Chapter 2
The Changing Typologies and Emerging Trends of Money Laundering Practices

2.1. Introduction

This chapter presents a comprehensive descriptive analysis of issues related to the changing typologies and emerging trends of money laundering activities. It is apparent that money laundering is evolving where it takes place. At first, money laundering was committed through financial institutions. Over time, it has also been accomplished through non-financial institutions and professional agencies. In financial institutions, money-laundering trends have become more complicated and sophisticated from traditional laundering methods. Whereas in non-financial institutions, money laundering vulnerability affects, among others, insurance companies, security sectors, travel agencies, real estate industries, casinos, underground bank systems, and international trade transactions. Professionals such as accountants, lawyers, notaries, and other independent legal professions are also susceptible to money laundering. These developments prove a significant shift in laundering activities from financial institutions to non-financial institutions and then move to professional launderers. All of these methods can also be done through electronic money and the internet, otherwise called cyber-laundering. This chapter analyzes the changing typologies and emerging trends of money laundering activities by giving detailed hypothetical cases in order to create a better understanding of these trends. Understanding the precise nature of these challenges and assessing the extent to which anti-money laundering policy has enabled to control the vulnerability of money laundering are also discussed in this chapter.

2.2. Money Laundering through Financial Institutions

Criminals carry out conventional laundering methods by depositing illegal cash into financial institutions and then, if necessary, transfer the cash to overseas by wire. The ability to launder the proceeds of crime through the banking system is vital to the success of criminal operation. The increased integration of the world's financial system and the removal barriers to the free movement of capital are two causes why money laundering through the banking system are increased significantly.[1]

---

[1] Ira Sohn, "Money Laundering: The Dark Side of Capital Account Liberalization", Montclair State University, p.4-5.

Another method in conducting money laundering is converted the illegal cash into cheques, money orders, traveler's cheques, or other monetary instruments and then, send abroad by mail or courier.[2] Through these methods, criminals use the financial system to place and move illicit funds in giving them the appearance of legitimacy. However, this laundering method results in a problem for criminals because the application of customer due process and the reporting requirements. Cash paid in bulk deposited in banking institutions will attract the attention of bank employees and it might be reported to the competent authorities as a suspicious transaction. To avoid this challenge, criminals try other laundering techniques by means of the following: 'smurfing' or structuring, placing illicit funds into offshore banks, and currency smuggling.

'Smurfing' or 'structuring' has to do with breaking large sums of illicit money into smaller sums and then depositing it into bank accounts in order to avoid the limited reporting requirement of $10,000.[3] By using this method, the illegal cash is converted into an amount which is less than the threshold of reporting requirement. In order to disguise the beneficial owner of the account and the true nature of the funds, the bank accounts are opened in the name of a business or other legal entities. Thus, through this method, a large amount of money, which is derived from illegal activities, evades from the reporting requirement. In this case, the illicit funds are available for moving without attracting attention from bank employees as well as law enforcement authorities.

Laundering method can also be done through offshore banking or offshore financial centers.[4] Offshore banking in this context refers to countries that follow a strict bank secrecy law, have minimal regulations, and have to do

---

[2]Bonnie Buchanan, "Money Laundering - Global Obstacle", Research in International Business and Finance", Vol.18, 2004, p.117.

[3]Kirk W. Munroe, "Surviving the Solution: The Extraterritorial Reach of the United States", Dickinson Journal of International Law, Vol.14, 1995-6, p.506. *See* also Sarah N. Willing, "Smurfs, Money Laundering, and the Federal Criminal Law: The Crime of Structuring Transactions, `U. Fla. L. Rev., Vol.41, 1989, p.289.

[4]'The meaning of 'offshore financial center' (OFC) varies with the context, but recent International Monetary Fund (IMF) definition points to centers where most business transactions involve non-resident and some or all of the following services: bank secrecy and anonymity; moderate or light financial regulation; and low or zero taxation. Many of the OFC jurisdictions appearing in recent IMF background paper are Caribbean Island Nations; nevertheless Europe and Asia appear as hosts to dozens OFCs each. A sampling of listed OFCs include Andorra, Bahamas, Cyprus, Dublin, Guam, Israel, Lebanon, Liberia, Nauru, Netherlands, Panama, Puerto Rico, Singapore, Switzerland, Tangier, Thailand, and the United States'. Cited in Jesse S. Morgan, "Dirty Names, Dangerous Money: Alleged Unilateralism in U.S. Policy on Money Laundering", Berkeley Journal of International law, Volume 21, 2003, p.778. *See* also Kirk W. Munroe (1995-6), *Supra* note 3, p.507. *See* also International Monetary Fund, *Offshore Finance Centers*, IMF Background Paper, June 23, 2000.

with non-residents for the financial transactions.[5] Through this method, countries try to design its policy to attract businesses and achieve self-enrichment in ways that are detrimental to global welfare and the rule of law.[6] Besides, in the offshore financial center, there are no taxes and less cooperation with tax authorities of the country where the depositor originates from.[7] Under these circumstances, there is no need to declare the transactions to the domestic fiscal authorities because offshore banks usually do not strictly implement currency transaction reports. This condition allows criminals to launder vast amounts of wealth for the purpose of avoiding income, gift, and inheritance taxes.[8] As a consequence, home countries lose enormous amounts of money in tax revenue.[9]

Currency smuggling is another technique in concealing and placing illicit funds. It refers to the physical movement of cash from one location to another to disguise its source and ownership.[10] Three ways in carrying out this method involve by shipping the cash, by a courier to hand-carry the cash, or by changing the cash into negotiable instruments such as money orders or traveler's cheques, and then, mailing these to foreign banks or other foreign destinations.[11] The FATF reported that cash smuggling is one of the three major categories of money laundering besides trade-based money laundering and finance-related money laundering.[12] In reducing the currency smuggling, the only law enforcement weapon that currently available is a requirement that shipments of more than $10,000 in cash should be accompanied by a report to the authorities. According to this rule, failure to file such a report is the confiscation of bulk cash when it discovered.

Money laundering through banking institutions is a method that has been used for a long time. Criminals use these institutions to conceal illicit

[5]James R. Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook to Law Enforcement Officers, Auditors, and Financial Investigations*, (Washington DC: CRC Press, 1999), p.51. *See* also Colin Powel, "The Regulation of Offshore Financial Centres", 31 Commonwealth Law Bulletin, 2005, p.72.

[6]Bent Sofus Tranoy, "Offshore Finance and Money Laundering: The Politics of Combating Parasitic Strategies", Institute for Research in Economic and Business Administration, Bergen, April 2002, p.5.

