Economics and Management
ISSN: 2367-7600; 1312-594X
Volume: XVII, Issue: 1, Year: 2020, pp. 81-88

CYBERCRIME AND MONEY LAUNDERING IN 21ST CENTURY

Aleksandra Stankovska[1], Elizabeta Stamevska[2]

Received: 31.03.2020 Accepted: 15.04.2020

Abstract

This paper focuses on cybercrime and money laundering. Proceeds of these activities may be used to fund further criminal activities and to undermine the integrity of financial systems worldwide. Money laundering is the biggest method followed by the cyber criminals to hide their black money which they get themselves courtesy to financial frauds they involve into.

Money laundering is the process of making large amounts of money generated by a criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. The money from the criminal activity is considered dirty, and the process "launders" it to make it look clean.Unlike the "traditional" money laundering methods, which rely on the banking system, cyber-laundering depends on the use of various types of transactions and financial services providers, ranging from wire transfers, cash deposits/withdrawals and e-money transactions to "money mules" and remittance services.

Keywords: *cybercrime, money laundering, cyberlaundaring, financial service providers & wire transfer.*

JEL Codes: *G21*

1. Introduction

In today's word moneys are not generally in hand cash, but rather the electronic media we use to keep or transfer money. Thus laundering in such regard is considered as cyberlaundering. It helps in illegally acquire or transfer money.

According to Ibish &Nedelkovska (2018,p.136), in the unconventional types of crime (the modern types), especially the computer crime and the abuse of transactions, the main problem is the evidence as a main thing for detecting the offender and the crime. Most offenders are educated hackers and, by using special computer programs, the hacker accesses the victim's personal data and, by their abuse, transfers the funds from the victim's transaction to their transaction; in these situations, the only evidence is the

[1]European University, Skopje, Faculty of Economics, Full Time Professor, PhD, aleksandra.stankovska@eurm.edu.mk
[2]European University, Skopje, Faculty of Economics, Associate Professor, PhD, elizabeta.stamevska@eurm.edu.mk

network and ICT (Information Communicatin Technology). These evidences are located in the cyberspace.

Organizations are now faced with a challenge of integrating cyber incidents into their anti-money laundering (AML) programs. While cybersecurity is an extremely complex issue, the AML portion can be distilled down to a much leaner process. The first step in building a cyber-program is to identify all relevant stakeholders within the organization. At minimum, this should include personnel from the AML, fraud, and information technology (IT) or information security (IS) teams. Outside of these core functions, key lines of business may be of assistance as well.

Cyberlaundering refers to the way in which the mechanism of the internet is used to launder illegal proceeds of crime in order to make such proceeds appear clean. n principle, cyber-laundering is the same as the conventional money laundering practice which consists of three stages:

- Placement, placing dirty money into a legal financial system.

- Layering, transferring or changing the form of money through complex transactions to obscure the origin of funds.

- Integration, returning money that has been 'laundered'. The anonymity and convenience of the internet and other Information and communications technologies (ICT) allow cybercriminals to target victims globally, raising cross-jurisdictional considerations and complicating investigations.

Cyberlaundering is basically committed in 3 steps: Placement of funds, i.e. when illicit money is put into a financial institution, funds are stolen online through digital transactions; Layering, i.e. moving funds inside the financial system and into unregulated financial e-cash systems; Integration, i.e. removing funds all together from the financial system.

As cyber-attacks increase worldwide, financial institutions are working to integrate their compliance department with the Information Management and Information Security ("IM/IT") department. Innovation in cyber security is crucial in levelling the playing field in the fight against cybercrime. Improved visibility is important because it enables organizations to remove unnecessary network and access privileges, track data movements, limit what applications can run on particular computing assets and reduce how much control users have over their systems and their ability to install malicious software inadvertently.

2. Literature

There are a lot of Literatures about cybercrime, money laundering & cyber - laundaringincluding academic studies and empirical studies. The term "money laundering" started to draw attention in the early nineties and it has been defined in different ways. Regardless of definitions, the core meaning of the term is the process of

turning illegally gained money into legal and lawful money with the purposes to disguise original source of criminal or illegal money. Money laundering is the attempt to conceal or disguise the nature, location, source, ownership or control of illegally obtained money. Money laundering is illegal. Boskovic, G. (2003), "Types of money laundering and suppression methods. MA Thesis, Police Academy, Belgrade, p. 31" has concluded that while money laundering methods vary in national and international framework, contemporary tendencies in money laundering include abuse of money deposit cards,use of Internet banking, abuse of electronic cash, abuse of securities, international trade abuse etc. EAG (2013) "Typology Report on Money Laundering Through the Securities Markets" has recommended inter alia that jurisdictions that have not designated securities market offences viz., insider trading, market manipulation and securities-related fraud as ML/TF offences may make the necessary changes in their laws to include the same.

