CYBER LAUNDERING: AN OBSTACLE IN TRANSPARENCY AND ACCOUNTABILITY OF INDIA

Nidhi Tewari & Srishti Vaishnav

INTRODUCTION

The advent of digital technology has made the world interconnected and has made the entire economy of a nation or a world at large increasingly reliant upon a single, network infrastructure called-*the Internet*. Although, it offers tremendous opportunities to many industries like, financial, telecommunications, health, and transportation but, it can create serious security issues if appropriate preventive measures are not taken. The nature of cyber space is such that, regulating and controlling it completely is not possible. It is for this very reason many crimes such as theft, fraud and extortion can occur in greater magnitude within a few seconds and the feature of anonymity, sometimes, makes it impossible to reach the offender. Thus, the new network-mediated economy paradoxically presents unparalleled opportunities for the creation of good outcomes or the perpetuation of bad ones.

One such internet crime is, Cyber Laundering. It is money laundering through internet i.e. it is a new way to hide the illegally obtained money and integrating it in the mainstream economy as legitimately earned money. Its advance technological nature has eliminated the need for time and space as compared to the traditional way of money laundering. Money laundering in any form imposes a serious threat to the nations' economy but cyber laundering imposes an increased threat as in a virtual space, where identities can be easily hidden or changed, it becomes a difficult task for enforcement authorities to control the same. The reasons to take serious and immediate measures against Cyber Laundering are numerous for example, over throwing governments, turning black money into white money, financial frauds, hiding the source of income, drug dealing and black market of weapons of mass destruction and last but not the least it is because of the gains involved in this business.

Since it is 'world wide web', the preventive measures should also be such which covers the complete world. Governments of the world are working towards preventing cyber laundering. They have come up with various combating mechanism at international level which will be dealt with in this paper. At national level, India has laws to curb money laundering but, there is no specific provision regarding cyber laundering.

The authors, through this paper, will deal with the concept of cyber laundering in detail and discuss the combating mechanism at both, national and international level. Suggestions to improve the present condition will also be put forth.

MONEY LAUNDERING AND ITS STAGES

Prior to taking a leap into what cyber laundering is, the understanding of the concept of money laundering and how it is carried on is vital. In simple words money laundering is the process by which black money is converted into white money.

Black money is the generic term used for the money acquired through illegal sources, which range from tax evasion to terrorism. Since the money has been acquired through illegal means, it is not accounted for and hence, kept hidden because transactions can be traced back to the illegal source. To save themselves from the apprehended trouble, the black money holders adopt the method of money laundering.

It is like washing all the dirt off the money and hence, the term 'laundering' is used. It is a process, which builds an illusion that the black money was acquired through a legitimate source. To make the meaning more lucid and specific, we will use the definitions of money laundering.

The first one is given by ***International Compliance Association*** and it states: Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.[1]

The second is the definition listed in the ***Business Dictionary****:* Money Laundering is the Legitimization (washing) of illegally obtained money to hide its true nature or source (typically the drug trade or terrorist activities). Money laundering is effected by passing it surreptitiously through legitimate business channels by means of bank deposits, investments, or transfers from one place (or person) to another.[2]

[1] *What is money laundering?* (2016) Available at: http://www.int-comp.org/careers/a-career-in-aml/what-is-money-laundering/ (Accessed: 2 April 2016)

[2] Web Finance, 'What is money laundering? Definition and meaning', in Available at: http://www.businessdictionary.com/definition/money-laundering.html (Accessed: 1 April 2016)

And, the third is the one used by **INTERPOL**: INTERPOL's definition of money laundering is: "any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources".[3]

All three definitions point out that there are three main components:

1. Source used is black money
2. There is a process to make the black money appear as white money
3. The product is white money, or to be more specific, black money with an appearance of white money

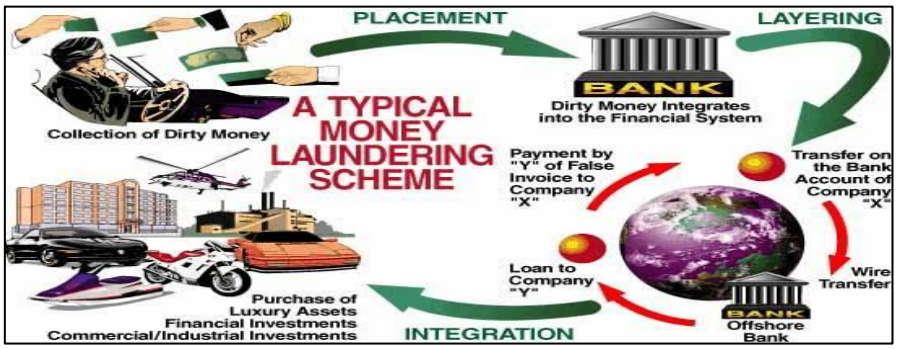
The source and product are, both, clear and palpable. What attracts curiosity is the process and therefore, we shall now be dealing with the process in detail.