[7]Jeffrey I. Horowitz, "Piercing Offshore Bank Secrecy Laws Used to Launder Illegal Narcotics Profits: The Cayman Islands Example", Texas International Law Journal, Vol.20, 1985, p.134.

[8]*Ibid.*

[9]*Ibid.*

[10]Financial Action Task Force, Report on Money Laundering Typologies 2002-2003, p.4.

[11]James R. Richards (1999), *Supra* note 5, p.51. *See* also Jeffrey I. Horowitz, (1985), *Supra* note 7, p.139.

[12]Increasingly more attention is being given to trade-based money laundering by the FATF through 2006 typology, a 2008 best practice report, and most recentlty a report on Free Trade Zone (FTZ). *See* Jasper Liao and Arabinda Acharya, "Transhipment and trade-based money laundering", Journal of Money laundering Control, Vol.14, No.1, 2011, p.81.

proceeds. Through the banking system, criminals can invest and manage their money in different ways, including deposits, transfers, exchanges, and the delivery of funds to accounts under different names and countries. This would then allow the criminal to cover up, hide, conceal, or disguise the nature or the source of the illegally obtained money. As a response, the FATF provided several recommendations to prevent the use of financial institutions for money laundering purposes. The FATF also put banking institutions as the groundwork in preventing money laundering practices. Here in this context, the FATF introduced principles to prevent money laundering from occurring in the financial institutions. These include customer identification, record keeping, and the reporting of suspicious transactions.

In Indonesia, the principle of 'know your customer', or KYC, was implemented through regulations of Bank Indonesia No.3/10/PBI/2001 and No.3/23/PBI/2001. According to these regulations, KYC is used as a principle for knowing the identities of customers, monitoring financial transactions of customers, and reporting suspicious transactions. The regulations in this context impose an obligation for the banking institutions to set up and arrange a policy for accepting customers, a procedure for obtaining customer identification, a procedure for monitoring customer accounts, a procedure for risk management, and a procedure for reporting suspicious transactions. However, these policies are hard to implement consistently due to several obstacles. Firstly, from the view point of the banking institutions, banks face difficulties in implementing the KYC principles because there are a vast number of banks, each of which having their own branches and employees. As a consequence, they have to incur significant costs for identifying customers, reporting and maintaining documentations, training official employees, and so on. In addition, banks are also afraid of customers moving their accounts to other banks that follow a less regulative system. Some banks are even reluctant to implement these principles consistently. Secondly, from the view point of the customer, some are reluctant to give information regarding the purpose and business relation with banks. Others are reluctant to report large transactions that uncover the nature and source of the funds. In addition, some customers feel that the fulfillment of identification is excessive and creates difficulties, or that there is no benefit in providing detailed identification and related matters. The reluctance of customers to comply with the obligation is due to these new requirements that did not exist in Indonesia prior to the year 2000. At that time, there was no obligation for banks to ask the nature and source of the money invested or transferred by customers into the banking system.

2.3. Money Laundering through Non-Financial Institutions

Over time, anti-money laundering and law-enforcement efforts in many countries have become increasingly advanced and sophisticated in the field of financial institutions. This condition urges criminals to move their attention towards intermediaries other than financial institutions to launder their proceeds of crime. Non-financial institutions such as insurance sectors, security sectors, travel agencies, real estate industries, casinos, and gambling are used as vehicles for laundering the proceeds of crime. Each of these distinct laundering techniques is addressed in turn.

The first method is through insurance companies. Money laundering in this sector is aimed at breaking the connection between the illicit money and the predicate offence that generates the funds. There are several reasons why criminals tend to use the insurance sector as a vehicle for laundering their illicit funds. These include the size of the industry, the diversity in its products, and ease of availability.[13] Other reasons utilizing the insurance companies for money laundering are the difficulty in detecting illicit funds from large investments due to high transaction levels and due to the good return on investment.[14]

Money laundering through the insurance sector can be done through various techniques and tools. Principally, there are two kinds of techniques in this context. The first is by investing illicit funds into a joint venture with an insurance company.[15] In this case, the launderers transfer illegal funds into a large investment without drawing attention because it is not unusual for an insurance company to do that. The second one is by means of insuring themselves through life insurance, non-life insurance, reinsurance, return pension, or fraudulent claims.[16] Other methods include the payment of premiums with illicit money, borrowing against policies purchased with illegal money, one-off payments for policies that are subsequently terminated within the contract cancellation period, and fraudulent loss claims involving high value goods purchased with illegal funds.[17] The following is an example of laundering method through the insurance sector.

> "A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows: he contacted an insurance broker and delivered a total amount of USD 250,000 in three cash installments. The insurance broker did not report the delivery of that amount and deposited the three

---

[13] Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2003/2004, p.15.

[14] George Farrugia, "Money Laundering and Insurance Business", Paper, p.1.

[15] Arthur Pittman, "Money Laundering: A Challenge for Canadian Law Enforcement", Criminal Law Quarterly, Vol.41, 1998-1999, p.p.243-244.

[16] *Ibid.*

[17] Financial Action Task Force on Money Laundering, Money Laundering and Terrorist Financing Typologies, June 2005.

installments in the bank. These actions raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totaling USD 250,000, thus avoiding the raise suspicions with the insurance company."[18]

Until recently, it is believed that the insurance sector is still vulnerable to money laundering. However, money laundering activities detected in the insurance sector is relatively small when comparing it with the size of the industry. The FATF identified at least two dominant factors why money laundering is difficult to detect within the insurance sectors. These factors are the inadequacy of compliance with anti-money laundering regulations and the lack of commitment throughout the entire industry.[19]

The second method is through security sectors, which refer to the trading of securities. This is a place where buyers and sellers come together to trade. This sector is vulnerable to money laundering particularly at the layering stage. Several methods in the security sectors, which may pose a substantial threat to anti-money laundering, involve the misuse of trading operations, the establishment of legal entities, or the exploitation of various market mechanisms.[20] The techniques used by criminals in the security sectors are though purchasing publicly traded securities by using illicit funds and then converting them into stocks and bonds.[21] Through this method, the identity of the launderer may be concealed by using another name, through a third party like an investment advisor, or through a shell corporation located in a tax-haven jurisdiction.[22] The FATF experts pointed out that illegal fund laundered through the security sectors can be carried out from outside and within the sectors.[23] If it is carried out from outside the sector, the source of the funds is concealed through securities transactions or the creation of legal entities. If it is done within the sector, securities transactions or manipulations that generate illegal funds need to be laundered. The following two cases represent examples of fraud money invested in the securities market and laundering methods through the sector respectively.

"A brokerage firm opened several accounts for a group of twelve linked individuals, including a non-resident account that was used to record very large movements and

[18]Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2002/2003, Case number 3.