According to Shinder (2011) manylaws have been passed to deal with any type of cybercrime. Although these laws didn't exists many years ago government officials, today they are written and made for cyber criminals. According to Stephen Jeffrey Weaver (2005), cyber-laundering may be defined as the use of internet-based electronic wire transfer methods in order disguise the source of the illicit funds. This type of crime occurs because of the emergence of electronic money66 which has diverged into various systems of global payment networks and the internet. These include electronic payment system, wire transfer system, or internet banking.

3. Methodology

In the research and development of this paper a combination of qualitative and quantitative methodology has been implemented. To achieve the object of this paper, the cybercrime & money laundering data has been collected. The research is based on accessible data from papers, journals, various reports, etc.

4. Analysis and discussion

Cybercrime is criminal activity or a crime that involves the Internet, a computer system or computer technology; identity theft, Phishing and other kinds of cybercrime. In practice, two categories of cybercrime exist:

- The computer as target (using a computer to attacks other computer, e.g. Hacking, virus/worms attacks, Dos attack etc;
- The computer as a weapon (using a computer to commit real world crime e.g. cyber terrorism, credit card fraud and pornography etc.

Types of cybercrime: hacking, cyber terrorism, information theft, phishing, software piracy and virus dissemination. Cyber criminals are using a combination of new cryptocurrencies, gaming currencies and micro-payments to launder up to $200bn in ill-gotten gains. Cyber criminals are responsible for up to 10% of the total illegal profits being

laundered globally, which UN figures indicate equates to about $200bn a year. To achieve this, they are using a combination of crypto-currencies such as Monero, gaming currencies and micropayments, according to a study commissioned by virtualisation-based security.

In the initial - or placement - stage of money laundering, the launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

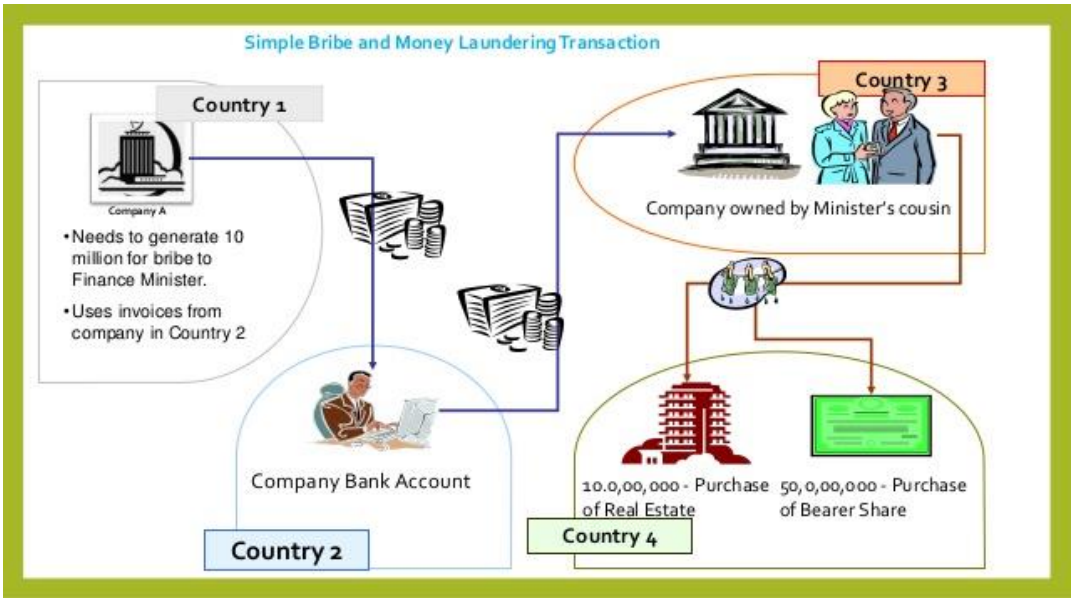
Having successfully processed his criminal profits through the first two phases the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

Figure 1 Money Laundering Cycle

Covert data collection indicate that about 10% of cyber criminals are using PayPal to launder money. A further 35% use other digital payment systems, including Skrill, Dwoll,

Zoom and mobile payment systems such as M-Pesa. Methods such as “micro laundering”, where thousands of small electronic payments are made through platforms such as PayPal to avoid triggering alerts, are increasingly common and more difficult to detect. Another common technique is to use online transactions via sites such as eBay to facilitate the laundering.

Figure 2 Money Laundaring Transaction



Around $2 trillion is laundered every year and everyone is paying the price. Banks have huge regulatory overheads. Businesses and consumers encounter friction to open a bank account, transfer funds or instruct a lawyer. The best companies manage risk best.

The deeper "dirty money" gets into the international banking system, the more difficult it is to identify its origin. Because of the clandestine nature of money-laundering, it is difficult to estimate the total amount of money that goes through the laundry cycle.

The estimated amount of money laundered globally in one year is 2 - 5% of global GDP, or $800 billion - $2 trillion in current US dollars. Though the margin between those figures is huge, even the lower estimate underlines the seriousness of the problem governments have pledged to address.

