IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Origin, Growth and Evolution of Money Laundering in the Cyber World

Dr.Sudarshan Nimma[1]

[1] Faculty Member & Chairman, Board of Studies, Dept of Law, KAKATIYA UNIVERSITY, Telangana

Abstract

Internet transformed the entire world into a global village. E-Commerce created a market without boundaries, cutting across the countries and the continents. A new dimension of offences has emerged in the present internet dominant world. New and novel style has begun in commission of money laundering offences with the dawn of IT revolution. The mode of commission of offence has changed. I.T is facilitating and contributing for the commission of money-laundering with the assistance of Internet. Like many illegal activities, money laundering is also underwent a rapid change due to technological advancements . These are facilitating the criminal syndicates to transfer their illegally gained money just with a click of a mouse across the globe using credit cards, e-wallets, internet banking facilities etc. Fund transfers are made directly between the parties. Thus unlimited amount is being transferred without having any strict checks today[2]

'Money Laundering' in Cyber Space

Today 'information and communication technology(ICT)' has penetrated in to all spheres of life. Internet transformed the entire world into a global village. Another latest feature of E-Commerce made this global village a market without boundaries. A new dimension of offences has emerged in the present internet dominant world. A new trend has begun in commission of money laundering offences with the dawn of IT revolution. The mode of commission of offence has changed. I.T is facilitating and contributing for the commission of money-laundering with the assistance of Internet. Like many illegal activities, money laundering is also underwent a revolutionary changes due to technological developments. These technical advancements are facilitating the criminal syndicates to transfer their illegally gained money just with a click of a mouse across the globe using credit cards, e-

[1] *Faculty Member & Chairman, Board of Studies, Dept of Law, KAKATIYA UNIVERSITY, Telangana;snimma26@gmail.com*

[2] such as checking cross border transactions by central banks of respective countries, that existed earlier.

wallets, internet banking facilities etc. Fund transfers are made between the parties directly. Thus unlimited amount is being transferred without having any strict checks today[3] Digital cash is sent around the world in a matter of seconds without raising any suspicion. These transactions leave no trail and are fairly easy to carry out.[4]

Facilitators to Cyber Laundering[5]

Internet

There has been a decline in face-to-face contact between customers and the financial institutions.[6] The increasing mobility of internet access virtually from any corner of the world, hence, the money launderers are facilitated very much operating their bank accounts from any where.[7]

- *Anonymity*

The internet on account of its novel feature of anonymity, easily facilitates the criminals to proceed with their activities suppressing their true identities and traceability. There are two aspects which help the launderers from disclosure or being caught.[8]

Faceless Contacts

There are only two checks for a bank customer in Cyber Space through the financial institution's server i.e. Log In (Unique ID) and Password. The customer is granted access upon furnishing true information.[9]

- *Faster Transactions*

It facilitates the movement of funds more speedier to the distant places within short span of time. Sadly, it also allows the movement of funds of launderers faster, sometimes outside the

[3] such as checking cross border transactions by central banks of respective countries, that existed earlier.

[4] Manmeet Singh, The Internet and Money Laundering, The Lawyers Collective May 2000, p.24.

[5]Skalski, 2004; GIFI, 2008

[6] The account usually operated by the customer on his personal computer using Internet browser software and world-wide web access through an Internet Service Provider (ISP). Access is obtained when the customer provides his personal identification code to the banks web server, and, when encryption software is used, the browser software generates the appropriate key. Because this access is indirect, the financial institution has no means of verifying identity of the individual actually accessing the account.

[7]FATF 1999-2000 Report on Money Laundering Typologies).

[8] Anonymity in internet communication and also the difficulty in following the path of communication from one Internet server to another.

[9] as such it would be harder to detect and hold up transactions related to money laundering activities. It also cuts out another potential source of reporting suspicious transactions.

country too. Resultantly, it facilitates the hiding of illicit source of money very easily and makes it difficult to trace it. The entire process does not cost much and cheaper.[10]

- *Internet without Boundaries*

The emergence of information and communication technology, brought a revolutionary change by transforming the entire world in to a global village. The information can be easily accessed today on the Internet cutting across all the geographical borders, barriers and boundaries.