[19]*Ibid*.

[20]Arthur Pittman (1998-1999), *Supra* note 15, p.243.

[21]*Ibid*.

[22]*Ibid*.

[23]Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2002/2003, paragraph 31.

apparently to centralize most of the suspected flows, which totaled more than USD 18 million. The launderers used the following two mechanisms:

First, the accounts of some of the parties involved were credited with large sums received from the countries in question, which were invested in the stocks of listed companies in country W; and second, the accounts of the individuals concerned were credited with sums from regions in question, which were transferred to the non-resident account (the first accounts were used as screens). This securities buy/sell mechanism was used to filter the flows through the broker and subsequently the clearer and custodian. Once filtered, the funds were sent to locations in regions and offshore financial centers. This information showed that the co-opted broker had been used to launder the proceeds from various forms of frauds. The manager of the brokerage firm served as a relay for the criminal organizations involved."[24]

The third method is through travel agencies. Travel agencies function as a broker which brings the buyer and seller together. They play this role in providing information and access to visitors. Travel agencies are exposed to several money laundering methods. This includes the purchase of expensive airline tickets for another person who then requests a full cash refund. Another method is to structure outgoing wire transfers in small amounts to avoid reporting requirements.[25] Through the travel agencies, criminals transfer large amounts of money without attracting attention because travel agencies do this as part of their regular course of business. The following case is an example of laundering methods through travel agencies.

"An IRS investigation in Virginia was initiated on the owner of a travel agency for currency structuring charges after analysis of SAR and CTR filings. The suspect operated, in addition to the travel agency, a money transmittal business that was wiring funds to his business interests in Lima, Peru, and Bogota, Colombia. An analysis of subsequent SARs and CTRs, coupled with various investigative techniques, including execution of several search warrants, led to the suspect entering a plea to one count of money laundering. The defendant admitted structuring transactions to avoid a CTR filing. The defendant structured deposits totaling between USD 2.5 to 5 million and used six business accounts at five financial institutions to facilitate his activities. The defendant consented to the administrative forfeiture of monies seized from his business accounts."[26]

The fourth method is through a real estate industry. In an international market, it is a reality that the real estate industry attracts large amounts of money which might be both legitimate and illegitimate.[27] In the Netherlands,

---

[24]*Ibid*, paragraph 36.

[25]Carl A. Fornaris, "USA PATRIOT Act - Treasury Department Solicits Comment on Proposed Regulations That Could Affect Travel Agencies and Businesses Engaged in Vehicle Sales", at http://www2.gtlaw.com/pub/alerts/2003/fornarisc_03b.asp

[26]Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2002/2003.

[27]Hans Nelen, (2008), *Ibid*, p.755.

the vast majority of money laundering activities takes place in the real estate industry.[28] Criminals entrusted the proceeds of crime through purchasing real estate in order to launder and conceal their illegal funds.[29] In this context, real estate agents become attractive for criminals because it is nontransparent market that the values of the object difficult to estimate and can increase easily. As a means for carrying out money laundering in the real estate industry, cash can be used for purchasing a property. Through this method, criminals create the appearance of a legitimate source when they sell the property.[30] It also can be carried out by buying, reselling, exchanging, swapping, or bartering the property.[31] These methods make it more difficult to trace the origin of the funds. Furthermore, the criminals can sell properties, meaning that the money re-enters the economy as a legitimate payment.[32] In addition, through the real estate industry, criminals can earn money from the increasing value of the property.[33] It is also worth noting that in conducting money laundering easily, the real estate industry can be combined with other sectors, such as lawyers, notaries, accountants, or insurance companies. The following case is an example of them.

> "A local property deals occurs where they will purchase a piece of property, paying less than the real market value on paper. The rest of the purchase is paid in cash under the counter. The property is then resold for the full market value and the money recouped with the illegal component now appearing to be capital gains. Another option is for the criminal to use international real estate flips. Here they arrange to sell a piece of property to a foreign investor who is, in reality, himself working through one or several offshore companies. The sale price is suitably inflated above acquisition cost, and the money is repatriated in the form of a capital gain on a real estate 'deal'.
>
> Suspicious flows of more than USD 2 million were identified being sent in small amounts by different individuals who ordered wire transfers and bank drafts on behalf of a drug trafficking syndicate who were importing 24 kg of heroin concealed in cargo into country Z. Bank drafts purchased from different financial institutions in country Y (the drugs' source country) were then used to purchase real estate in country Z. An accountant was used by the syndicate to open bank accounts and register companies. The accountant also offered investment advice to the principals. A firm of solicitors was also used by the syndicate to purchase the property using the bank drafts that had been purchased

---

[28]Brigitte Unger and Greg Rawlings, et al, "The Amounts and Effects of Money Laundering", Report for the Ministry of Finance, Den Haag, 2006. Cited in Hans Nelen, "Real estate and serious forms of crime", International Journal of Social Economics, Vol.35, No.10, 2008, p.755.

[29]Hans Nelen (2008), *Ibid*, p.757.

[30]*Ibid.*

[31]*Ibid.*

[32]Ibid, p.69.

[33]*Ibid*, p.119.

overseas after they had first been processed through the solicitor's trust account. Family trusts and companies were also set up by the solicitors." [34]

The FATF identified some indicators that can be used as instruments for detecting money laundering within the real estate sector. These include 'the client wishes buying with a substantial amount in cash; the client buys real estate without having seen the property; the client buys real estate in the name of a third party without establishing an apparent link to the client; the client uses different names for the sale agreement and the payment; the client wishes to pay cash in advance amounting to more than 10% of the sales price of the real estate; and the client wishes to pay upfront in cash amounting to more than 15,000 EUR'.[35]

The fifth method is through casinos. A casino is a cash intensive business where the majority of transactions are in cash. Like other financial transactions, casino operations are also vulnerable to association with suspected money laundering activities. In this case, criminals attempt to infiltrate or influence casinos to facilitate money laundering. This can be done by means of casino chips, casino cheques, casino accounts and facilities, structuring through the casino, currency exchange, etc.[36] Value instruments of casinos are used in the placement and layering phases of money laundering activities. In this case, illicit funds are placed when they are used to purchase casino chips. After minimal play, it will be layered by redeeming the casino chips for a casino cheque. Casino vulnerability was recognized in the revision of the FATF recommendations, with the obligation to report transactions.[37] The following highlights the techniques observed by FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) in 2008-2009 the use of casino value instruments for money laundering activity:

- Customers made casino chip purchases, using illicit cash (in some instances small denomination bank notes) or a bank draft, purchased with illicit funds and made payable to the casino-the customers engaged in minimal or no game play and then redeemed the chips for a casino cheque;
- The amount and/or frequency of casino chip purchases made by a customer did not correspond with the stated income/occupation of the customer (or the income/ occupation details provided by the customer were vague and/or insufficient) - for example, a customer claimed full time employment, but was observed attending the casino on a daily basis, during working hours;

---

[34] Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2002/2003.