Many countries’ governments are trying hard to implement rules and regulations to counter cyberlaundering. Steps like putting a limit to store value card is proposed by American government’s financial intelligence unit. Points like if all the transactions in a system can be logged at a central point has also been raised. It helps the investigators to reconstruct an electronic audit trail. However, determining the jurisdiction in

cyberlaundering cases is difficult. It has also been discussed to attach unique electronic serial numbers to transactions to prevent criminals for adopting cyberlaundering techniques.

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLR 2019 came into force on 10 January 2020. These regulations implement the EU Fifth Money Laundering Directive (Directive (EU) 2018/843, '5MLD')) in the UK, and follow a high-level consultation in summer 2019. There was no opportunity to consult on the regulations which were laid before Parliament on 20 December 2019.

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLR 2019 came into force on 10 January 2020. These regulations implement the EU Fifth Money Laundering Directive (Directive (EU) 2018/843, '5MLD')) in the UK, and follow a high-level consultation in summer 2019. There was no opportunity to consult on the regulations which were laid before Parliament on 20 December 2019.

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLR 2019 came into force on 10 January 2020. These regulations implement the EU Fifth Money Laundering Directive (Directive (EU) 2018/843, '5MLD')) in the UK, and follow a high-level consultation in summer 2019. There was no opportunity to consult on the regulations which were laid before Parliament on 20 December 2019.

Under the MLR 2019, the scope of persons and firms subject to MLR 2017 has expanded to include:

- Tax advisers – now includes those who provide 'material aid, or assistance or advice, in connection with the tax affairs of other persons, whether provided directly or through a third party'. Instead of 'advice about the tax affairs of other persons'.

- Lettings agents – this includes persons acting on behalf of either landlords or tenants, but only where agreements are concluded for the letting of land (including buildings) for a term of a month or more and a monthly rent (at any point during the term) of €10,000 or more. Certain exclusions apply, for example in respect of businesses which only publish lettings advertisements.

- Art market participants – this comprises (a) persons who by way of business trade in, or act as intermediaries in, the sale or purchase of works of art in respect of trasnactions amounting to €10,000 or more, and (b) the operators of freeports, who store works of art worth €10,000 or more in the freeport.

- Cryptoasset exchange providers – this comprises persons who, by way of business, exchange, or make arrangements to exchange, cryptoassets for money, money for crypto-assets, or one cryptoasset for another, and persons who operate machines which use automated processes to exchange cryptoassets for money (or vice versa). As foreshadowed in the Government consultation, and in line with the FATF Recommendations, this 'gold-plates' the requirements of 5MLD, which focus on fiat-virtual currency exchangers and do not cover virtual-virtual currency exchangers.

- Custodian wallet providers – this comprises persons who, by way of business, provide services on behalf of customers to safeguard, or safeguard and administer, either private cryptographic keys (in order to hold, store and transfer cryptoassets) or cryptoassets.

With cybercrime estimated to cost the global economy $445 billion a year (McAfee 2014), it is now on par with the global drug trade.I n 2015, the Bitlicense was the first bill to be passed in the US that contained considerations of both AML and cyber security Some cryptocurrencies such as Bitcoin have played a major role in the proliferation of online money laundering as it possesses characteristics that criminals are fond of. Bitcoin and other cryptocurrencies are decentralised, anonymous/pseudonymous and irreversible. They provide the means to skirt the Anti-Money laundering safeguards that have been put in place.

5. Conclusion

The future of cyber security and anti money laundering need to be imagined together. With increasingly similar objectives, threat actors and challenges; the industries have much to learn from each other. Both industries face the challenge to continue being effective and yet minimize the amount of information they harvest from regular citizens. Despite being a medium to exchange information in real-time and with scale, the Internet is being misused in several ways.

Among the slew of financial crimes facilitated by the Internet, money laundering draws importance due to its gigantic size and the diverse methods used online to legitimize ill-gotten profits. The criminal practice of money laundering carried out in cyberspace through online transactions has been termed as cyber-laundering. Money launderers are constantly looking for new ways to avoid detection from law enforcement, and the Internet has opened a large window of opportunities for them.

REFERENCE

Nedelkovska, V..Ibish, E., (2018) Banking Management and Economic Crime of Data Abuse, Economics and Management ISSN: 2367-7600; 1312-594X Volume: XV, Issue: 2, Year: 2018, pp. 134-137

https://www.unodc.org/documents/southeastasiaandpacific/2009/02/TOCAMLO/07-CHAPTER_II.pdf

https://www.ifa.org.uk/technical-resources/aml/whistleblowing/money-laundering-regulations-2019

https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014_English.pdf

https://medium.com/@jony_levin/is-anti-money-laundering-and-cyber-security-that-different-these-days-49db609a0aab

https://www.cybersecurityintelligence.com/blog/cyber-criminals-have-ingenious-money-laundering-methods-3280.html

https://www.unodc.org/unodc/en/money-laundering/globalization.html

http://documents.worldbank.org/curated/en/962591468313816602/Money-laundering-in-cyberspace