Using Internet for the purpose of money laundering was analysed by the Financial Action Task Force on Money Laundering.[11] 'Cyber laundering' is considered to be the latest and most improved technique of money laundering. The FATF identified money laundering method using Internet[12] which contributes major part of G.D.P[13]. in many States like U.K, BRICS nations and the Asian block.[14] It is expected that these nations will be prone to embrace the internet for availing opportunities for entrepreneurial prosperity in the interest of their countries/people. No doubt, economic growth is appreciable, but such growth through e-commerce is also vulnerable and likely to be exposed to the risk of cyber attacks. This economic growth has also burgeoned the crime concomitantly.[15] Cyber victimization in U.K. reported alarming bells.

[10] Wojciech Filipkowsk, Cyber laundering: an analysis of typology and techniques International Journal of Criminal Justice Sciences, Vol. 3. Issue 1. 2008

[11] Financial Action Task Force submitted a report on new payment methods, based on a global survey. Still, some methods can be described as potential threat to financial institutions. These include electronic purse, mobile payments, and Internet payment systems, and there were only three cases connected with open system of pre-paid cards and the other two cases of close system of pre-paid cards. According to research, there were also 3 cases connected to digital precious metal services. At the same time no cases involving electronic purse, mobile payments, nor Internet payment systems were reported by member countries.

[12] wherein the launderer starts a company, offering payment services on internet, and the launderer makes use of services and charges through his credit and debit cards linked to accounts under his control, generally located in an offshore area that contain criminal proceeds. The launderer's company send invoice to the credit card company, which make payment for the service rendered. Later, these payments for the services, would be justified by the company of the launderer.

[13]According to Phil Butler, in his book "Cyber Crime, Financial Fraud and money laundering*acceluscdn.thomsonreuters.com/accelus-pdf/GRC00331-Cybercrime-Phil-Butler.pdf*

[14] In the UK alone, the internet is estimated worth over £100 billion and that 7.2% of the UK's GDP is generated over the internet. In 2009, the so-called BRICS nations, Brazil, Russia, India, China and South Africa, represented 45% of the world's population and were responsible for 15% of global GDP.

[15] In the UK, the cost of cybercrime is estimated at £27 billion per year, whilst global cybercrime is estimated at US$1 trillion per year - and growing. Furthermore, research shows us that 23% of all UK web users have fallen foul of a phishing scam and 1 in 5 has been a victim of a scam email or website, with an associated cost of about £3.1 billion. Over 20 000 hacking attempts on the government infrastructure of the UK are detected each week. Of major concern are Trojans, Worms and hackers infiltrating IT systems and stealing money and information.

Globalization of World Economies

'Globalization of Economies' across the World facilitated free movement of goods and services, between the counties cutting across continents. The economic globalization includes, entrepreneurs and customer's need of moving, investing and spending money wherever they wish. With the help of growing information technology, new payment technologies have emerged. These facilitated to do businesses over long distances and not required to carry large quantities of cash today. Next is 'investments mobility'. Access to the Internet and on-line services is easy. This channel of the distribution of monetary or investment product has become a vital issue. These services may become more significant for monetary establishments in near future. To promote trade between different nations or movement of funds across the globe, there is a rising trend to reduce certain legal obstacles, more efficient way of investing them are being explored.

Perceptions on 'Cyber Laundering'

The phenomenon of cyber laundering emerged with the advent of internet, which has become a powerful tool/medium for the criminals to launder their criminal proceeds. Cyber laundering covers two distinct fields of crime 'Cyber Crime' and 'Money Laundering'. This combination of hybrid discipline raises a doubt as to how cyber laundering should be seen and under which category of crime does it fall. To understand this confusing situation to establish suitable legal framework, it is essential to view it from a right perspective, so as to fix its position in the right place. The concept of cyber laundering falls in to the following 3 categories.