[35] Belgian Financial Intelligence Processing Unit, *Op.Cit*, p.6.

[36] Brigitte Unger and Greg Rawlings, et al (2006), *Supra* note 28, p.69.

[37] The Forty Recommendation of the FATF (2003), Recommendation 12.

- Customers made casino chip purchases, engaged in minimal or no gaming, and left the casino in possession of chips-casino chips may be used as an alternate currency in illegal transactions such as drug sales.[38]

Based on the above elaborations, non-financial institutions are also vulnerable to money laundering. The vulnerability of non-financial institutions is seemingly more serious than in the financial institutions. This is due to the following reasons. Firstly, transactions in the field of non-financial institution are predominately done in cash. This condition makes it easier for criminals to use illicit funds, for example, in buying real estate or conducting joint ventures with an insurance company without attracting any attention from law enforcement authorities. This is due to fact that non-financial institutions use or transfer of large amounts of money, thus minimizing suspicion. Secondly, there are various ways to launder illicit funds in the field of non-financial institutions. Under the surface of legitimate economic activities, tracing the origin of money laundering funds in this field is becoming increasingly difficult. This is one of the reasons why criminals feel safe in conducting money laundering within this field. Thirdly, not all kinds of non-financial institutions are included under the anti-money laundering regime in many countries. Despite its coverage by the anti-money laundering regime of a country, there are still some obstacles in implementing the regulations. Lastly, non-financial institutions have a lack of authority in conducting investigation.

To solve these problems, the FATF has expanded the scope of preventing money laundering in the field of non-financial institutions. The FATF focuses on detailed aspects of activities in this field that is vulnerable to money laundering. Through recommendation 12, the FATF expanded on the various methods used in laundering illicit funds to designated non-financial businesses and professions. The FATF also encourages countries to improve their anti-money laundering regime and implement customer due diligence. This includes the identification and verification of their customers to non-financial institutions in the same way that has been implemented by financial institutions. Within this context, recommendation 8 encourages non-financial institutions to follow and adapt to new or developing technologies in order to minimize the risk of new money laundering exploits.

2.4. Money Laundering through Underground Banking System

The ‘underground banking system’, also refers to an ‘alternative remittance system’[39], ‘informal value transfer system’[40], ‘informal funds transfer

[38]Financial Transactions and Reports Analysis Centre of Canada, November 2009. Available at http:// www.fintrac.gc.ca/publications/typologies/2009-11-01-eng.asp#f11

system',[41] or 'parallel banking system', is an informal method of moving money around the world without using formal financial institutions. The term 'alternative remittance system' stands for informal banking arrangements that run independently from any formal banking system.[42] Here in this context, an alternative remittance system allows for the payment of a corresponding amount of cash or other form of value to a beneficiary in another location. This would be achieved through a means of communication, message, transfer, or through a clearing network where the money or value transfer service belongs. In this method, the value is moved from one location to another without the physical movement of currencies. The method has developed in many parts of the world such as in South Asia and Middle East.

Hawala and Hundi are the most commonly examples of alternative remittance systems.[43] In term of its origin, hawala refers to the transfer of money or information through a third person.[44] In this case, the transfer of money is not used of a formal financial institution such as banks; otherwise called as informal business transaction. Hawala also refers to a transaction that is based on trust without any paper trial. Through this system, hawala includes two main aspects, the sending and receiving of money and the settlement process.[45] The former concerns the relationship between a hawaladar and his or

---

[39]Financial Action Task Force on Money Laundering (FATF) 1999. 1998–1999 Report on Money Laundering Typologies.

[40]FATF defines a money or value transfer system as 'a financial service that accept cash, cheques, other monetary instruments or other stores of value in one location and pays corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer, or through a clearing network to which the money/value transfer system belong". See Interpretative Note to FATF Special Recommendation VI: Alternative Remittance, Issued on February 2003, p.5.

[41]World Bank & IMF 2003. Informal funds transfer systems: an analysis of the informal hawala system. Washington DC: World Bank.

[42]Rob McCusker, "Underground Banking: Legitimate Remittance Network or Money Laundering System", Trends and Issues in Crime and Criminal Justice, No.300, 2005

[43]The literal meaning of 'hawala' in Arabic is 'transfer'. In Hindi, it is translated as 'reference'. In the historical perspective, hundi is the oldest term of used for credit or bill of exchange. Even though the traditional meaning and purpose of hundi was different from the contemporary use of hawala, the two terms have come to be used as synonymous to each other. It could be said that hawala is a variation of the centuries-old hundi-system. In term of its origin, hawala is stands for the transfer of money or information through a third person. *See* Divya Sharma, "Historical Traces of Hundi, Socio-cultural Understanding, and Criminal Abuses of Hawala", International Criminal Justice Review, 2006, p.p.99, 103, 105. *See* also Shahid Nawas, Roddy McKinnon, and Robert Webb, "Informal and Formal Money Transfer Networks: Financial Service or Financial Crime?", Journal of Money Laundering Control, 2002, p.333.

[44]Shahid Nawas, Roddy McKinnon, and Robert Webb, (2002), *Ibid*.

[45]Lisa C. Caroll, "Alternative Remittence System Distinguishing Sub-system and Its Role in Money Laundering in Interpol Member Countries on the Asian Continent"; available at http://www. interpol. Int/Public/FinancialCrime/MoneyLaundering/EthnicMoney/default.asp.

her client, while the latter refers to a relationship between intermediaries. The third party, broker or hawalander, which might be a private person, has a corresponding business with their counterparts in another country. The work of the system can be illustrated in the example below.

