ITHEA® Doctoral Consortium

DO TRENDY TECHNOLOGIES FACILITATE MONEY LAUNDERING

Aleksandre Mikeladze

***Abstract**: Information technologies community includes the use of computers, specialized gadgets and different equipment. The spread of the PC and IT interconnected national economies. Trendy technologies give anonymity to an increasing number of individuals tempted by an opportunity to turn into wealthy in a very fast manner. The net gains popularity for obvious reasons - a user is capable of accessing large volumes of data, quickly share information with different users and exchange transactions in any place or time. That is why people would also ask: do trendy technologies facilitate money laundering. The given article mainly focuses on the modern technologies facilitating money laundering crime. It offers an insight on the scheme of how advanced computer users transfer finances using digital tools, avoid attention from the enforcement bodies, and ultimately withdraw the laundered money. In the end of the article, a reader will find some recommendations for the detection of money laundering.*

***Keywords**: Cybercrime, Money Laundering, Modern Technologies, Legislation*

***ITHEA Keywords**: H. Information Systems, H.0 General, H.2 Database Management*

Introduction

Illicit cash flows has become a cross cutting issue on the international agenda in recent years. This term refers to money illegally earned, transferred or used. Digital technologies facilitate illicit money flows at each stage of money laundering remodeling illicit funds to legal. There are several areas wherever clear links between technology and illicit cash flows is also established.

Money laundering is the disguising of the origin of lawlessly gained funds to form them and seem legitimate. Hiding legitimately acquired cash to avoid taxation conjointly is qualified as money laundering. Money laundering is related to nearly all types of crime for profit, including organized and white-collar crimes, like the real estate fraud, savings and loan abuses.

There are three main stages in money laundering:

1. "Placement, the process of placing, through deposits, wire transfers, or other means, unlawful proceeds into financial institutions;
2. Layering, the process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions;
3. Integration, the process of using an apparently legitimate transaction to disguise the illicit proceeds. Through this process the criminal tries to transform the monetary proceeds derived from illicit activities into funds with an apparently legal source" [U.S. Department of State, 2018].

Information and communication technologies created new and expedited traditional ways for earning and laundering money. The development of the digital economy dramatically modified the criminal landscape and therefore the motivation of offenders, transforming connected crime into a complex criminal business. There are not any reliable estimates on the criminal profits and therefore the reputational losses. "The uncertainty about crime profits and losses for businesses, however, does not mean that there is no general understanding that the aggregated criminal profits and direct and indirect losses for businesses are very high" [Tropina, 2016].

Money Laundering and the Digital Age

The main targets of criminals are developing countries that heavily rely on information technologies. Numerous criminal activities are developed and are unendingly improved with an aim to extend the value of services. Technological development and innovation have driven the globalization of the legal sectors and affected business structures, creating them a lot of decentralized. The vulnerabilities of software package and systems are exploited to form so-called crime ware, that is, malware developed with the intention of making a profit and which might cause damage to the user's financial well-being. Crime ware offers cybercriminals the pliability to steal and control information, produce and manage malicious programs, and run networks of interconnected computers infected with malware. "Cybercrime is not going to go away – especially when there are unsuspecting victims to exploit" [Cox, 2017].

Cyberspace and digital technologies are brand new tools for facilitating the criminal business of traditional mafia-style social group teams. Under the overall assumption, traditional organized crime always searches for safe havens with weak government and unstable political regimes. Cyberspace, with its namelessness, absence of borders, constitutes an ideal atmosphere, particularly, criminals will operate from countries that do not have proper legal frameworks or technical capabilities for digital investigations. The trade of crime ware tools for law breaking exists with the trade of ill-gotten product and very different services related to offline crimes. Crime teams had started using digital technologies