1st View:- "Cyber Laundering - A 'Subset of Cyber Crime"

When cyber laundering is viewed as a subset of cyber crime, it comes under cyber crime, ignoring the money laundering element. In that situation, it can be confined solely to the field of informatics. But, this notion is not completely acceptable. Although the Cyber laundering has roots in cyber crime, the core element of money laundering cannot be ignored. Hence, the crime as basic element of money laundering, with a technological advancement.

2nd View:- Cyber Laundering - A Money Laundering Technique

Another famous school of thought treats it just as technique within the big canvas it as of money laundering. Since the technique used internet, it is concluded that money laundering is executed with that technique.[16]

[16] This notion might be plausible if one looks at the broad concept of money laundering, which entails several other aspects, for instance, trade-based money laundering. It is totally incorrect to accept that cyber laundering is only a technique of money laundering. To think of something as a 'technique' of another would mean that the latter is a means to an end, and, impliedly, that it cannot stand on its own. As regards cyber laundering, the fact that a criminal utilizes technological resources does not make such resources mere a tool for the money laundering enterprise; conversely, this makes the criminal's activity the money laundering enterprise.

3rd View: Cyber Laundering, an Advanced form of Money Laundering

Appropriate answer for conceptual phrasing of cyber laundering lies at the heart of the crime is money laundering itself. It is appropriate to say that cyber laundering is money laundering, of more advanced form, having its roots in technology.[17] Since it is accepted that cyber laundering is money laundering and the primary liability is created for such money laundering.[18]

Mentioning Crime in the 'Charge Sheet'

When the cyber launderers are prosecuted by the prosecution for their involvement in cyber laundering activities, it is only the name of the crime written in the charge sheet is 'money laundering, but not cyber laundering. In essence, cyber laundering is not a separate crime and it remains only under the umbrella of money laundering [19].

Process of Cyber Money Laundering

In simple terms it is the offence of money laundering executed in cyberspace using online transactions.. It involves three stages[20] The perpetrators can act from any corner of the world, the only requirement is internet access. Like Traditional type of Money laundering, the case of money laundering in cyber space also, the same 3 stages for laundering money are involved i.e. Placement, Layering and integration stages.

1.Placement

It consists of introducing illegally gained criminal proceeds into the legal financial system. These proceeds are mostly in the form of 'e-money' to be used for subsequent transactions, Foreign currency and High value goods are purchased and resold again. Therefore e-money is used to introduce illegally acquired money without smuggling cash and without face to face transactions.

[17] Although it overlaps with the concept of cyber crime, it should not be seen entirely in that light. The gravity of the cyber laundering problem, which already embodies the behemoth weight of money laundering, exceeds the severity of other kinds of cyber crimes combined. It is important to know the right category in which cyber laundering falls, because understanding the right framework, would inadvertently determine the kind of liability it creates

[18] However, cyber laundering is unique for the fact that it is likely to create subsidiary or ancillary liability for the criminal other than the liability for money laundering. It could incur liabilities under the broad notion of cyber crime, or other subsets of cyber crime, in jurisdictions where such crimes are recognized. Such ancillary liability differs from the traditional predicate offences that usually establish liability for the crime of money laundering. For example, a cyber launderer is found liable for the crimes like hacking or cyber-vandalism, and both of them not necessarily be predicate offences for the main crime of money laundering.

[19] The sad reality is that the gravity of the cyber laundering dilemma gives rise to an escalation of the current money laundering problem. This hinges on the overall purpose of this study, which assesses the possibilities of forging a proper legal framework to counteract the problem. However, a foreseeable challenge to actualizing this goal lies in one underlying truth - cyber laundering is a complex problem with very serious legal ramifications.