> 'A customer – usually a migrant worker- approaches a Hawala broker and gives him a sum of money to be transferred to a beneficiary – usually a relative - in another city or country. The Hawala broker often runs a legitimate business in addition to the financial services he offers and has a business contact, a friend or a relative in this city/country. The Hawala operator contacts their Hawala partner – usually a contact from their personal or business network - in the recipient city/country by phone, fax or e-mail. The operator instructs the partner to deliver the funds to the beneficiary, providing amount, name, address and telephone number of the recipient and promises to settle the debt at a later stage. The customer does not necessarily receive a receipt but is given an identification code for the transaction. The Hawala broker in the recipient city/country contacts the beneficiary and delivers the funds. The recipient can receive the funds without producing identity documents other than the previously agreed code. There is no recorded agreement or written contract for the transaction. The deal is secured by the trust between the parties with no legal means of reclamation'.[46]

Historically, in the past time, a hawala system was used to transfer legal money from immigrant workers to their family. However, over the years, besides transferring legal money from migrant workers, this system became attractive for those who want to conceal illicit funds. Someone can misuse hawala system to avoid tax and currency regulations. Terrorist groups, for example, need this system to conceal the proceeds obtained from criminal activities. Also, corrupt officials need it to launder the proceeds of corruption. Other varieties of criminal proceeds laundered through hawala system include profits from drug trafficking, arm trafficking, people and women trafficking, gold smuggling, and extortion.

There are many reasons why people wish to transfer funds outside the formal banking system. It is because such a system provides fast, safe, and cost-effective way to transfer funds domestically as well as internationally.[47] Other reasons for using this method are due to distrust of banks, religious

---

[46]Marie Cheney, Hawala Remittance System and Money Laundering". Article, Anti Corruption Resource Center, 28 May 2008, p.2.

[47]The Commonwealth Secretariat in its report on parallel economies and money laundering noted at least four reasons: 'firstly, in certain countries, local banks often do not have overseas remittance arrangements, or where they do exist, the operation can be cumbersome and time-consuming; secondly, the alternative system can be cheaper than official channels; thirdly, this method protects assets from theft or seizure by government, e.g. nationalization; and lastly, it permits evasion of stringent import/export duties, evasion of exchange control regulations, and facilitates evasion of tax'. *See* Commonwealth Secretariat, 'Money Laundering: Special Problems of Parallel Economies', Paper prepared for the Joint Meeting of Commonwealth Finance and Law Officials on Money Laundering, London, 1-2 June 1998 (May 1998), p.10-11.

grounds, tax evasion, and avoiding currency regulations.[48] Several characteristics of alternative remittance systems that differ from the conventional banking systems are anonymity, require minimal documentation, and follow a less regulative system.[49] This is to say that the system does not maintain an audit trail that functions to follow the money. The system also does not maintain customer identification, record keeping, and suspicious transaction reports which are obliged to the formal banking systems.

Due to the crucial problem of alternative remittance systems for illegal purposes such as money laundering and terrorist financing, the FATF released eight Special Recommendations on terrorist financing after the September 11, 2001 attacks. In Special Recommendation VI, which addresses alternative remittances, the FATF requires the licensing or registration of all formal and informal money or value transfer services. The FATF also requires that they be subject to the FATF forty- recommendations. However, in practice it is difficult to implement due to the informal nature of the business. Alternative remittances are used through 'sandy word' or 'an identification code' within the community. In addition, alternative remittances can disguise itself under the cover of as a legitimate business. One solution for this is through encouraging governments to identify alternative remittances in their jurisdictions and then implement due process for the clients who want to send money.

2.5. Money Laundering through International Trade Transaction

The international trade transaction is a system run by cross-border commercial entities for the buying and selling of commodities.[50] However, the system is vulnerable to abuse by criminals to launder illicit funds, which are commonly referred to 'trade-based money laundering'. The term 'trade-based money laundering' concerns the process of disguising illicit funds, obtained from trade transaction, as having a legitimate origin.[51] The U.S. Customs officials refer to this as an act of converting illicit money into a less suspicious form.[52] There are various methods in which illicit funds may be laundered through trade-based activities, such as the Black Market Peso Exchange and manipulating trade documents. Through these methods, the importers and exporters enable to

---

[48] Alan Lambert, 'Underground Banking and Financing of Terrorism', Fla. J. Int'l L., Vol.15, 2002, p.12. *See* also Lan Cao, "The Transnational and Sub-National in Global Crimes", Berkeley Journal of International Law, Vol.22, 2004, p.72.

[49] Marie Cheney (2008), *Supra* note 46, p.1.

[50] *See* http://www.teachmefinance.com/Financial_Terms/international_trade.html

[51] Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies, 2005-2006, p.3.

[52] Narcotic Report 2003, p.21.

move large amount of money without transaction records. The following provides a brief review on how these laundering methods operate.

'Black Market peso Exchange' is the most common method of trade-based money laundering. This method functions as an alternative remittance system used to transfer monies or values without physically moving them. This method was initially used by Colombian immigrant workers to send monies back to their home countries. It was also used by Colombian importers to exchange pesos into dollars for buying U.S. properties without paying taxes and duties. Through this method, drug-traffickers launder and convert their illicit proceeds from U.S. dollars to Colombian pesos. The *U.S. versus Jose E. Stroh* is a case of Black Market Peso Exchange. The position of the case can be read in the following.

> "The indictment charges that Stroh was involved in an extremely large-scale international money laundering conspiracy involving the proceeds generated from the sale of cocaine in the United States. His alleged co-conspirators are Szion Abenhaim, David Vanounon, Adi Tal and Raymond Chochaia. According to the indictment, Stroh, in partnership with Abenhaim, was a currency broker from May, 1986 to April, 1990. As such he arranged for the exchange of U.S. currency generated from the sale of cocaine in the U.S., for Colombian pesos. He received a commission on each currency transaction. As a broker, he negotiated the terms for the currency exchange with numerous intermediaries representing various factions of the Cali cartel who had control over the cash generated from drug trafficking in the U.S. To effectuate the currency exchanges, Stroh would provide the intermediaries with beeper numbers and code names of individuals in the U.S. to contact for pick up of the U.S. currency that had been received from the sale of cocaine. Stroh's conspirators would then convert the cash to checks, money orders and wire transfers that could be transferred within and outside the U.S. The transactions were structured in a way that would avoid the U.S. Treasury's currency reporting requirements for transactions exceeding $10,000".[53]

By way of illustration, the following figure describes a simple scheme of the Black Market Peso Exchange that is used to facilitate money laundering.

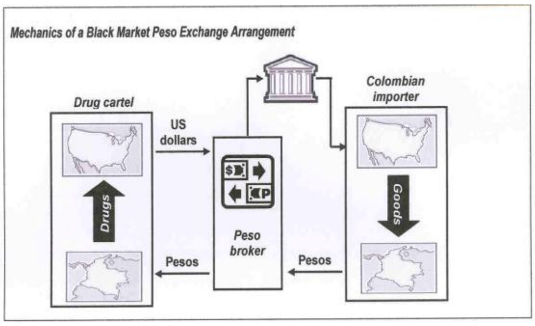

Figure 2: Mechanics of the Colombian Black Market Peso Exchange
Source: FATF Report on Money Laundering Typologies 2005-2006

[53]United States District Court, District of Connecticut, The *U.S. versus Jose E. Stroh*. See http:// www.ctd.uscourts.gov/Opinions/110300.AHN.Stroh.pdf, p.2.