to facilitate illegal operations. In addition, it is unclear to what extent digital technologies will facilitate illegal attempts to evade tax payments making it exhausting to assume that the development of world communication has no effect on tax evasion. The global digital economy create loopholes within the taxation frameworks and blur the road between illegal evasions. The most challenges are the globalization of the economy, the chance that digital technology makes it easier for corporations to supply services without a physical presence and to appear for the most effective place for establishing their headquarters and moving their profits. Money laundering has been influenced by the development of knowledge and communication networks. Digital technologies give varied opportunities to facilitate illegal money transfer. The foremost recent trends in hiding involves digital currency, as there are opportunities to exchange real money for on-line cash. Some virtual currencies are very anonymous and cannot be tied to a selected person or entity. There is an area for virtual world that use or give on-line currency that alter on-line games to perform unregulated channels for money launderers. Concealing through on-line games has gone neglected by social control for some time because it absolutely was appeared to be sophisticated. These on-line games and other ways are going to be discouraging. "Cybercrime is becoming a global plague - new technologies provide anonymity to criminals and an increasing number of people lured by a chance of becoming rich in a quick and easy way are getting engaged in this type of criminal activity" [Eurasian Group on Combating Laundering, 2014].

Money generated in massive volume by banned activities should be laundered, before it will be freely spent or endowed. Transferring funds by electronic messages between banks - wire transfer - is a technique to move banned profits and at a similar time begin to launder the funds by confusing the audit path. The identification of the illicit transfers may reveal unexpected criminal operations by providing proof of the flow of illegal profits. It looks not possible to observe or screen wire transfers as they occur, due to the outstanding volume of transactions and since most wire, transfers flow through totally automatic systems with very little or no human intervention. Initially, the matter of money laundering with the utilization of digital technologies was largely connected to the underground economy of crime. The payment systems are getting complicated and criminals will fancy the opportunities of digital technologies that transfer any kind of illicit funds. Criminals will use totally different techniques and ways to gain illegal profits, tools to distance this capital from illegal activity and any cash.

The distinction between on-line and offline criminal activity is money gained from crime typically existing in computer network and must be transferred into money and distanced from its supply, so the placement stage of cash laundering would be missing. However, this may conjointly happen with the illegal trade of products on-line in digital currencies; cash during this case is prelaundered because it is placed in an unregulated institution. "…ever since they noticed that Bitcoin was large enough to pose a risk of money laundering" [Narayanan, 2015].

Digital technologies have variety of distinctive options that create them a game changer for money laundering, e.g. automation, speed, and their cross-border nature, anonymity, less or no regulation. There are many tools that are largely connected to hiding in cyberspace: banking product and services, electronic payment systems via nonbank intermediaries, digital currencies that are largely unregulated and might even be decentralized, on-line services and commercialism platforms, on-line gambling and e-commerce. These new tools may be combined with traditional strategies of money laundering, so creating a complex on-line and offline chain of multiple transactions that are arduous to trace and monitor.

Online banking is one amongst the foremost accepted nexuses of technology and cash transfers, each legal and ill gotten. The link additionally represents the affiliation between technology and ill-gotten ways within which banks and their customers are still one amongst the foremost targets for profit-driven criminals. In several cases, inside the starting of the method of ill-gotten transfers, offenders are still keen about the web transfers via regulated money intermediaries. Since regulated money intermediaries perform know-your-customer procedures and enter a relationship with customers before on-line banking may be used, criminals got to use a heap of advanced schemes than merely transferring funds using on-line banking. "The remoteness of these contacts may leave a potential for same to be abused where a launderer has access to various accounts by way of identity fraud or bribery" [McGowan, 2014]. Some studies reveal that money launderers will do many nonsense transactions across numerous bank accounts, followed by a restricted number of money withdrawals.

Mobile banking may be a method of carrying payments via mobile with the employment of various protocols like text or web. Inside the method of mobile banking communication, operators act as money intermediaries for handling the payment between a consumer and business or financial organization. "But while Liberty Reserve and similar currency exchanges are getting a lot of attention these days from regulators and enforcement agencies, another global money-laundering frontier is not: mobile payments. Millions of people now use their mobile phones to do their banking, especially in developing parts of the world, and their numbers are growing daily. And hidden among them are criminals who some experts believe are engaged in just as wide a range of criminal activity as those using Liberty Reserve, albeit on a smaller scale - for now" [Meyer, 2018]. The most driver for the evolvement of mobile banking is that the growing demand for micropayments, particularly in developing countries. The most vulnerability related to the danger of the employment of mobile banking for concealment in several jurisdictions is that the chance of shopping for a pay-as-you-go SIM-card while not registration and a good degree of anonymity, from that cash launderers will profit. The potential scope of using mobile banking for misbr transfers is debatable; because of most of the transfers involve tiny amounts of cash.