[20]CYBER-LAUNDERING, THE NEW FACE OF MONEY LAUNDERING IN THE DIGITAL AGE ---Putri Pertiwi; https://integrity-asia.com/blog/2018/09/26/cyber-laundering-the-new-face-of-money-laundering-in-the-digital-age/

2. Layering[21]

It involves too many complex transactions aimed at creating more distance between the source of origin of funds and laundered funds. Internet plays a vital role at this stage as it facilitates money laundering. Such money passes through many jurisdictions rendering it hard to be tracked and source becomes virtually untraceable.[22] Internet does have jurisdictional issue i.e. the place of the transaction i.e. whether at the place of launderer, or at the location of the server or where the accounts are recorded.[23] Some examples of layering phase include,

- Inter bank transfers
- Online fund transfers between various accounts
- Fund Transfers to foreign/offshore countries
- Chang of Currency
- Purchase of high-value goods

3. Integration

It consists of money returned, which is laundered'. At this stage, the money can be used by the owner, which appears as legitimate, legal wealth. Most common traditional technique used here include, raising false invoices for the goods and services and using the internet services of a company, projecting that, the services are rendered in return for payment of money routed through layering process.[24] Thus, owner's wealth appear as legitimate profits earned [25]

Cyber Laundering Techniques

Most of the cyber laundering activities are carried out by highly educated, technically competent persons. These experts develop very complex, unconventional and diverse money laundering methods. Certain Common features of Cyber laundering techniques are as follows.

- Using Accounts opened by submitting lost documents
- Using Shell /artificial companies

[21] Layering is the process of passing the dirty money by the launderer through a complex series of transactions separating it from its illegal source, i.e. transfer of money through offshore companies and purchase of goods for resale etc. and legitimizing money through accounts of others or paying tax on it as income from a business.

[22] Phil Butler, Cyber Crime, Financial Fraud and money laundering*acceluscdn.thomsonreuters.com/accelus-pdf/GRC00331-Cybercrime-Phil-Butler.pdf*

[23]Layering became very easy, if the money is transferred between banks, dealing with e-money. Then the anonymity features of some types of e-money may make the source virtually untraceable

[24] For example, the laundered money may be in a bank account held in the name of a fictitious person or shell company. Payment will be made from that account to the Internet service company, as purported payment for a service. The service may be an Internet casino or betting purpose.

[25] See generally: Phil Butler, Cyber Crime, FinanCial Fraud and money laundering*acceluscdn.thomsonreuters.com/accelus-pdf/GRC00331-Cybercrime-Phil-Butler.pdf*

- Fund transfers through too many Accounts with remotely accessing
- Using Cash at the final stage of after a series fund transfers
- Purchasing electronic money and e-wallets
- Converting illegal proceeds into goods through online purchases'
- Using Alternative Payment Systems/e-payments

  These Payment methods are used as an alternative to the credit card payments both nationally and internationally. More common alternative payment methods include, Debit cards, Prepaid cards, Charge cards, Bank transfers, direct debits, phone and mobile payments, cheques, Money Orders and Cash Payments. Electronic payment systems both at the national and international levels facilitate the criminal to launder cybercrime proceeds quickly[26] and effortlessly because of the following advantages such as,
- Easy Accessibility of the Accounts i.e, free to every User
- Opening and using electronic accounts does not require any special knowledge
- Online Operation of accounts by the User from remote places.
- Transactions are executed within seconds
- Protected data(since the data transferred is encrypted)[27]

These activities[28] consist of using lost/stolen counterfeit payment cards, skimming, cloning of plastic cards, Transaction Reversal Fraud, Cash Trapping etc.

The other important money laundering method involves '*Cash withdrawals through ATMs'* which facilitates the launderers to avoid direct facing of the launderer with the bank. Accordingly the cash withdrawn is sent to the cyber crime organizer through the brokers (money couriers/mules). Proceeds of the Crime are mostly used to buy prepaid cards, tickets, travel documents, household items, readily marketable goods etc.

[26] Criminals value electronic money for their anonymity in opening and replenishing e-wallets, round-the-clock availability and speed of transactions (within seconds). The e-wallets of private persons tend to be connected to such persons' e-mails or mobile phone numbers.