Based on the figure above, the mechanics of black market peso exchange can be explained in the following steps.

- First, the Colombian drug cartel smuggles illegal drugs into the United States and sell them for cash;
- Second, the drug cartel arranges to sell the US dollars at a discount to a peso broker for Colombian pesos;
- Third, the peso broker pays the drug cartel with pesos from his bank account in Colombia (which eliminates the drug cartel from any further involvement in the arrangement);
- Fourth, the peso broker structures or smurfs the US currency into the US banking system to avoid reporting requirements and consolidates this money in his US bank account
- Fifth, the peso broker identifies a Colombian importer that needs US dollars to purchase goods from US exporter;
- Sixth, the peso broker arranges to pay the US exporter (on behalf of the Colombian importer) from his US bank account.
- Seventh, the US exporter ships the goods to Colombia; and
- Finally, the Colombian importer sells the goods (often high-value items such as personal computer, consumer electronics and the household appliances) for pesos and repays the peso broker. This replenishes the peso brokers's supply of pesos.[54]

Another method is manipulating trade documents. It is inevitable that the international trade system can also be exploited by criminals to launder their criminal proceeds through manipulating trade documents. Through this method, the criminals can move large amount of money without transaction record (undetected). The FATF published a special report on trade-based money laundering on June 2006.[55] The report focuses on vulnerabilities in the import and export activities of international commerce that may be exploited for the transfer of illicit funds. In this report, the FATF identified the basic techniques of trade-based money laundering, including over and under-invoicing of goods and services, multiple invoicing of goods and services, over and under-shipments of goods and services, and falsely described goods and services.

The first technique is over and under-invoicing of goods and services. This method is carried out by increasing or decreasing the price of exports or imports. A difference in cost between the collusion price and the actual price will be disbursed with private instruction where to deposit it. The second technique concerns multiple invoicing of goods and services. This may be done by issuing more than one invoice for the same international trade transactions. By invoicing the same traded goods or services more than one, the launderers are able to justify multiple payments for the same shipments of goods or

[54]*Ibid.*

[55]Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies, 2005-2006.

services. The third technique is over and under-shipments of goods and services. Through this technique, the launderer overstates or understates the quantity of goods being shipped or services being provided. By colluding with the importer, the exporter under-ship goods or does not ship them at all. Finally, the fourth technique is misrepresentation goods and services. Through this method, the importer or exporter gives a fraudulent explanation regarding the quantity or types of goods or services that will be shipped.

It is recognized that trade-based money laundering is the most difficult form to detect due to the complexity of transactions and the large number of individuals involved in it. The scheme of trade-based money laundering, which often allows criminals to distance themselves from the money laundering process, is another reason for making it difficult to investigate. In addition, money laundering through international trade transactions is difficult to detect as the concealment of illicit funds is carried out under the cover of legitimate activities, namely, international trade transactions.

2.6. Money laundering through Professionals

Professionals – such as lawyers, accountants, notaries, and other legal professionals - perform a number of important functions in helping their clients organize and manage their financial affairs. However, these professionals can also abuse their legal standards by providing money-laundering services to individuals and organized criminal groups who want to conceal their illicit proceeds. In recent years there have been a significant number of cases involving professionals in carrying out money laundering. Laundering methods in this context have indeed moved from being conventional towards professionalism.

There are various methods and functions that can be used to launder criminal proceeds through professionals. These functions include financial transactions such as cash deposits and withdrawals, foreign exchange operations, issuing and cashing cheques; financial and tax advisory; gaining introductions to financial institutions; and complex legal arrangements such as trusts.[56] Two potential benefits of the launderers in carrying out their activities with professionals are the expertise of legal knowledge and the privilege of non-disclosure. The following provides a brief review on how these laundering methods operate.

The first method is money laundering carried out by lawyers. Lawyers may also be used as a vehicle to help criminals to launder their illicit funds. The 2001 FATF typologies identified the following money-laundering

[56] Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2000/2001, paragraph 33. *See* also Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2003/2004, paragraph 86-87.

vulnerabilities: 'the creation of corporate vehicles or other legal arrangements; buying and selling of real estate property; performing financial transactions; financial and tax advice; and gaining introductions to financial institutions'.[57] Lawyers can also involved in money laundering by giving advice on beneficial ways to transfer money, stored large sums of money on behalf of their clients, and passing illicit money through their accounts.[58] The following example illustrates how a lawyer may be involved in money laundering activities.

> "In the case in one country, a prominent attorney performed services for a whole clientele of launderers. A client with USD 80 million – worth of proceeds from an insurance fraud, used the lawyer to transfer this money to financial institutions in countries where there were few or no anti-laundering regulations. The attorney opened accounts in various banks under false names of individuals or corporations. The illegal funds were placed in the form of cash or cheques in banks, then wired to the different accounts controlled by the attorney. Because of his professional reputation, the domestic banks never considered it necessary to look more closely at the nature of the transaction in question".[59]

The second method is money laundering done by notaries. Notaries are largely concerned with the verification of documents and information that will be used around the globe for clients who have a business or property overseas, or who are involved in litigation in foreign courts. Nelen and Lankhorst noted that the cases of the notaries are related to either transactions on the property market or the creation of corporate vehicles and other complex legal arrangements.[60] Notaries also function to provide advice and fiscal information regarding various types of companies that may be established. However, by their expertise, notaries abuse their status and function to help criminals in conducting money laundering. A notary's laundering methods can be seen in the following example.

> "A real estate agent in a tax haven jurisdiction opened an account at a bank in a European country. The account was used to cash in a cheque drawn signed by a foreign notary. Once the cheque had been cleared, part of the funds were withdrawn as cash, parts were transferred back to the original jurisdiction, and the balance was credited to the account of a notary in that country and used to purchase real property there. The account opened at the bank was only used as a temporary transfer account for the laundering of the proceeds of financial crime".[61]

[57]Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2000/2001, paragraph 35.

[58]Hans Nelen and Francien Lankhorst, "Facilitating Organized Crime: The Role of Lawyers and Notaries", in D. Siegel and H. Nelen (eds.), Organized Crime: Culture, Markets and Policies, Springer, 2008, p.135.

[59]Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 1997/1998, Case number 4.

[60]Hans Nelen and Francien Lankhorst (2008), *Supra* note 58, p.137.

[61]Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 1997/1998, Case number 1.