Therefore, mobile payments are off-times named in several studies together of the attainable sources of digital money laundering.

Online nonbank payment services give a cheap, fast and anonymous way to create international cash transfers. In distinction to regulated financial institutions like banks, these intermediaries do not appear to be subject to anti-money laundering obligations and so do not have to be compelled to perform checks on their customers. Some countries even started taking actions toward the mentioned problem. "At the end of December 2015, the People's Bank of China (PBOC), the central bank and national financial regulator, issued new rules governing online payments for non-banks. Citing concerns about risks due to fraud and money laundering, the PBOC has introduced much stricter rules that have caused concern from some industry experts who claim it will negatively impact payment innovation" [TRULIOO, 2016]. Currently, the foremost important on-line payment service suppliers developed antimoney-laundering policies and try to trace suspicious transactions. Although, there are still several intermediaries who allow criminals to enjoy freedom of cash transfers with no checks. Variety of the services enable peer-to-peer cash transfers, creating observance of suspicious activities more durable and giving a heap of prospects to criminals for money laundering. Criminals will enjoy the chance of aggregating giant sums by transferring little amounts of cash many times while not attracting techniques to observe suspicious behavior, and then move this cash between totally different e-payment suppliers.

Digital currencies represent value exchange systems that operate electronically and build transactions with the currencies that exist on-line, do not seem to be issued by financial institutions and are exempted from regulation. "The statutory review of Australia's AML/CTF regime highlighted some of the benefits and risks associated with the growing use of digital currencies. While digital currencies offer the potential for cheaper, more efficient and faster payments, the associated money laundering and terrorism financing risks are well-documented" [Australian Government, 2016]. These currencies are often changed between account holders or turned into traditional money. They are accessible from any part of the globe and permit creating cash transfers instantly, at low cost and with anonymity, typically exploit no trace nearly. The namelessness of digital currencies and not strict regulation during this field build this kind of payment a gorgeous choice to criminals: the utilization of digital currencies for illegal money has been confirmed by many criminal investigations against currency suppliers moreover because it could be a well-known undeniable fact that digital currencies, like Bitcoin, are used for payments at the net underground markets. Several of these currencies are decentralized and therefore exhausting to regulate. Digital currencies, as the simplest way to transfer cash illegally, is more converted into money or alternative means of traditional payments. Casinos within the offline world are thought of a certain way to launder illegal cash. It is natural, that on-line casinos attracted the eye of enforcement and regulators as an attainable way to use digital technologies for illicit funds transfers.

On-line gambling will permit cash to be distanced from the illicit supply for the criminal enterprise of any size, each by gambling or by establishing a web casino in an offshore jurisdiction.

The internet offers uncounted prospects for commercialism of products or exchanging cash for product marketing them more. These activities will definitely use as a way for laundering illicit profits. Another risk of using the web for illicit transfers is the establishment of an e-commerce company, be it real or pretend, and to supply services or trade goods that are never truly delivered. The landscape of the illicit money flows on the web is complicated and might be attributed to varied on-line activities and distinct areas of regulation. The web itself is already a posh and suburbanized cross-border network, wherever the possibility of tracing and prosecuting crimes needs effort and international cooperation. Tackling the problem of illicit money flows in Internet represents a good challenge for regulators and enforcement agencies due to the complexity and borderless nature of the net environment.

Technologies for Detection Money Laundering

Many of the technologies depend upon techniques developed within the field of computer science. Others involve computer graphics and applied math computing. Wire transfer observation proposals usually involve a mixture of technologies, institutional structures and reportage needs. In addition, "graph database technology therefore has the power to unearth data and connections that can lead investigators directly to money laundering cases from what may initially seem like totally unconnected events. This innate ability is opening up a whole new way of detecting money laundering as it is happening, via real time analysis of data relationships" [Jiang, 2017]. There are very different classes of technologies that will be helpful within the analysis of wire transfers. These technologies are often classified by the task they are designed to accomplish. Technologies for screening wire transfers embody knowledge-based systems and link analysis. Knowledge-based systems mechanically produce inferences concerning wire transfers and completely different data. Effective use of data based systems desires effective information acquisition - the simplest way of constructing profiles of money laundering. Link analysis helps determine relationships among individual accounts, people or organizations.