Stages of Money Laundering:

The process of money laundering, conventionally, has three main stages:

1. Placement
2. Layering
3. Integration

Figure 2.1[4]



Placement: It is the first step, i.e. the step, which introduces the black money into the financial system. Generally, this stage serves two purposes: (a) it relieves the criminal of holding and guarding large amounts of bulky of cash; and (b) it places the money into the legitimate financial system. It is during the placement stage that money launderers are the

[3] 2016, I. (2016) *Money laundering / financial crime / crime areas / Internet / home*. Available at: http://www.interpol.int/Crime-areas/Financial-crime/Money-laundering (Accessed: 8 April 2016)

[4] *Money-laundering cycle* (2007) Available at: https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html (Accessed: 18 March 2016)

most vulnerable to being caught. This is due to the fact that placing large amounts of money (cash) into the legitimate financial system may raise suspicions of officials.[5]

There are a number of methods, which are adopted to introduce the dirty cash into the financial system. Some of them are as follows:

1. Loan Repayment – Repayment of loans or Credit bills with the illegal proceeds
2. Gambling – Using black money for the purchase of gambling chips or placing bets/wagers on sports events
3. Currency Smuggling – Physical movement of illegal cash over and across borders
4. Currency Exchanges – Purchasing Foreign money with illegal funds through foreign currency exchange
5. Blending Funds – Using a legitimate cash focused business to co-mingle dirty funds with the day's legitimate sales receipts[6]

The above listed methods are mere illustrations. The black money holders come up with new tips and tricks to launder the dirty cash and the innovation is unparalleled.

Layering: Once the money is introduced in the financial system, the second stage of layering comes into picture. Layering, basically, comprises of certain transactions, which conceal the illegal source of the money introduced. There are multiple transactions done in order to hide the actual source of the dirty money. The transactions act as layers to camouflage the illegal origin and hence, this stage is called layering.

Layering can be done through all or any of the following methods:

1. Sending funds to different onshore and offshore banks
2. Creating complex financial transactions
3. Loans and borrowing against financial and non-financial assets
4. Letters of credit, bank guarantees, financial instruments et cetera
5. Investment and investment schemes
6. Insurance products[7]

---

[5] *bout business crime solutions - money laundering: A Three-Stage process* (2015) Available at: https://www.moneylaundering.ca/public/law/3_stages_ML.php (Accessed: 25 March 2016).

[6] *Ibid* Note 5

[7] Renner, P. (2012) *What is money laundering?*. Available at: http://kycmap.com/what-is-money-laundering/ (Accessed: 25 March 2016).

Integration: Post layering, comes the final stage of money laundering – Integration. Integration refers to the acquirement of the money, which has been generated through the transactions under the second stage. Here, the illegal proceeds are reintroduced in the legitimate financial system. This gives it an appearance of having been acquired through legitimate means. The money, hence, comes back to the criminal and can be used in any way he fancies. Again, there are several ways in which it can be done, for example:

1. Buying business
2. Investing in luxury goods
3. Buying commercial property
4. Buying residential property[8]

There are many different ways in which the laundered money can be integrated back with the criminal; however, the major objective at this stage is to reunite the money with the criminal in a manner that does not draw attention and appears to result from a legitimate source.[9]

There are three stages, but together they form one single transaction of money laundering. Also, it should be noted that the entire transaction is impossible to execute without the involvement of banks. Banks are doing business as a service industry and as an intermediary in formal sector dealings in finance. Entry of cash into the financial system requires banking services. A bank's source of funds are deposits received from depositors in return for various kinds of services and placement of funds for exchange of value (sale of goods and property) and land in banking accounts.[10]

Banks are the most widely used institutions because of the advantages they offer. These advantages are convenient, accessible and safe for money launderers to use banks and to access to International payment system, which offers them the ability to transfer money through modern electronic methods instead of using the traditional methods.[11]

[8] *Ibid* Note 7

[9] *About business crime solutions - money laundering: A Three-Stage process* (2015) Available at: https://www.moneylaundering.ca/public/law/3_stages_ML.php (Accessed: 26 March 2016).

[10] Kidwai, A.J. (2006) 'Money laundering and the role of banks', *Pakistan Horizon*, 59(2), pp. 43–47. doi: 10.2307/41394125.

[11] *The positive and negative role for banks in money laundering operations* (2012) Available at: http://www.cscanada.net/index.php/css/article/view/j.css.1923669720120805.1742/3111 (Accessed: 30 March 2016).

Having understood what money laundering is and how it is carried out, we shall now proceed to discuss what cyber laundering is.

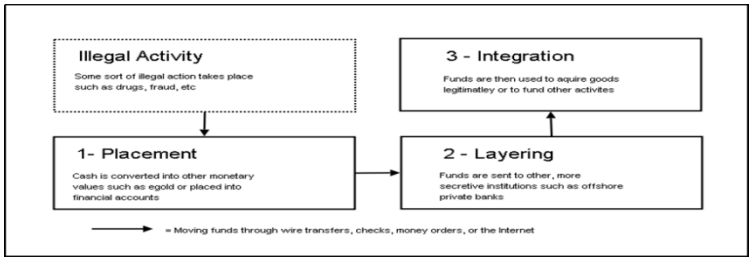
CYBER LAUNDERING: MEANING AND STAGES

The advancement of technology has benefitted everyone, including criminals. Fiscal transactions, as it is, are complex and cash transactions are difficult to trace. The conventional methods of monetary transactions are barely used nowadays. Most of the people, who have an access to Internet, prefer executing transactions over cyberspace. As already discussed in the previous chapter, to wash the filth off the dirty money, a number of transactions are performed using that money. Now, with the help of online transactions, money laundering is also carried out. This form of money laundering is popularly called as cyber laundering.

Cyber laundering can be defined as: utilizing Internet-based electronic wire transfer methods, such as Internet banking or online gambling, in furtherance of disguising the source of illegally obtained money.[12]

To break it down in simple words, money laundering executed over cyberspace is cyber laundering. Sometimes, it is also referred to as cyber money laundering.

The stages of cyber laundering, obviously, are similar to that of traditional money laundering. The different lies in the modes adopted.