The third method is money laundering carried out by accountants and auditors. Accountants and auditors are exposed to provide financial services or advice in companies' operations. They are considered to be experts in the design, manage, organize, and maintenance of financial affairs of their clients. They also can be involved in carrying out financial transactions on behalf of their clients. Such activities include wiring money to and from various bank accounts, making cash deposits in different financial institutions, and issuing checks to the clients or their vendor and return for cash. These kinds of activities can also be misused for money laundering purposes. The following case is an example of an accountant's laundering methods.

> "A law enforcement operation identified an accountant, Mr. J, who was believed to be part of the criminal organization involved in money laundering and re-investment of illicit proceeds derived from drugs trafficking led by Mr X. Mr. J' s role was mainly that of 'legal and financial consultant'. His task was to analyze the technical and legal aspects of the investments planned by the organization and identify the most appropriate financial techniques to make these investments appear licit from a fiscal stance. He was also to try as much as possible to make these investments profitable. Mr J was an expert in banking procedures and most sophisticated international financial instruments. He was the actual financial 'mind' of the network involved in the re-investment of proceeds available to Mr X. Mr J operated by sub-dividing the financial transaction among different geographical areas through triangle transactions among companies and foreign credit institutions, by electronic transfers and stand-by credit letters as a warrant for commercial contracts which were later invested in other commercial activities".[62]

Based on the above explanations, it is clear as to how professionals assist in the laundering process of illicit funds. In conducting the crime, there is a co-operation between the primary criminals and professional launderers. This cooperation causes 'a progressive separation between criminal activities and money-laundering'.[63] Primary offenders, such as drug traffickers, carry out criminal activities that generate vast amounts of illegal funds. Meanwhile, professional launderers, such as lawyers, accountants, notaries, and other legal professionals, act as either supervisors or intermediaries that set up and carry out complex money laundering schemes. Money laundering through professionals is difficult to detect because this method is carried out under legitimate activities. It is even more difficult when sheltered under client confidentiality and the lawyer-client privilege. By taking advantage of the lawyer-client privilege, lawyers can avoid disclosing suspicion to the authorities.

---

[62]Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2003/2004, Case number 11.

[63]E.U. Savona, *Responding to Money Laundering: International Perspective*, Harwood Academic Pablishers, 1997.

2.7. Money Laundering through Electronic Money

Money laundering through electronic money, which is also called cyber-laundering, concerns the transfer of illicit proceeds into legitimate funds through the use of internet tools and stored value cards.[64] Cyber-laundering may be defined as the use of internet-based electronic wire transfer methods in order disguise the source of the illicit funds.[65] This type of crime occurs because of the emergence of electronic money[66] which has diverged into various systems of global payment networks and the internet. These include electronic payment system[67], wire transfer system[68], or internet banking.[69] These systems are used for laundering illicit funds for two reasons, namely, untraceable and incredibly mobile.[70] The first reason is supported by the fact that e-money is paid anonymously[71] and, as a consequence, it is difficult to implement the reporting requirements and an audit trail to follow the money. While in the second reason, e-money enables an instantaneous transfer of funds without the intervention of a financial institution. The speed and relative anonymity of wire transfers make it difficult if not impossible for law enforcement agencies to trace the trail of illegally generated cash. In this context, great quantities or high transaction levels of wire transfer are the main reason why tracing trails in this laundering method is extremely difficult.

Electronic money is also called e-money, e-cash, digital cash, digital money, digital currency, cyber currency, or New Payment Methods. E-money

[64]'Store value card or electronic purse is value stored electronically in a device such as a card with an integrated circuit chip (called a smart card or chip card)'. *See* Sarah N. Willing and Andy G. Rickman, "The Risk and Responses", 50 Florida Law Review, 1998, p.310. *See* also FATF Report on New Payment Methods, 2006, p.5.

[65]Stephen Jeffrey Weaver, "Modern Day Money Laundering: Does the Solution Exist in An Expansive System of Monitoring and Record Keeping Regulation", Annual Review of Banking & Financial Law, Vol.24, 2005, p.449.

[66]Hereinafter electronic money or e-money and electronic cash or e-cash are used interchangeable.

[67]The cyber payment system enables one to conduct significant transaction anonymously and entirely outside of the banking system.

[68]Wire transfer is the electronic transfer of money from one bank or entity to another.

[69]Internet banking is a new type of financial service created by the intersection of traditional retail financial services delivery and the emergence of the internet.

[70]Department of Justice Canada, Solicitor General Canada, "Electronic Money Laundering: An Environmental Scan", October 1998, p.8.

[71]As one report noted: '[t]he ability for criminals to remain anonymous on the internet presence a huge challenge for police and policy maker. Anonymity is assisted by proliferation of internet cafes and web kiosks, the emergence of data haven, the availability of tools for 'spoofing' and the presence of anonymising services on the internet". *See* Susan W. Brener, "Toward Criminal Law for Cyberspace: A New Model of Law Enforcement?". Rutgers Computer & Tech. L. J, Vol.30, 2004, p.32.

provides a way of paying for goods and services via the internet, otherwise known electronic trade (e-trade). In concept, e-money replaces cash for normal internet transactions. Customers use traditional money to buy e-money from an issuing company, and then use it to buy goods or services from a merchant who accepts the e-money as payment.[72] E-money might involve the use of store value cards (SVCs)[73] or the internet.[74] Some potential benefits of e-money to consumers include faster and efficient transactions; less need to carry cash; loyalty and frequent user plans; automatic personal financial record keeping; potential financial anonymity; potential security from theft; access to electronic commerce; and more personalized banking services and instruments.[75]

Smart cards are another example of e-money. The card has a potential to hold millions of dollars 'stored' on its micro-chip. Through e-cash and digital payments, the money can be transmitted electronically to another card on line without financial intermediaries. The process of cyber-laundering gives us an understanding into the unique characteristics of this kind of laundering, namely, instantaneous and anonymous.[76] The nature of these transactions is marked by the capability of criminals to deposit e-money via internet without the need of adhering to reporting requirements. This also means that the creation of an audit trail can be ignored.[77] Criminals also benefit in cyber-laundering since it becomes possible to use high level of encryption to block all law enforcement and transactions that fall outside the existing regulatory definition.[78]

The essential question in this context is how does cyber-laundering work? The process of cyber-laundering is almost similar to conventional

[72]Sarah N. Willing and Andy G. Rickman (1998), *Supra* note 64, p.298.

[73]Store Value Cards (SVCs) are the physical cards that contain the electronic cash. SVCs also called prepaid cards and value-added cards.

[74]It is a network-based system. In this system, a customer can purchase goods or services through internet by using personal computer.

[75]Department of Justice Canada, Solicitor General Canada, "Electronic Money Laundering: An Environmental Scan", October 1998, p.7.