Some technical selections use a knowledge-based system alone. Others at the beginning screen all wire transfers employing a knowledge-based system and then enable analysts to scrutinize some or all transfers using link analysis. Knowledge-based systems are computer programs that process information in ways that within which emulate human consultants. Information that is embedded within the system is freelance from the reasoning ways that accustomed operate that data. Knowledge-based systems can build a case for the inferences that they have created. Most generally, databases are created by interviewing one or plenty of specialists in area in ways in which are meant to elicit the details of their reasoning processes. Associate analyzing of cases where the right decision is known

creates info bases. Additionally, there is a link associate analysis technique to explore associations among an outsized form of objects of varieties. Inside the case of money laundering, objects may embody folks, bank accounts, businesses, wire transfers or money deposits. Link analysis operates on a bunch of information records, where each record has several fields containing info. Link analyses are utilized in many criminal investigations, furthermore as fraud, and conspiracy cases.

Several business software system packages are typically accustomed to conduct link analyses. Databases are often made in two ways: by interviewing a professional or by analyzing an outsized range of cases. Information engineering attempts to use rules of thumb, utilized by consultants to succeed in conclusions within the relevant domain. Data engineering is tough, because of consultants usually cannot simply articulate their decision-making processes inside the narrow language utilized by knowledge-based systems. Data engineering within the space of wire transfers is just attainable if there are people who know how to screen transfers for proof of money laundering. Data discovery techniques are numerous and many-sided, as well as techniques from statistics and therefore the computer science subfield of machine learning. Researchers have developed many techniques within the past decades for automatically finding patterns in massive amounts of information. In most cases, the information comprises an oversized variety of observations, wherever every observation represents one object, e.g. a person, account, or wire transfer and consists of values for every of many numeric or symbolic variables. Analysis begins by designating one variable, e.g. money laundering because the variable of interest. The rest of the analysis consists from models that commit to predict this variable by using the remaining variables like dollar amount, foreign beneficiary, client kind, etc. Models that correctly predict the variable of interest are maintained and fewer accurate models are discarded. It is not possible to look through all attainable models; therefore, techniques usually limit the amount of models searched by selection altering the foremost accurate models that have already been made. Interest in analysis of enormous databases has grownup hugely within the past years, as major firms have begun to mine massive databases of client info. Cluster analysis is accustomed to determine underlying groupings that do not seem to be otherwise apparent within the information. Analysis may reveal teams of transfers whose originators are extremely similar. In financial information, clusters would possibly reveal similar styles of accounts, individuals or organizations. The currency and wire transactions of producing corporations would possibly cluster closely along compared to different corporations. Insurance companies would possibly resemble one another closely in terms of their money transactions. The clustering would possibly permit investigators to spot producing corporations whose money transactions are atypical and examine them a lot of closely to work out whether or not the corporation is just a shell inside that to hide money laundering. Rather than automating the development of helpful models like machine learning techniques, visualization techniques offer human analysts powerful tools to look at

information - permitting analysts to explore and apply their own data to the information analysis problem. Case-based reasoning techniques place confidence in the storage and process of first cases. These first cases would then be compared to new records supporting to determine what sort of activity they represent. "In particular, we show how case-based reasoning techniques can be extended from the domain of decision support to help analysts retrieve information about previous incidents" [Johnson, 1999].

Money-laundering techniques will change speedily and therefore the profiles in knowledge-based systems meant to observe money laundering would need to change moreover. All banks and wire transfer systems can be needed to use a software package provided by regulative agencies. Knowledge-sharing techniques do not seem to be well developed and are well less mature than alternative techniques. The utilization of data sharing techniques will simply be phased-in over a period, beginning with communication profiles using comparatively customary nomenclature and moving toward electronic dissemination of specially formatted databases. Information transformation is a few of the foremost worrisome and time overwhelming aspects of analyzing financial records that do not forever contain unambiguous indicators. Money launderers will use multiple, shifting account numbers. A blackboard could be a central database wherever multiple problem-solving agents will share connected info of a few particular problem. Agents could also be banks that report wire transfers, typical PC systems, data primarily based systems and human analysts that make aggregate records. The data concerning those cases are often updated and developed by totally different analysts whose solely communication is thru the blackboard. Agents enter reports that are employed by later investigators while not the necessity for direct communication between them even if they are separated in time or geographically. "Analysis at any single level may miss indicators of activity at other levels. Different levels of analysis may be best done in different places. For example, banks are uniquely equipped to detect money laundering at the transaction and individual/account levels. They have access to customer information and account history which can be brought to bear on evaluating suspiciousness. In contrast, FinCEN is uniquely equipped to detect money laundering at the business and ring level. They have aggregated data and additional information from law enforcement and commercial sources that can be brought to bear" [U.S. Congress, 1995].

