Mircea Constantin ŞCHEAU, PhD Candidate
E-mail: mirceascheau@hotmail.com
"Alexandru Ioan Cuza" Police Academy of Bucharest
Assistant Professor Stefan POP ZAHARIE, PhD
"Dimitrie Cantemir" Christian University

METHODS OF LAUNDERING MONEY RESULTED FROM CYBER-CRIME

Abstract*: Regardless the level they're at and the referenced timeframe, economic exchanges are based on two fundamental elements – demand and supply. The new technologic revolution altered existing parameters, the transfer speed being strongly affected. Economic models unknown at the time were the basis of the development of new applied strategies that proved useful or lead to financial collapse. Liquidity deficits created as a result of wrong interpretations and the involvement of some financial- banking and insurance institutions in market regulation mechanisms spurred the emergence of international entities aimed at recovering and maintaining balance.*

Key words: *globalization, financial transfer, money laundering, cyber-crime, bank.*

JEL Classification : F60, K24, 033

1. Introductory notions

One of the questions experts were asked revolved around the role that these entities have in terms of stabilizing markets in crisis situations while offering support for further development (Cüneyt Dirican, 2016). The International Monetary Fund and European Central Bank are the most eloquent examples in this regard. Regulations and banking system management differ from one country to another. National central banks supervising their functioning apply regulations which may be or may not be in agreement with the current European legislation. Particularities are what set differences. Unlike traditional banks, central banks have the possibility of generating denomination called „emissions" but the impact of developments in digital payment systems and electronic currencies lead to a new paradox that is about to become a global trend. Historically, there have been several similar cases, one of them even sparking controversy regarding the emergence e of the first central banks. The dispute is carried out between supporters of the two ideas. On one side are those who believe that the first central bank was established for the Netherlands in Amsterdam and on the other hand those who argue that it was created in 1668, as the central bank Riksbank in Sweden. Regardless of contradictions on the timing of the event, what's important

is that Riksbank is known as the first issuing bank notes instead of coins, rediscounting claims and bills (http://www.riksbank.se/en/The-Riksbank/Research/Historical-Monetary-Statistics-of-Sweden/).

Central independent banks are ranked according to purpose, type of institution, financial capacity (capital strength and its budget) and the ability of using and controlling financial instruments, their goal being to support ongoing economic objectives. It is true that the appearance and the development of „financial derived instruments" led to the increase of a system of dealers which made possible the strengthening of the banking system, evading international regulations, named in the media as „the shadow banking system" (https://regulation.revues.org/7473?lang=en). Also, operations can sometimes get out of control due to the propensity of the physical/juridical bodies for alternative digital coins for the Gold Standard system, Bretton Wouds or the current International Financial System (defined generically and viewed as a set of tools, standards and techniques, agreed and accepted on the basis of regulations institutionalized designed to coordinate and conduct of the member countries in the markets, financial flows and international money generated by the conduct of trade or commercial and to ensure movement in time and in space capital resources). Electronic coin parity was even at the level of one ounce of gold during the crisis period in the South of Cyprus, investors trying to avoid the transfer/withdrawal of financial deposits (Cüneyt Dirican, 2016). To this are added the advantages and disadvantages of digitization which allow performing most banking and financial operations and of insurance from home or from a simple office. Cases in which a person has to personally sign documents at the bank are becoming scares.

Although so far there are no reliable studies prepared for the possibility of analyzing the collapse of several banks or central banks, it is quite clear to policy makers that a large part of the system will be redesigned. More banks went bankrupt at about the same time (Lehman Brothers case was one of the most publicized in 2008), producing a major imbalance in the interior and exterior of banking system, questioning the system of issuing actives without cover that had worked until then. Massive interbank lending and the support intended to be given by several states to resolve the issue in a positive way, did not save the situation.