Placement: As already discussed in the previous chapter, this stage involves the introduction of dirty money in the financial system. The traditional methods have already been enumerated and in cyber laundering, the placement is done through internet transactions and e-cash. E-cash is Electronic cash. Examples include prepaid cards, payment cards, special electronic checks from electronic bank accounts; micro-payments, anonymous cash, also

[12] Stephen Jeffrey Weaver, Modern Day Money Laundering: Does the Solution Exist in An Expansive System of Monitoring & Record Keeping Regulations?, 24 Ann. Rev. Banking & Fin. L. 443, 444 (2005).

coupons, scrip, smart cards as well as debit cards and electronic wallets.[13] There are various e-cash service providers and the most popular ones are google checkout and paypal. The reason why e-cash or internet transactions are used is that it provides for anonymity. The identity of the one making transactions is protected and the transactions go undetected.

Layering: Traditionally, layering involves a number of complex transactions to hide the source of black money. Because a high number of transactions are involved, there is a risk of exposure at one level or the other. In this reference, cyber laundering provides for a much safer platform. The launderers have made the optimum use of internet services to bring layering into effect. The launderer usually finds an institution, such as an online gambling site that will permit him to set up an account without physical verification or documentary identification. This makes it extraordinarily difficult for enforcement authorities to trace the account back to the cyber launderer. Furthermore, the internet provides near instantaneous transfer of funds which can occur anywhere in the world, as the only requirement is to possess an internet connection. Online bank transfers are particularly difficult to trace back, particularly where there is use of disguised IPs etc.[14] As the money moves from one transaction to another, it becomes more and more difficult to trace its source, and hence, cyber laundering is being practiced far and wide.

Integration: Mingling the 'clean' money back into the system so that the investor can gain it back is, again, a complicated process. Cyberspace, however, makes it easier. Internet gambling, online casinos, pre-paid debit cards and virtual economies are a few ways adopted by the launderers to regain their money back. For instance, a launderer could setup an online gambling site and transfer illegal funds, mixing it with the proceeds of the site itself. The funds then appear legitimate to authorities tracing the audit trail of the profits. In fact, the launderer could use legitimate bankers and lawyers at this stage, without too much hassle. Other modes of integration include using debit cards issued by offshore banks to make purchases online, fake loans from offshore companies, or simply executing a traditional integration measure, like purchase of real estate, online.[15]

[13] *The definition of e-cash - electronic cash* (no date) Available at: http://www.itvdictionary.com/definitions/e-cash_definition.html (Accessed: 1 April 2016).

[14] Jonathan P. Straub, The Prevention of E-Money Laundering: Tracking the Elusive Audit Trail, 25 Suffolk Transnat'l L. Rev. 515, 522 (2002)

[15] Steven Philippsohn, The Dangers of New Technology – Laundering on the Internet, 5 J. Money Laundering Control 87 (2001).

A merely reading of the stages of traditional and cyber money laundering makes it so evident that the use of internet has given the crime of money laundering new dimensions and made it easy for the criminals to camouflage and money, but extremely difficult for the authorities to trace the transactions. It is discernable why cyber laundering cases have increased by leaps and bounds in the last one decade and there is an urgent need to keep a check on the issue, in order the keep the national away from the perils of fiscal crisis.

THREATS DUE TO CYBER LAUNDERING

Money laundering (whether in physical form or through cyber space) can impose following threats-

Terrorism Financing: To combat terrorism, it is necessary to destroy support systems that aid execution of a terrorist attack. This would include the financing of terror groups, which is usually done using laundered money. The scale of the problem came to light immediately after the September 11, 2001, attack on the World Trade Centres in New York. Terrorists themselves are not too concerned about disguising the origin of the money, but rather on concealing its destination and purpose. The widespread availability of the internet provides a convenient method for terrorist organizations to transfer funds, both illegal and legal, to cells across the globe.[16]

Fuel for Organized Crime: The concept of money laundering is applied mainly to carry out organized crime like drug trafficking. With most countries having strict laws on drug control, money collected from the sale of drugs will always need to be laundered. Large-scale drug traffickers face a unique problem of managing large sums of cash, much of it in small bills obtained from the payments made by customers and therefore, they tend to launder the amount so earned.

Corruption: Corrupt public officials have to launder their illegal money earned through bribes, kick-backs and siphoned public funds. The famous Koda Scandal, involving money laundered by the former Jharkhand Chief Minister, Madhu Koda, is a prime example of such threats.[17]

[16] Stephen I. Landman, Funding Bin Laden's Avatar: A Proposal for the Regulation of Virtual Hawalas, 35 Wm. Mitchell L. Rev. 5159, 5169-5171 (2009).

[17] News Report, Madhu Koda and Associates Laundered a Staggering Rs. 3356 crore, INDIA TODAY, February 20, 2012, New Delhi.

Negative Impact on the Economy of the Country: Money-laundering may affect a nation's economy by increasing the rate of inflation, making the interest and exchange rates high and reducing the value of rupee.

Loss of foreign investment: Nations with weak anti-money laundering mechanism attract less foreign investors as, these countries lack to fulfil the two key requirements of such investors i.e., stable conditions and good governance.

BENEFITS OF CYBERSPACE- WHAT ATTRACTS LAUNDERERS?