Conclusion

Cyberspace has become the source of illegal proceeds. An efficient anti-cybercrime strategy consists from a series of legal, technical, organizational and informational activities. The success of any money laundering and crime fighting measures depends on the timely detection of economic transactions probably connected to the laundering of law-breaking takings and therefore the effectiveness of

international cooperation. Digital technologies supply variety of distinctive tools to facilitate illicit money. A mixture of the subsequent tools permits criminals to distance their profits from illegal sources. However, digital technologies are often used as a tool to fight corruption and promote a culture of transparency. To understand their full potential as a transparency and authorization tool, though, digital technology tools ought to be combined with infrastructural, social, and economic changes. The utilization of digital technologies for investigation, interference and detection represents an enormous challenge due to the meddlesomeness of those techniques and therefore the necessity of finding a balance between crime interference and crime management, human rights or privacy issues.

Bibliography

[Narayanan, 2015] Arvind Narayanan, J. B. Bitcoin and Cryptocurrency Technologies. In J. B. Arvind Narayanan, Bitcoin and Cryptocurrency Technologies (p. 160).

[Australian Government, 2016] Australian Government, A.-G. D., Regulating digital currencies under Australia's AML/CTF regime. In A.-G. D. Australian Government, Regulating digital currencies under Australia's AML/CTF regime (pp. 3-4).

[Cox, 2017] Cox, L. Developing Countries – a Hotbed of Cybercrime?

[Eurasian Group on Combating Laundering, 2014] Eurasian Group on Combating Laundering, Cybercrime and Money laundering. In E. G. Laundering, Cybercrime and Money laundering (p. p.3).

[Jiang, 2017] Jiang, J., How to use graph technology to detect money laundering. Retrieved from Neo4j News: https://neo4j.com/news/use-graph-technology-detect-money-laundering/

[Johnson, 1999] Johnson, C. Using Case-Based Reasoning to Support the Indexing and Retrieval of Incident Reports.

[McGowan, 2014] McGowan, P. J., Money Laundering, Terrorist Financing and New Technologies: Potential for Misuse of New Payment Methods in the UK. In P. J. McGowan, Money Laundering, Terrorist Financing and New Technologies: Potential for Misuse of New Payment Methods in the UK (pp. 39-40).

[Meyer, 2018] Meyer, J., Digital Money. Retrieved from Quartz: https://qz.com/94570/how-mobile-payments-might-be-the-global-money-laundering-machine-criminals-have-dreamed-about/

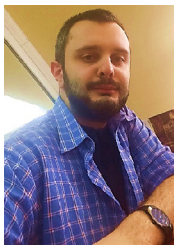
[Tropina, 2016] Tropina, T., Do Digital Technologies Facilitate Illicit Financial Flows? In T. Tropina, Do Digital Technologies Facilitate Illicit Financial Flows? (p. 6).

[TRULIOO, 2016] TRULIOO. Retrieved from TRULIOO: https://www.trulioo.com/blog/how-will-chinas-new-regulations-impact-online-payments/

[U.S. Congress, 1995] U.S. Congress, O. o., Technologies for Detecting Money Laundering. In O. o. U.S. Congress, Technologies for Detecting Money Laundering (pp. 51-71).

[U.S. Department of State, 2018] U.S. Department of State, Retrieved from U.S. Department of State, Diplomacy in Action: https://www.state.gov/j/inl/rls/nrcrpt/2001/rpt/8487.htm

Authors' Information



Aleksandre Mikeladze - *PhD Student of Tbilisi State University, Georgia*

Faculty of Economics and Business Administration

E-mail: lx.mikeladze@gmail.com

Major Fields of Scientific Research*: Computer vision, Money Laundering*