[76]Steven Philippsohn, "The Dangers of New Technology: Laundering on the Internet", Journal of Money Laundering Control, 2001, p.87.

[77]Douglas, Fein, Indick, Mathews and Parker (eds), *The Emerging Law of Cyber banking: Dealing Effectively with the New World of Electronic Banking and Bank Card Innovations*, New Jersey: Glasser Legal work, 1996, p.415. Cited in Bren Fisse, "International E-Money System and Money Laundering", Paper, Presented at ASC Electronic Commerce Conference in Sydney, 4 February 1997.

[78]*Ibid.* Within this context, Weimer pointed out that 'the 'virtual reality' is that technology has provided individuals with a tool to place money on electronic cards. The launderers in this instance, could have carried out the alleged $7 billion on a card resembling an ordinary credit card, and transferred it directly to Noura without ever having traveled to New York. In this case, the internet transfer would be completed in seconds, law enforcement would have no means to trace the funds'. *See* Wendy J. Weimer (2001), *Supra* note 84, p.201

laundering methods, where it consists of three stages: placement, layering, and integration. The difference between these two laundering forms is primarily in the placement stage. For conventional laundering, the illicit funds are placed in a regulated financial institution. In cyber-laundering, the illicit funds are placed in an unregulated financial institution by means of a smart card or a computer-based internet connection. However, in the layering and integration stage, there is no significant difference between the two. An essential difference between them is the use of personal computers in carrying out the layering and integration.

A completed process of cyber-laundering which describes the three steps of laundering techniques can be elaborated in the following example.

> "In the first step, placement, cash may be deposited into unregulated financial institutions. Placement may easily be achieved by using a smart card or personal computer to buy foreign currency, goods, etc. Powerful encryption may be used to guarantee the anonymity of e-money transactions. The second step, layering, can be done through a personal computer. There is usually no audit trail in this stage. In addition, e-money systems allow for instantaneous transfer of funds over a system that, in effect, has no borders. The third step, integration, the criminal may be able to achieve by using a personal computer to pay for investment or to buy an asset without having to call on the services of intermediary financial institutions".[79]

Mark Borner describes a hypothetical case of cyber-laundering as follows:

> "Doug Drug Dealer is the CEO of an ongoing narcotics corporation who wishes to convert hard currency, the profits of his enterprise, into legitimate money. Doug employs Linda Launderer to hire couriers to deposit funds under different names in amounts between $7500 and $8500 at branches of every bank in certain cities [below the $10,000 cash transaction reporting limit]. This is repeated twice a week for as long as required. Linda has in the meantime been withdrawing these same funds and depositing the money with internet banks that accept e-cash. To be safe she limits these transfers to $8200. Now that the currency has been converted into digital e-cash, the illegally earned money has become virtually untraceable and Doug Drug Dealer has access to legitimate electronic cash."[80]

Another question is how does cyber-laundering threaten current anti-money laundering policies? The characteristics of cyber-laundering threaten current anti-money laundering which are designed to create reporting requirements and an audit trial.[81] Evaluating these potential threats, experts in law enforcement and cyber crime predict terrible consequences for the future of

---

[79] *Ibid*, p.11.

[80] R. Mark Bortner, Cyberlaundering: "Anonymous Digital Cash and Money Laundering" Paper Seminar at the University of Miami School of Law, 1996.

[81] Jonathan P. Straub, The Prevention of E-Money Laundering: Tracking the Elusive Audit Trail". 25 Suffolk Transnational Law Review, 2002, p.521.

anti-money laundering efforts and for society as a whole. Michael Nelson, a Clinton administration official in information security, predicts that by the year 2020, when the world is globally connected and where e-cash becomes the norm, the traditional notions of sovereignty, national security and welfare will fade.[82] Other experts predict that due to money laundering becoming increasingly undetectable and unpreventable, governments will start to lose its control over criminal organization.[83] The potential for the rapid movement of large sums of e-money transaction over the internet may also make it difficult for law enforcement to identify or track the transfers of illegal funds.[84]

2.8. Final Remarks

This chapter set out to understand the changing typologies and emerging trends of money laundering activities that have evolved over time. Initially, money laundering activities are conducted in the banking sector. However, due to the implementation of the anti-money laundering measures, money laundering activities became more difficult to carry out in this sector. This condition led criminals to try other sectors such as non-bank financial institutions that still have loopholes when it concerns anti-money laundering regulations. After the regime focuses on this target, the offenders search for other sectors such as professional agencies that involve lawyers, notaries, accountants, and other professionals. The movement of money laundering activities from banking sector to non-bank financial institutions, and then shifted to professionals, demonstrates the increasingly diverse methods are being used in conducting this type of crime.

The above description illustrates that in conducting money laundering, criminals attempt to find different targets and victims through the use of different methods and techniques. In this setting, criminals carry out money laundering through various techniques, from simple to complex and professional methods. Complexity refers to the use of sophisticated technologies in which laundering techniques are infinite and complicated. Professionalism deals with the employing of professional money laundering facilitators who assist and design schemes for conducting money laundering.

---

[82] *Ibid.* p.p.848-849.

[83] *Ibid.*

[84] Financial Action Task Force on Money Laundering, Annual Report 1997, Paragraph 25. ‘Once e-money system are used on a large scale. They will also handle a certain amount of these illicit funds. While it is not anticipated that e-money will consist of the same value as the wire system, it may consist of a larger value of transactions, thus illegal funds may be even more difficult if only because of the sheer volume of funds circulating within the system. The mass volume of the processing of computerized data will make it different to develop indicator to detect suspicious activity’.

These trends have also evolved from a domestic to a globalized scope. As a consequence, law enforcement authorities face great challenges in investigating and prosecuting these emerging threats of money laundering activities.

The FATF, through its recommendations, responded to this matter by obliging its member and non-member states to implement anti-money laundering measures in the banking sectors, non-bank financial institutions, and professionals. Major international standards were implemented that made it a requirement to follow the Know Your Customer (KYC) principle, to keep financial transaction records, and to report unusual or suspicious transactions. However, implementing these standards poses great challenges since criminals try to create new techniques and methods for laundering illicit funds that hinder the awareness of law enforcement authorities. In facing this problem, international as well as intergovernmental organizations, such as the United Nations, the World Bank, the International Monetary Fund, and the Financial Action Task Force, encourage countries to establish anti-money laundering regimes in all aspects of financial, business, and professional activities which are susceptible to money laundering practices. Here in this context, the expansion of anti-money laundering policy through the creation of international standards, that internationalize and criminalize money laundering activities, is extremely important. The following two chapters will discuss and analyze these matters comprehensively*****