Loan limitations to non-banking institutions that perform financial banking activities (demand for fast loans on the market today can lead to a system and speculative financial investment beyond the control of central banks/national), coupled with control over electronic coins is a desideratum very difficult to achieve since it is hard to believe that a global financial harmonization may be achieved in a reasonable period of time (European Union anti movements may hamper efforts and bring serious harm to systems). As already mentioned, the appearance of electronic money and the ability to operate mainly from a simple phone opened the door for some new opportunities, payment systems and financial transfers entering a new phase. For example, certain beneficiaries there have the possibility of paying

bills without going to banks branches for encashment. Even if the amounts transacted separately aren't large, the cumulated volumes may become very important if they they're not monitored by banking systems and may lead to leaks and massive redirections of funds. The virtual environment did not only enabled a formal globalization, in the sense that data can be saved and synchronized „in the cloud", but offered the possibility for financial organizations to start discussing about how to synchronize all account numbers banking payment cards with mail accounts, with personal property computers, mobile phones and related phone numbers. It would not be surprising to witness mergers on functional lines between banks and groups of banks and telephone providers or groups of providers. Of course, in these projects providers of virtual internet service will be taken into account. The risks are proportionate to benefits. At that moment, in the event of an unwanted breach, criminal organizations may have access to absolutely all resources of individuals / companies. That is why analysts are trying to highlight two major issues facing the global banking system - financial stability and security. For stability, designing an interbanking compensation system was asked for in the new SEPA (Single Euro Payments Aria) space along with application policies, as well as bidding through absorption by the central banks of the bit coin issuing companies. To these are added the necessity of remaking the system of inflation in relation to the adoption and use of electronic money. To emphasize one aspect related to security, even though it may seem a misplaced proposal, there are calls for a monitoring of new 3D printers capable of reproducing and producing more variants of denomination close to the original than conventional printers. The limit in this case between control and economic freedom is fragile.

2. International standards regarding the money laundering

2.1. Recommendations and sanctions

As a particular case in the international financial system, monetary integration in Europe has generated, as benefits, the reduction of transaction costs, elimination of the currency risk of intra-Community transactions, the increased efficiency and competitiveness, increased integration between European financial markets which increases the efficiency of capital allocation, a greater discipline in terms of inflation and fiscal discipline required to enter and stay in the Eurozone, accelerated structural reforms in the EU to support the deepening of integration, etc. On the other hand, in terms of costs for monetary integration in Europe, the possibility of using the exchange rate as a policy tool to mitigate the effects of asymmetric shocks is eliminated because the system based on the fixity of exchange rates, countries could no longer use monetary policy and their own fiscal policy instruments to mitigate country-specific shocks and economic stabilization (Cristian Păun – Cours I), etc. The voices that strongly argue the union system, however, are sometimes contradicted by decisions taken at national, long-term

implications being particularly hard anticipated (Brexit is one of the most eloquent examples).

We mentioned these elements to understand the dynamics of financial systems that act together as a unified organism that must adapt to social developments. In this context, standards or changes are in turn annotated to be able to respond to new challenges. That is why FATF/GAFI (Financial Action Task Force (on Money Laundering) eng./Groupe d'action financière fr.) recommendation are or should always be in the limelight. AML/CFT (Anti-Money Laundering and Counter Terrorism Financing) policies and coordination policies refer to risk evaluation and application of risk-based approach as well as cooperation and coordination, at national level, while money laundering and confiscation refer to the money laundering offense, the confiscation and the insurances measures. Financing of terrorism and proliferation treated areas related to crimes of financing terrorism, financial sanctions concentrated linked to terrorism financing and terrorism, financial sanctions concentrated related to proliferation financing and regulations on non-profit organizations that may be misused. Preventive measures refer directly to the law of secrecy by financial institutions, including banking secrecy law, procedures for customer due diligence and record keeping (customer identification and document processing), additional measures for customers and specific activities (politically exposed persons, correspondent banking services, transfer money or valuables, new technologies, electronic transfers…), audit, control and financial groups (confidence on collaboration with third parties to obtain additional information, internal controls and branches/subsidiaries of foreign, high-risk countries…), reporting the suspect transactions (confidentiality in conjunction with reporting of information by national/international investigation) and the designated non-financial businesses/professions (casinos, real estate agents, legal entities marketing activities metals and gems, professional, independent activities…). Another recommendation concerns transparency on establishing real beneficiary person / entity. Powers and duties of competent authorities and institutional measures aimed at regulating, supervising and law enforcement operations (Financial Intelligence Unit (FIU), responsibilities, skills, detection of trans boundary through cash couriers…), general requests (statistics, guides ad reactions) and sanctions. Last recommendation, of the forty mentioned until now, refers to international cooperation in mutual legal assistance, including when it comes to blocking and confiscation of the instruments to joint action, extradition and other forms of cooperation (The FATF Recommendations, 2012).