- **Anonymity:**

  The Internet provides a virtual world where anyone can hide his/her actual identity and pretend to be someone else. But it seems that is no longer true, since there are some legal obligations put on Internet Service Providers to record and keep log files for a long period of time. However, there are some means to circumvent them and to keep the anonymity. They include Internet Protocol (IP) spoofing, use of modem connections (every time user connects he gets different IP address), Wireless Fidelity technology which allows to abuse publicly open so called "hot spots". Also the use of encryption technology (widely available on the Internet) and many proxy servers hinders the efforts of law enforcement to catch cybercriminals.
- **No face-to-face contacts:**

  The whole process of placing orders (making requests) and executing them is fully (or partially) automatic without the presence of a human factor. So in fact we can very easily pretend to be someone else each time we "visit" bank in the cyberspace. The financial institution's server checks only two things, the Login ID and the password – not the true identity of a customer and grant access. As a result, it would be harder to detect and hold up transactions related to money laundering activities
- **Speed of the transactions:**

  New payment technologies permit to move funds more rapidly on long distances and make law enforcement work even more complicated.
- **Globalization process: free movement of goods, services, people and new payment technologies:**

  The globalization of economy includes the necessity for people (entrepreneurs and customers) to move, invest and spend money wherever they want to. In order to achieve that with the help of developing information technology, there have emerged

new payment technologies. They allow freeing ourselves from carrying large quantities of cash, as well as to do businesses at a long distance.

- **Cross border activity: involves several jurisdictions, mutual legal assistance treaties issues:**

  The on-line service provider's abode usually differs from the place where the servers are located in reality, from where these servers are administrated, or from where the client accesses the Internet and thereby involves different countries & several jurisdictions, in the case of an offence. The cooperation between law enforcement, revenue services and judiciary is one of the most difficult tasks as far as the trans-national criminality is concerned.[18]

MECHANISM AND WORKING OF CYBER LAUNDERING

As discussed above, the concept of cyber laundering mirrors the traditional concept of money laundering. However, the method in which the money is laundered varies in the virtual space. Cyber laundering has eliminated the physical effort of actually transporting currency as was the with classic methods which included, flying hard cash out of one country and depositing it in a foreign bank, bribing a bank teller, discretely purchasing property, or for "smurfs" to deposit small cash amounts at a bank to avoid reporting requirements.[19]

These methods have now evolved with advent of cyber laundering. Now, the goal of any mechanism applied by the launderer is to convert one liquid asset into another asset, which is preferably in a less liquid form. This helps in making the identification of the source of the acquisition as difficult as possible. In cyber laundering, the principle followed is "dispositional imperative" of money, which treats money only as medium of exchange and not an end in itself. According to it, it is useless to keep money as a product in itself, and needs to be "disposed" to yield any benefit to the holder.[20]

Mechanism and techniques carried out by cyber launderers largely focus on two aspects-

[18] Wojciech Filipkowski, Cyber Laundering: An Analysis of Typology and Techniques, available at- http://www.sascv.org/ijcjs/Wojciechijcjsjan2008.pdf, (Accessed 6th April 2016)

[19] Sarah N. Welling, Smurfs, Money Laundering and the Federal Criminal Law, 41 Fla. L. Rev. 287, 290 (1989)

[20] Brett Watson, The Global Response To Money Laundering, available at http://www.aic.gov.au/events/aic%20upcoming%20events/2002/~/media/conferences/2002-ml/part1.pdf (Accessed 5th April, 2016)

1) To legitimize illegal obtained money, 2) To dupe the enforcement authorities so as to escape without being noticed.

The mechanisms and incidents of cyber laundering can be read under two heads, firstly, the traditional mechanism and secondly, the modern approach.

TRADITIONAL APPROACH-[21]

- **Wire transfers:**

  Wire transfers i.e. electronic transfers allow swift and nearly risk free channel for moving money between countries. As, on average 700,000 wire transfers occur daily in any major jurisdiction like the US, UK or India, moving billions of dollars, illicit wire transfers are easily hidden. This is often employed for bulk-cash movements across jurisdictions and into banks where the regulations are not so strict.

- **Cash incentives business:**

  Any business typically involved in receiving large cash inflows will use its accounts to deposit both legitimate and criminally derived cash, claiming all of it as legitimate earnings, as the source of the funds is difficult to trace when payments are made in cash. Any service-based online business is best suited for such a mechanism of laundering as the source of the funds is difficult to trace when payments are made in cash.

One such example is **Online Casinos.** They are the hotbed for cyber laundering activities. Cash may be taken to a casino to purchase chips which can then be redeemed for a casino cheque. Person could deposit cheques in the bank account and claim it as gambling winnings. For this amount, he would have to pay a negligible amount of tax as compared to his total illegal earning. Hence, the illegal money is easily integrated with the mainstream economy. Moreover, non-requirement of physical cash in the whole process has made this mechanism all the more viable for launderers. E-cash can be used and later converted into legitimate physical earnings.[22]

[21] Jagdish Menzes, Cyber Laundering: The new Internet Crimes, available at- http://thegiga.in/LinkClick.aspx?fileticket=xpxlb4qgFTw%3D&tabid=589 (Accessed: 4th April, 2016)

[22] Financial Action Task Force, Report on the Vulnerabilities of Casinos and the Gaming Sector, 1 February 2012, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf (Accessed: April 5 2016)

Having a physical address over the internet does not really mean that something exist there. Due to huge financial support from the criminals these online casinos sometimes operates anonymously without the need to have a physical address (IP-address) and to register this anonymity on the internet the owners of the online casino pays huge monthly and annual fees to the government of that country. Due to the non-existent background checks by the jurisdiction of these online casinos website it is difficult to regulate this market to restrict Cyber laundering.

- **Trade Base Laundering**

  In order to disguise the movement of illegal funds through trade based transactions, under-valuing or over-valuing of invoices could be done. Similarly, in cyber laundering invoices can be quickly created and easily tampered so as to adjust illegal amounts with legal payments.