[27]Cybercrime and Money Laundering - eurasiangroup.orghttps://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014_English.pdf

[28] a) Use of lost/ stolen/ counterfeit payment cards.
b) Theft of payment card details, inter alia, with the application of card cloning devices,
c) Skimming – production, sale and installation of devices on ATMs for reading/ copying data of a payment card's magnetic stripe and stealing PIN codes,
d) Use of white plastic for cloning (counterfeiting) payment cards and withdrawing cash from ATMs,
e) Transaction Reversal Fraud
Interference with ATM operation where an error condition is created which makes it appear that cash will not be dispensed. This forces a re-credit of the amount withdrawn back to the account when in fact a perpetrator gets the cash,
f) Cash Trapping
attaching a device to ATM so that when ATM tries to dispense cash the cash is trapped and legitimate card holder cannot receive it.A perpetrator then returns to the ATM and retrieves the trapped cash.

FATF's Concern on New Methods of Money laundering

The internet today is giving scope for certain novel, undetectable methods of money laundering without necessity for interface between money laundering and technology. Thus, Banks are moving money through available messaging systems, instead of physical movement from one place to another place.[29]The following 3 kinds of transactions were considered as risk factors[30]a) Electronic Payment Systems[31]These payments are made through internet.[32]b) Converting Illegal Real Cash in to e-Money'[33]

E-money is gradually assuming importance due to the concept of 'illegal e-money.'[34] Today, using Internet's e-payment systems[35] illegal hard cash can be easily converted into e-money comfortably. c) Laundering through 'e-money'/Digital Money. Internet allows digital money transfers without the requirement of any financial institution. The e-money systems do not verify each and every money transaction. Only checks certain suspicious activities. Therefore, cyber laundering effectively eliminates the recording intermediary. This renders ineffective traditional tracking systems via a paper trail of monetary transactions. It means, the cyber launderers can be able to make large payments to individuals/corporation in other jurisdictions, which will not be noticed completely. It facilitates integration/investment of the money in capital rich economies. The direct transfer of money from cardholder to cardholder eliminates the audit trail.[36]

[29] In this context, the Internet is simply an updated check system or a more efficient, cheaper, and more secure means of moving financial information. Morris-Cotterill, N. (2001), Money Laundering, Global Policy Forum Web, http://www.globalpolicy.org/nations/corrupt/2001/05morris.htm

[30] 1.Internet is used as a distribution channel for financial instruments, cards, etc.; 2. No face-to-face contact with the customer who purchases such an instrument, card etc. 3.Payment method is an open network type, which can be accessed in numerous jurisdictions. http://www.fatf-gafi.org.

[31]It refers to a financial exchange in the form of an encrypted financial instrument.[31]

[32] The evolution of e-payment systems began with the concept of electronic funds transfer (EFT) in 1940s. EFT gave rise to the notion of a transferable information-based data through computer and telecommunication components. The concept of EFT has now been largely replaced with electronic commerce payment systems which are online-based.[32] such as an encrypted credit card number, digital cash or an electronic cheque, which is usually backed by a bank, an intermediary, or a legal tender. It refers to a financial exchange in the form of an encrypted financial instrument.

[33]E-money, also known as digital money, electronic money and e-currency, is a form of money that is digitally stored as opposed to actual paper or coin currency. use of e-money involves the computer, the internet and wireless transfers.

[34]Illegal e-money refers to funds which are either derived from the cyber world, the internet environment, or funds that were originally hard cash of illegal nature are transformed into e-money of illegal character.

[35] Ibid note supra

[36] In addition, Internet commercial transactions allow the user to dial up and shop online with only an Internet address of IP number. Therefore, the identity of the customer is not known. Moreover, the Internet could be a mediator which facilitates money laundering. Specifically, it promotes two factors that are conducive to money laundering i.e. a) Trans-national transactions cutting across the national boundaries and b) Anonymity

Emergence of internet and e-cash got rid of the risks of traditional form of carrying cash physically The money launderers opted for new modes and modus operandi of cash transactions and wire transfers facilitating organized crimes and legitimate business.[37]

[37] and individual banking customers enjoy a swift passage for moving money between jurisdictions, although there are very few criminal cases connected purely with Internet (it depends on jurisdiction), it does not mean that there is no cyber laundering activity going on.