Financing of terrorism is widely regarded as a very serious offense. In some states it is punishable by imprisonment from five or ten years to life imprisonment, and in other countries apply capital punishment. The top ten states with the most convictions are Saudi Arabia, USA, Turkey, Algeria, France, Israel, Russia, China, and Kazakhstan (FATF, Report to G20 Leaders, 2015). It has been discussed in many treatises on terrorist financing, but in very few cases the study

of financial terrorism was addressed. Money laundering is often linked umbilical to both subjects. For funds to be reinstated after gaining legal aspect placement and layering, they first have to be obtained, the diversity of sources being just an additional form of masking the ultimate goal. To tackle illegal actions more successfully, it is necessary to quickly implement United Nations sanctions. Therefore, many states have adopted additional measures. While eighteen of the twenty-eight member states of the European Union have implemented national measures that could maximize the FATF recommendations and UNO requests, the legal system in other states allow temporary freezing of suspicious transactions to prevent the dissipation of assets or even disappearance funds. The time required to activate sanctions and activation requests including measures accelerated are often treated differently. There are states whose legal framework and infrastructure allow sanctions and the freezing of funds, but there are countries inside and outside the European Union whose laws can be reshaped in order to improve formal powers, to eliminate loopholes and restoration priorities. National strategies are not always consistent with international recommendations even if in compensation, the financial institutions use in practice more automated compliance software to detect clients and monitored activities, updated in real time and loaded in special lists. Consequently, the FATF/GAFI decided in October 2015 operational and closer ties with the experts of the Egmont Group/FIU (http://www.egmontgroup.org/) and develop an additional process tracking to improve compliance with specific recommendations and increased legal frameworks to support member states and jurisdictions requiring advice and assistance. Other jurisdictions will be monitored by the relevant regional body. New legislation is already proposed for implementation in several jurisdictions to address issues identified through this exercise. Work has started on reviewing the standards of FATF and preparing a manual for streams on requests for blocking actions to money laundering and terrorist financing, which will lead to addressing potential obstacles by centralizing information on responsible authorities, points of contact, procedures, requirements and evidentiary legal in all jurisdictions members of FATF/GAFI. Improvement of multilateral coordination on the implementation of targeted financial sanctions will reduce delays involved in implementing sanctions. Research program regarding the financing of terrorism aims to better understand risks, trends and methods of terrorist financing and emerging risks ((FATF, Report to G20 Leaders, 2015).

2.2. Analysis and investigation

In some specialized studies concepts of tax evasion and tax fraud (Emil Dinga, 2008) have been clearly defined. If we try a general classification, money laundering activity may be treated as fraud rather than tax evasion. Crimes competition and the stages taken generate this conclusion.

Carefully planning an investigation can identify a priori some of the issues related to management and people responsible for this, strengthen internal control,

stop the bud of the leak, send a message of intolerance of any deviation, determination and cessation of possible consequences /losses. The screening process involves several stages among which we can mention without a predetermined order to obtain evidence, reports, depositions, detection and prevention. Even if the term „forensic accounting" (the ability to investigate fraud or embezzlement and analyze financial information used in legal proceedings) doesn't involve automatically the investigation procedure of a fraud, it may contain elements related to computer forensics, electronic forensics, the study of fraudulent bankruptcy and of masked insolvency, the economic calculation of losses, the real evaluation of the business and the determination of the cases of professional negligence. The examination methodology involves the assumption of investigating potential litigation, predictability, approaching the issue from two perspectives (the investigator must take into account both the possibility/probability offense/crime and their absence), moving from the general to the specific subject tackled, access the similar theoretical casuistry analysis of available data, create hypotheses, hypothesis testing, redefining and add additional information assumptions, compliance reporting protocols, compliance with the decisions makers on ways to share, etc. Structuring data is particularly important and therefore a digital forensics expert identifies, recovers, collects, preserves, protects, saves and processes digital information extremely volatile sometimes necessary for investigation. Often, to get access to such data it is necessary to support law enforcement teams. Determining location information-gathering is another issue that can pose serious problems given that the cloud space is viewed as an interim step toward a new concept of concatenation. Even if it is desired to merge used sources, transmission and processing, gaps in current monitoring systems easily allow avoiding long-term in the sense of discovery and production samples. Dealing with the connected elements to physical persons suspicious of being involved in criminal activities, with elements collected during the supervision of the transactions ordered for legal persons, may lead to determining results for the success of discovering and building the evidence in case of frauds.