- **Round tripping**

  In this mechanism, money would be deposited in a controlled foreign corporation offshore, such as in a tax haven with minimum regulatory requirements, and then shipped back as foreign direct investments, exempt from taxation.[23] In respect of cyber laundering, all jurisdictions allowing related transactions to be done in electronic form would be preferred by the launderers.

- **Shell companies / Black Salaries / Fictitious Loans**

  Shell companies are meant to disguise the true beneficial owner of the assets. Black salaries are either where salaries are "paid" to employees who don't actually exist, or illegal funds are used to pay parts of the salaries of employees. Fictitious loans are advanced to launderers who "repay" them using their illegal funds. Each of these mechanisms is facilitated by moving the associated transactions online, which further disguises the identities of the beneficiaries.[24]

Open a bank account for this shell company and you don't even need to render service but rather use this shell company to make it appear that the services are being provided in return

[23] See the definition given by the Supreme Court of India in Vodafone International Holdings B.V. v. Union of India, (2012) 6 SCC 369, ¶105.

[24] Kim-Kwang Raymond Choo and Russell G. Smith, Criminal Exploitation of Online Systems by Organised Crime Groups, Asian journal of criminology 3(1) 37-59, 46 (2008).

of payment of funds that have passed through layering process. This way the wealth of the owner looks legitimate which can be said as the profit of the service provider.[25]

- **Bank capture:**
  In this, launderer buys a controlling interest in a bank and uses it at his whim mainly for the purpose converting illicit money into legal money. The advent of online banks and payment portals, like PayPal and DigiCash mean that such a mechanism can easily be moved online. Recent cases involving PayPal will be discussed later in this paper.
- **Real estate and online auctions:**
  With advent of online property portal like, MagicBricks27, 99 Acres[26] etc., money laundering through purchase of real estate has now moved online. Online auctions are another mechanism, by creating fake auctions, or grossly overstating the price or worth of goods.

MODERN APPROACH-

- **Online games:**

Online games are arguably the most notorious space for money laundering online that is available today as they provide nearly a fool proof way to disguise and move money across the jurisdictions. Multiplayer online role-playing games, called Massive Multi-player Online Role Playing Games (MMORPG), like Linden Lab's "Second Life" and Blizzard Entertainment's ―World of Warcraft, are some of the examples for it. Most of these games have various opportunities for money based transactions, such as buying of virtual property, or gaming props etc. For instance, Second Life, which has approximately 21.3 million account holders globally, uses a virtual currency called ―Linden dollars‖ for its transactions. Although the exchange rate fluctuates, on average, approximately 100 Linden dollars is equivalent to 1 US$. The virtual account is tied up to an actual bank account, and the daily turnover generated by the game is estimated at almost 1.5 million US$. Earlier, digital earnings had to be converted into real currency directly through the use of virtual currency arbitrage trading websites, which was at least a small opportunity for regulators to keep an eye on transactions. But in May 2006 Entropia Universe introduced real world ATM cards to

[25] Mohammad Salman Jamali, Cyber Laundering,
[26] See http://www.magicbricks.com/; http://www.99acres.com/

its 250,000 players, allowing them to instantly withdraw hard cash from their virtual world assets. This was followed by other game developers and now the entire process is wholly outside the ambit of authorities.[27] Enforcement agencies find it difficult to take actions against such practices because-

a. The transactions in the games involve small amounts that are hard to detect as they are funnelled in to a master account held by the launderer;
b. The digital transfer taking place need not be reported to any regulatory agency;
c. Jurisdiction of investigation, prosecution and enforcement authorities.[28]

- **Online Banking:**

Online banking has created threat of cyber laundering for Online Banks in two ways-

1) Account holder may be carrying out the process of Cyber laundering through a phenomenon called 'smurfing'.
2) Enabling people to open accounts in online banks without verifying the identities of their customers creates a greater threat which is exploited by criminals in hiding their real identities.

Online banking is regulated by the policies of the banking regulations that require knowing your customer and their business. In case of any suspicious transaction, banks are required to report it to the law enforcement agencies. The criminals can easily avoid such restrictions by opening online accounts with so many unregulated electronic banking companies that use electronic payment systems to provide online banking like functionalities with the added layer of hidden transaction. Prepaid cards provide anonymity feature which gives the criminal and edge over the physical banking systems as anonymity feature of the card helps in the layering and integrity stage of Cyber laundering.

Lack of international standard of regulation makes it difficult to regulate online banks accounts. A lot of the countries are still not cooperating with the international treaty to share

[27] Angela Irwin & Jill Slay, Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft, International Cyber Resilience Conference (2010), available at http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1004&context=icr (Accessed: April 2, 2016)
[28] Wendy J. Weimer, Cyberlaundering: An International Cache for Microchip Money, 13 DePaul Bus. L.J. 199, 220 (2001)

intelligence and suspicious transaction records with the member countries to monitor and control Cyber laundering.[29]

Recent examples of Cyber Laundering:

- **HSBC Case (2012)**

This is a famous case of cyber laundering with PayPal and HSBC bank. In this case launderers created a set up through which up to $800 million were laundered using PayPal to deposit money into HSBC. The key here was that the money launderers had a man on the inside at HSBC opening multiple fraudulent accounts and allowing large transfers without triggering AML investigations.

