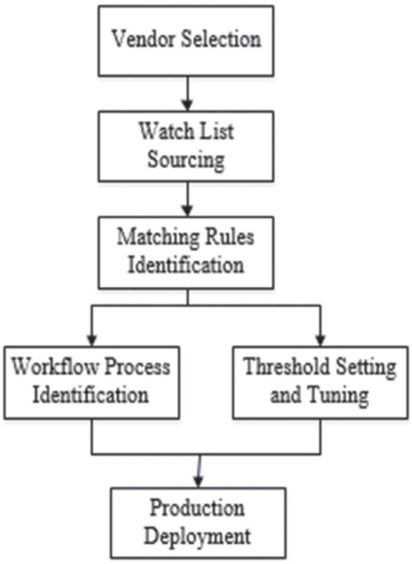
Vendor Selection
Watch List Sourcing
Matching Rules Identification
Workflow Process Identification
Threshold Setting and Tuning
Production Deployment

Fig.2 Lifecycle of sanction screening

transaction violations and processing payments for their clients without unnecessary delay. To overcome this problem, the financial institutions understand their screening environments. The lifecycle of sanction screening is shown in fig.1. It includes the following stages: Vendor selection, Watch list sourcing, Matching rules identification, Workflow process identification, Threshold setting and tuning, and Production deployment.

1) Vendor selection

Selecting a knowledge *vendor* is possibly one of the most important tasks. It considers the following factors: technology infrastructure, data volume and matching algorithm library.

2) Watch List Sourcing

This stage addresses the watch list selection of both public and internal to the institution. It estimates the processes to enhance the watch list and they are updated accurately, timely and completely.

3) Matching Rules Identification

Organizing a sanction screening included understanding whether the institutions various processes can support or facilitate more refined matching rules. Generally, institutions use the name matching rules in the screening system. There are additional features are available in the customer data. Some of the features include address, date of birth, identification numbers etc.

4) Workflow Process Identification

The hits occurred by the sanction screening systems which are need to be examined and the system should contains an investigation flow. The flow must be recognized and implemented such that the hits are examined based on the business flows of the institution.

5) Threshold Setting and Tuning

In this phase, an advanced statistical analysis are used to estimate the effective threshold values to be utilized for each of the matching rules for successful estimation. A successful examination of the matches can offer insight into the quality which can be expected in the production side. This phase is important to perform threshold tuning before placing the selected thresholds for production.

CONCLUSION

This paper presents an introduction about the money laundering process and its activities. The three stages of money laundering activities such as placement, layering and integration are explained. Money laundering zones and their categories are presented to understand how the money laundering occurs in financial institutions. The tools and techniques applied to launder the money is also discussed which helps to prevent the banking sector from the future illegal transactions. It is recommended that the financial systems should apply the AML solutions to combat with the ML issues in today's environment. Finally, the paper presents the recent trends of screening applied in financial institutions.

REFERENCES

Aiolfi,G., and Bauer, H. P. 2012. *Collective Action: Innovative Strategies to Prevent Corruption,The Wolfsberg Group, Zürich: Dike,* 97-112.

Bortner, R. M. 1996. Cyberlaundering: Anonymous digital cash and money laundering, *final paper, University of Miami School of Law.*

Buchanan, B. 2004.Money laundering—a global obstacle, *Research in International Business and Finance,* 18: 115-127.

Choo, K.-K. R. 2014. Designated non-financial businesses and professionals: A review and analysis of recent financial action task force on money laundering mutual evaluation reports, *Security Journal,* 27:1-26.

Council, F. F. I. E. *2005.* Bank Secrecy Act Anti-Money Laundering Examination Manual: *Federal Financial Institutions Examination Council.*

Gilmore,W.C. and de l'Europe, C. ,1999. Dirty money: The evolution of money laundering counter-measures ,*Council of Europe Strasbourg,* 609.

Grosse, R. E. 2001. Drugs and money: laundering Latin America's cocaine dollars: *Greenwood Publishing Group.*

Ferrall, B. R. 2000. Transnational Criminal Organizations, Cybercrime and Money Laundering: A Handbook for Enforcement Officers, Auditors and Financial Investigations, *Journal of Criminal Law and Criminology,* 91: 308-308.

Lilley, P. 2003. *Dirty dealing: The untold truth about global money laundering,* international crime and terrorism: Kogan Page Publishers.

Minority Staff Report for Permanent Subcommittee on Investigations Hearing on Private Banking and Money Laundering,1999. A Case Study of Opportunities and Vulnerabilities.

Moneylaundering.com. 2009. *AML Basics*. Available: http://www.moneylaundering.com/subscribers/amlbasics/mlintro.aspx

Nikander, P. 2000. Method and system for performing electronic money transactions, *ed: Google Patents,*

Quirk, P. J. 1997. Macroeconomic implications of money laundering Trends in Organized Crime, 2: 10-14.

Reuter, P. 2004. *Chasing dirty money: The fight against money laundering*: Peterson Institute,

Schneider,F., and Windischbauer, U. 2008. Money laundering: some facts," *European Journal of Law and Economics,* vol. 26, 387-404.

Sullivan, K. 2015. What Is Money Laundering?," in Anti–Money Laundering in a Nutshell, ed: *Springer*, 1-13.

Turner, J. E. 2011. Money laundering prevention: Deterring, detecting, and resolving financial fraud: *John Wiley & Sons.*