3. Cyber-crime – source of funds for money laundering

Talking about Internet vulnerabilities and the risk of money laundering, we cannot fail to notice the sites that host online auctions, even large value transactions, in which the buyer and the seller are located in different locations, are not known and in some cases are not identified/ identifiable. Compensation system may be payment systems owned by commercial sites (PayPal, EBay…) or systems for fast transfers of funds, involving cards as a tool being optional. Some corporations that manage these sites have compliance structures because the number of users exceeds several hundred million and the turnover can pass quite easily, annually, the limit of tens of billions of dollars/eurs. In these conditions, in conjunction with fictitious sales and purchases with expenses accounts can lead to

covering their tracks. Besides, virtual international communities (an example is the „Second Life" Community, the reference coin being „Linden Dollar") where anonymity is respected, may have several million residents to create their own currency and economy based on a „gross domestic product" of hundreds of millions or billions of dollars / euro.

3.1. Money movement

In specialty literature, we often encounter the term „carriers" without which, actual movement of money would be more difficult for criminals. In classic cases, the physical transport of cash entails an analysis that attempts to answer some questions as to the need for moving money (taking money, the move, the deposit and further use of money), from a criminals' point of view. Methods and techniques involve choosing the route, discussing the nature of the currency and its denomination, as well as its physical method of transport. Very close international cooperation is the only way to detect and monitor carriers' teams (FATF Report - Money Laundering, 2015).

In a specialized study (Rutger Leukfeldt & Jurjen Jansen, 2015), the authors depicted the characteristics that differentiate the carriers groups according to their technological level and according to the methods used to produce the fraudulent money. In the case of cyber-crime there are at least two separate, distinct lines. One of them refers to the physical aspect of the problem and the involvement of ATM type machines and point of sale (skimming ATM and PoS) and the second draws attention to some actions that involve collecting data, creating profiles and computer accessing accounts (phising, malware…). If we refer to the amounts obtained via PoS's or the amounts brutally obtained by accessing ATMs and destroying parts of these, the incomes gained by the criminals are quite fast, because the skimming devices for POSs and ATMs can copy the data, and then the information collected can be used to clone the cards and cash withdrawal. At the same time, methods of taking control over ATMs can provide almost instant access to the entire reserves stored in the vault, and in the case of doubling the amounts on POSs (double fictitious transactions through „trading/processing" leads to doubling the amount that should normally charged), the money goes directly into the offender's pocket. If not caught in the act, „arrows" with „operators" and „carriers" make disappear fairly quickly from perimeter devices amounts extracted but the amounts remain within the group and are reused almost immediately if the values are not important. Where funds are obtained through access to information from unauthorized accounts the victims using advanced technology and soft malicious, the money is often transferred to the accounts of people who may have knowledge of the criminal activity or be misled for being used as a „buffer" in the process of placement, layering and integration revenue. As a comparison with the methods used for ATMs and POS, phishing involves collecting fraudulent information and is considered low-tech, on