A normal person depositing more than $10,000 in cash into a bank account in person has to fill out official suspicious activity reports, but a corporate account in which tens or hundreds of thousands of dollars are flowing through the account monthly avoids scrutiny as long as the bank officer establishing and managing the account within the bank reports the transactions as normal for the business involved. Now, the man on the inside of HSBC opened several corporate banking accounts for various companies. He then made some prototypic arrangements to check the working of the process set by the launderers. In the beginning, small amount of $1 were received from PayPal which were then moved on to other accounts, just to see if the process itself works. After a grace period of 60 to 90 days the accounts were off the heightened scrutiny list of newly opened accounts. Then the payments became larger. Initially around $10,000 a piece, and later $200,000 to $300,000, flowing into the HSBC client's corporate account from Paypal, and shortly after that out of the account into other accounts within and outside the bank. Because the HSBC employee involved in the scam was solely responsible for the monitoring and alerting of suspicious transactions, nobody inside or at the regulators knew about the suspicious money flows and payment patterns. There was no automatic pattern recognition software.

PayPal was particularly suited because as a corporation it exists to mask the accounts or credit card facilities from which a person pays into another account. PayPal's stated goal is to protect innocent Internet buyers for identity theft and subsequent credit card fraud. But seen through the eyes of criminal money launders, PayPal provides a convenient service for hiding

[29] *ibid 7*

their identities and masking where suspicious deposit transfers originate. A PayPal transfer to fraudulent account only needs to show up once – the first time the money comes into the bank. After the money is in the bank, the PayPal-derived funds can be transferred into multiple other fraudulent accounts, without PayPal being listed a second time as the source of the funds transfer.

In total, $800 million were laundered through the scheme in six short months. The Whistleblower was fired for "poor job performance," after, he claims, he refused to stop investigating, documenting and reporting suspicious activity he encountered almost daily in doing his job. A penalty of $1.9 billion was imposed on HSBC[30]

COMBATING MONEY AND CYBER LAUNDERING

International Regime

From an international perspective, there are three main institutions that are working to counter the issue of money and cyber laundering, namely, The United Nations, The Finance Action Task Force on Money Laundering and INTERPOL.

The United Nations

In 1998, UN held a special session on drug trafficking. It was then that the issue of money laundering as also identified, as it was one of the sources of finance for drug trafficking. Consequently, a number of conventions were brought into force.

The first is United Nations Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988. Popularly known as the Vienna Convention was the first instrument to recognize the issue of money laundering as a crime. Article 3(v)(b)(i) and Article 3(v)(b)(ii) criminalize the financing of any of the offences covered under the Convention and attempts to disguise the source of funds used for such financing.

Although, this instrument criminalizes money laundering, it has no provisions to combat the issue of cyber laundering.

The next in row is the UN Convention against Transnational Organized Crime, 2000 or the

[30] Viswanatha, A. and Wolf, B. (2012) *HSBC to pay $1.9 billion U.S. Fine in money-laundering case*. Available at: http://www.reuters.com/article/us-hsbc-probe-idUSBRE8BA05M20121211 (Accessed: 3 April 2016).

Palermo Convention. While the Vienna Convention dealt with money laundering related to drug trafficking, the Palermo Convention broadened the scope of the same by applying it to the proceeds of all serious crimes. Article 6 criminalizes the laundering of proceeds of crime by requiring State parties to adopt legislative and other measures against conversion or transfer of property', knowing that such property is the proceeds of a crime, for the purpose of concealing or disguising the illicit origin of such property. Another interesting provision is Article 19 of the Convention, which provides for joint investigation by States for cross border offences. This provision is of significance in the context of cyber laundering, which always has an international element.

The third in row is the United Nations Convention Against Corruption, 2003. Article 23 of the Convention deals with the laundering of the proceeds of an act of corruption. Article 24 criminalizes "concealment" of property when then person involved knows that such property is the result of any of the offences under the UNCOC. Article 27 criminalizes the participation and attempt to launder money as well, while Article 28 clarifies that knowledge, intent or purpose, established from objective circumstances is required to prove the offence.

The UNCOC also has a specific provision covering cyber laundering. Article 14(3) deals with preventive measures against money laundering and requires financial institutions and money remitters include on forms for the electronic transfer of funds and related messages, certain accurate and meaningful information on the originator, maintain such information throughout the payment chain, and apply enhanced scrutiny to transfers of funds that do not contain complete information on the originator. This provision is an excellent trend to dealing with the problem of cyber laundering.

Apart from these three major conventions, there are a couple of more instruments like the he International Convention for the Suppression of the Financing of Terrorism, 1999 and The Global Programme against Money-Laundering, Proceeds of Crime and the Financing of Terrorism, which is an ongoing program led by the UN Office on Drugs and Crime (UNODC) to assist the member nations to draft legislations, which give effect to the various adopted conventions.

Financial Action Task Force on Money Laundering: or Groupe d'action financiere (French) was established in 1989. It is an intergovernmental organization, which frames policies to combat money laundering. The main objective of the FATF is "the development

of and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing." The FATF's primary policies issued are the Forty Recommendations on money laundering from 1990 and the 9 Special Recommendations (SR) on Terrorism Financing (TF). Together, the Forty Recommendation and Special Recommendations on Terrorism Financing set the international standard for anti-money laundering measures and combating the financing of terrorism and terrorist acts. The 2003 Forty Recommendations require states, among other things, to:

1. Implement relevant international conventions
2. Criminalise money laundering and enable authorities to confiscate the proceeds of money laundering
3. Implement customer due diligence (e.g., identity verification), record keeping and suspicious transaction reporting requirements for financial institutions and designated non-financial businesses and professions
4. Establish a financial intelligence unit to receive and disseminate suspicious transaction reports, and
5. Cooperate internationally in investigating and prosecuting money laundering

In 2012 February, the SR VIII or Recommendation 8 was introduced by FATF, which includes new rules on wire transfers. The FATF, hence, has proved to be the most competent organization, which deals with the issue of cyber and money laundering.

INTERPOL: INTERPOL has been working to combat money laundering through the global exchange of data, supporting operations in the field, and bringing together experts from the variety of sectors concerned. The INTERPOL General Assembly has passed a number of resolutions calling on member countries to concentrate their investigative resources in identifying, tracing and seizing the assets of criminal enterprises.

These resolutions have called on member countries to increase the exchange of information in this field and encourage governments to adopt laws and regulations that would allow access, by police, to the financial records of criminal organizations and confiscation of proceeds gained by criminal activity.[31]

[31] 2016, I. (2016) *Money laundering / financial crime / crime areas / Internet / home*. Available at: http://www.interpol.int/Crime-areas/Financial-crime/Money-laundering (Accessed: 8 April 2016)

The resolutions passed by INTERPOL, however, are specifically targeted to deal with traditional money laundering and do not contain any specific provisions related to cyber laundering.

National Regime

In India, the legislation to combat money laundering is **Prevention of Money Laundering Act, 2002 (PMLA).** The central objective of the Act was to provide for confiscation of property derived from, or involved in, money laundering. However, after the amendment in 2012, its scope has been widened to some extent. The term 'cyber laundering' is not defined or specified under the Act. However, going by the judicial definition of money laundering as held in the case of **Hari Narayan Rai** v. **Union of India** as "any process or activity by which the illicit money is being projected as untainted."; the term 'process' and 'activity' could be widely interpreted to include the acts of cyber laundering as well. This is because the Act is concerned with the penalizing the act and not with the process. The FATF did point out several concerns with the PMLA, when India sought membership initially in 2006, including certain concerns relating to cyber laundering. On the basis of which, certain amendments has been made in the Act in 2012. But still, the Act fails to specifically address the key issue on hand i.e. cyber laundering. This is a major lacuna in the law against cyber laundering in India.

Apart from PMLA, there is Information Technology Act, 2000 (As Amended In 2008) which deals specifically with cyber-crimes. However, there is no specific provision in the Act which deals with the offence of cyber laundering. Also, the existing provisions of the Act are insufficient to prosecute a launderer under the IT Act based on even a wide interpretation.

One thing positive about the Act is that it applies to and recognizes the cross-border nature of offences. The words "computer" and "computer system", in Section 2(i) and 2(l) respectively, have been also widely defined to include all electronic devices with data processing capability.

Section 43 deals with the civil offence of theft of data and damage to computers, computer system. There is no real scope to seek damages for cyber laundering activities under this section. Section 43-A is a more relevant provision, making a body corporate that is negligent in implementing reasonable security practices and thereby causes wrongful loss or gain to any person, liable to pay damages by way of compensation to the person so affected. The practices extend to protection of "sensitive data", which includes password, details of bank

accounts or card details, medical records etc. Under the Rules[32], in the event of an information security breach, the body corporate shall be required to demonstrate that they have implemented security control measures as per the documented information security program. These provisions and Rules thus cover civil liability and corporate responsibility.

The cyber-crimes covered under the Act are quite limited. Section 65 criminalizes tampering with source documents. Section 66 covers several computer related offences, including criminal liability for data theft covered under Section 43, when done dishonestly and fraudulently. The other offences covered from Section 66A to Section 66F, introduced by the Amendment in 2008, are sending offensive messages, dishonestly receiving stolen computer resource, electronic signature or other identity theft, cheating by impersonation using a computer resource, violations of privacy and cyber terrorism respectively. All these offences are cognizable and non-bailable.

Thus, it can be seen that no law provides specific and exhaustive provision in this regard. Apart from this legislation, there are few regulations of some statutory bodies as well. They are as follows-

- **RBI's Know-Your-Customer Guidelines:**
  It was introduced by The RBI applicable to banks in India to reduce financial frauds and identify money-laundering transactions.
- **IRDA:**
  It issued anti-money laundering guidelines applicable to insurers. Insurers are also required to maintain records of their transactions under these guidelines.
- **SEBI[33]:**
  It has issued a circular with guidelines for Intermediaries in the securities markets. The guidelines include due diligence measures (Guideline 4.1), and a detailed Know-Your-Client procedure (Guideline 5.3), with special attention to be given to all complex, unusually large transactions or patterns of transactions which appear to have no economic purpose.

[32] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

[33] Securities and Exchange Board of India, Master Circular on Anti Money Laundering (AML) Standards/Combating Financing of Terrorism (CFT) Obligations, ISD/AML/CIR-1/2008, December 19, 2008.

TUSSLE BETWEEN RIGHT TO FINANCIAL PRIVACY AND COMBATING MECHANISM

Along with the immediate need to take action against the problem of money laundering in cyber space, it is also necessary to contemplate the effects of doing so. Since the internet offers anonymity and financial privacy, any changes made in the Indian law in this regard will, directly or indirectly, affect the right of financial privacy of citizens. Thus, it would be a tough task to make a balance between the concerns of the financial privacy on the one hand and combating mechanism on the other.

PRIVACY AS REGARDS 'CORRESPONDENCE

The right to privacy has been recognized as an extension of the Right to Life, guaranteed under Article 21 of the Constitution.[34] However, data privacy as such was not discussed in these cases.

The Universal Declaration of Human Rights, Article 12, lays down that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence..." Similarly, terms are found in Article 17 of the International Covenant on Civil and Political Rights, to which India is a signatory. The focus, for the present purpose of regulations against cyber laundering, is on the term "correspondence". The European Convention on Human Rights also stresses that "everyone has the right to respect for his private and family life, his home and his correspondence." It goes on to prohibit interference by a public authority "except such as is in accordance with law and is necessary in a democratic society in the interests of national security....or the economic wellbeing of the country". While the ECHR does not bind India, the approach taken therein as regards restrictions in the interest of "economic well-being" is relevant to cyber laundering. Nevertheless, it is submitted the privacy rights as regards "correspondence" do not and should not be extended to financial transactions or the documents used to execute such transactions.[35]

FINANCIAL PRIVACY

[34] *Kharak Singh* v. *State of U.P.,* AIR 1963 SC 1295; *R. Rajagopal* v. *State of Tamil Nadu*, (1994) 6 SCC 632

[35] Jagdish Menzes, Cyber Laundering: The new Internet Crimes, available at- http://thegiga.in/LinkClick.aspx?fileticket=xpxlb4qgFTw%3D&tabid=589, accessed 4th April, 2016

Financial privacy specifically refers to an evolving relationship between technology and the legal right to, or at least, the public expectation of privacy of one's financial data.[36] This right has not specifically been declared to be part of the right to privacy in India. The IT Act has substantial emphasis on data privacy and information security, but Section 69 empowers the Government or certain agencies, to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, subject to compliance with the procedure laid down. It may be exercised for security of the state and preventing incitement to the commission of any cognizable offence, both of which may be read broadly to encompass cyber laundering and terrorist financing using the internet.

The issue, with respect to India, was decided recently by the Supreme Court in the Black Money case i.e. **Ram Jethmalani** v**. Union of India**[37] wherein the court held, revelation of a person's bank account details, without establishing prima facie grounds of illegality violates their rights to privacy. The State could not compel citizens to reveal details of their bank accounts to the public at large, unless it had properly conducted investigations, to show wrongdoing. Thus, the Court recognized a limited right of financial privacy, which would protect transactions, unless laundering was established prima facie.

CONCLUSION AND SUGGESTIONS

We cannot deny that man, by nature, is ambitious. In this materialistic world, ambition ultimately means money. Sometimes, the greed overpowers everything else and then man forgets about what is right and what is wrong. For a few, money is necessary, regardless of how it is earned.

Thankfully, the government keeps a check on it. But the criminals have found ways to retain and use such illegally and illicitly earned money. Popularly known as black money, this dirty wealth is a threat to the financial system of various countries, including India. Therefore, to keep a check on the same, all fiscal transactions are monitored. The criminals have taken shelter of money laundering to make the illegal money appear as if it has been acquired through legitimate sources.

The process of money laundering involves three stages. The money is first introduced in the system, and then it goes through various channels and transactions to hide the source. And

[36] Benjamin E. Robinson, Financial Privacy & Electronic Commerce: Who's in my business 1-2 (2000)
[37] (2011) 8 SCC 1

finally, the money is returned back to the person introducing it. When reintegrated, the money appears to be clean. Time and again several international and national organizations, through conventions and legislation, have tried the address the issue of money laundering as it posed severe threat to the economies.

With the advancement of technology, the methods and modes of commitment of crimes have also advanced. Money laundering is done over cyberspace and using internet. The procedure and stages remain the same, only the interface differs. Transactions are done online, without any physical interaction. Accounts can be created and deleted. Hence, this method not only is quick and easy to operate, but also secures identity of the criminals.

It will have to be admitted that when it comes to cyber laundering, the remedies fall short. This is maybe because the transactions are too complex to decipher and too quick to trace that issue has not been addressed to adequately.

However, the treat of cyber laundering is real and the problem has to be combated at the earliest. Therefore, we put forth the following suggestions:

- All institutions involved in preventing and combating money laundering and terrorist financing, especially supervisory and law enforcement bodies, urgently need to strengthen their IT knowledge to keep up pace with criminals across the world. This includes increased training and, if needed, the hiring of former hackers,
- Criminals and terrorists can often operate largely anonymously due to lax enforcement of due diligence, in particular in areas outside the financial industry. We therefore have to introduce better ID checks with new financial instruments (e.g. prepaid storage cards), especially outside the financial sector. This could help reduce the use of anonymous payments.
- Cyber-savvy users can relatively easily avoid the tracking of their online identity by using proxy servers and software that trace anonymity. Although a certain degree of online anonymity is acceptable, especially in politically delicate regions of the world, financial operations should never be conducted anonymously. We therefore need better IP tracking to prevent criminals from hiding their online identities.
- Criminals can easily exploit the lack in international co-operation by moving from country to country. We therefore need much better international co-operation and co-ordination to prevent and combat money laundering and terrorist financing. We have

to strengthen national and international efforts and instruments aimed at combating online money laundering and terrorist financing, for example by allowing for faster exchange of information and speeding up requests for mutual legal assistance.

- Additionally, as banks play a crucial role in the process of laundering, it is important that they make schemes to implement the following:

1. Making effective provisions for determining the true identity and beneficial ownership of accounts
2. Understanding and tracing sources of funds
3. Understanding the nature of the customers' business
4. Understanding reasonable account activity

The crime of laundering is committed on various levels and hence, there should be a check on every level. It is a little difficult, but not at all impossible to combat the issue. The "objective" aspect of laundering has been covered under PMLA. However, cyber laundering should be made a specific offence under IT Act so as to make have a proper "mechanism" to combat the same. Therefore, we propose an amendment to the IT Act (by adding of Section 66G) wherein whoever commits intentionally, by use of a computer, computer system or communication device, any transfer or acquire any property or tries to disguise/conceal the true nature or source of such property is made guilty of the offence of cyber laundering and shall be punished in accordance with provisions of IT Act and Prevention of Money Laundering Act, 2000.