a scale far above being placed using malware that allows access to very large databases and feature even the possibility of penetration into the security systems of financial banking institutions. Subsequent transfers online can cause immense damage. Another feature is related to the number of participants required to conduct major similar operations. To earn incomes similar to those of a high-tech group, low-tech groups should be much larger or get engaged in more extensive activities leading to increased risk of being intercepted. Age categories are another yardstick, young people showing an appetite more pronounced for high-tech while middle-aged persons prefers be simpler methods and expose themselves less, even in terms of more modest earnings . On the other hand, members of the second group transfer in one transport much larger amounts than those of the first group, one explanation being that of building more solid trusting relationships. Computer dexterity allows members of the first group a „dosage" of amounts so as to avoid filters analysis of the institutions engaged in combating crime in general and in particular money laundering. Before the law, there come much harder and much rarely high-tech groups because the latest technology and software used allows them to conceal traces much better and to hinder the evidence that would lead to their conviction. Socio-economic status of the entire criminal group is directly proportional to revenues. On a graph with only two axles, low-tech versus high-tech revenues from cybercrime can be drawn at any time with exponential growth curve.

3.2. Virtual currency and money laundering

Modern technology has entered a new phase and the Internet's evolution for transmitting, storing and processing information generated new economic challenges but also big problems. One of these refers to electronic currency derivatives, especially since a large part of the online community believes that alternative currency will replace traditional units, being classified as crypto-currencies (digital currencies or electronic virtual coins). A crypto currency is essentially a digital currency conceived as an encrypted sequence, capable of meeting expectations such as anonymity too (Ajibola Adetilewa Ogunbadewa, 2013). It seems that the objective of one of the inventors (Satoshi Nakamoto) the most popular coin digital virtualized since then (Bitcoin) was a politically and economically, trying to create a new system that would solve many problems of the traditional (an example can be vulnerability to inflation) and had no reason related to the desire to fraud, but the economic crisis of 2008 offered users new perspectives exploitation.

Whatever the perceived or potential economic role for virtual money, the question remains as to the legal framework that will apply to similar technologies. If we want to talk about the legal status of virtual currencies, we can say that currently they have no equivalent of physically legal tender, and are not supported as an exchange coin by any legally constituted government. Because of the

possibility of their use for fraudulent activities such as money laundering, virtual currencies had a negative impact and some authorities may have seen it just as a platform for supporting criminal activities. Reputational security is particularly affected. More than that, in certain states (an example is in Thailand) some were outlawed together with those who would transact them. After the creator of Liberty Dollar was convicted because he had used for virtual payment inscriptions that appeared on other legal currencies in circulation (Von NotHaus designed the Liberty Dollar in 1998 but the Liberty coins were marked with „$"), the creators of the new crypto-currency were more careful concerning the international legislation in general and national legislation of the originated country, in particular.

There are also self-imposed limitations governing, in certain ways, their movements. An example is the Bitcoin, which can be put into circulation only at a maximum of 21 million units. Virtual currency has many forms: physical - where a virtual currency is represented on a physical support, centralized - where all transfers occur through a single intermediary or they're decentralized - where network share transactions nodes, part of the latter category and Bitcoin are traded directly between network users (peer-to-peer). A typical Bitcoin transactions, including those involving money laundering can include five entities: a sender initiates the transaction through the Bitcoin network (the placer of dirty money), a Bitcoin receiver accepts the transaction (the placer's accomplice helping him cover the tracks), the generator of Bitcoin „mine" intervening in the transaction, the processor that can charge a nominal fee and acts as developer that updates the Bitcoin base code as needed, and the operator of exchange that facilitates the conversion of Bitcoin in other currencies /values or vice versa (Danton Bryans, 2014).

Main features of Bitcoin that prove beneficial for survival and immune to the pressures of external regulation are anonymity and the flexible adaptation of the protocol. Bitcoin allows any potential user, to legitimately or criminally transfer money with high speed and low costs. However, although Bitcoin and other analog virtual currencies could allow criminals to move illicit funds faster, cheaper and more discreet than ever, part of the international community militate in favor of legitimizing them, considering that people should be free to use any currency they wish. At the same time, the report of the European Central Bank, Bitcoin is viewed as a virtual currency and in accordance with the legal framework of the European Union, Bitcoin falls most likely under Directive for electronic money, thus indicating that it falls clearly falls outside the scope of the Directive on payment services (http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf). The report further noted that, although such virtual systems are not a major risk for the stability of quotations of traditional coins and do not fall under the current regulatory scheme, they are within the area of responsibility of the Central Bank.

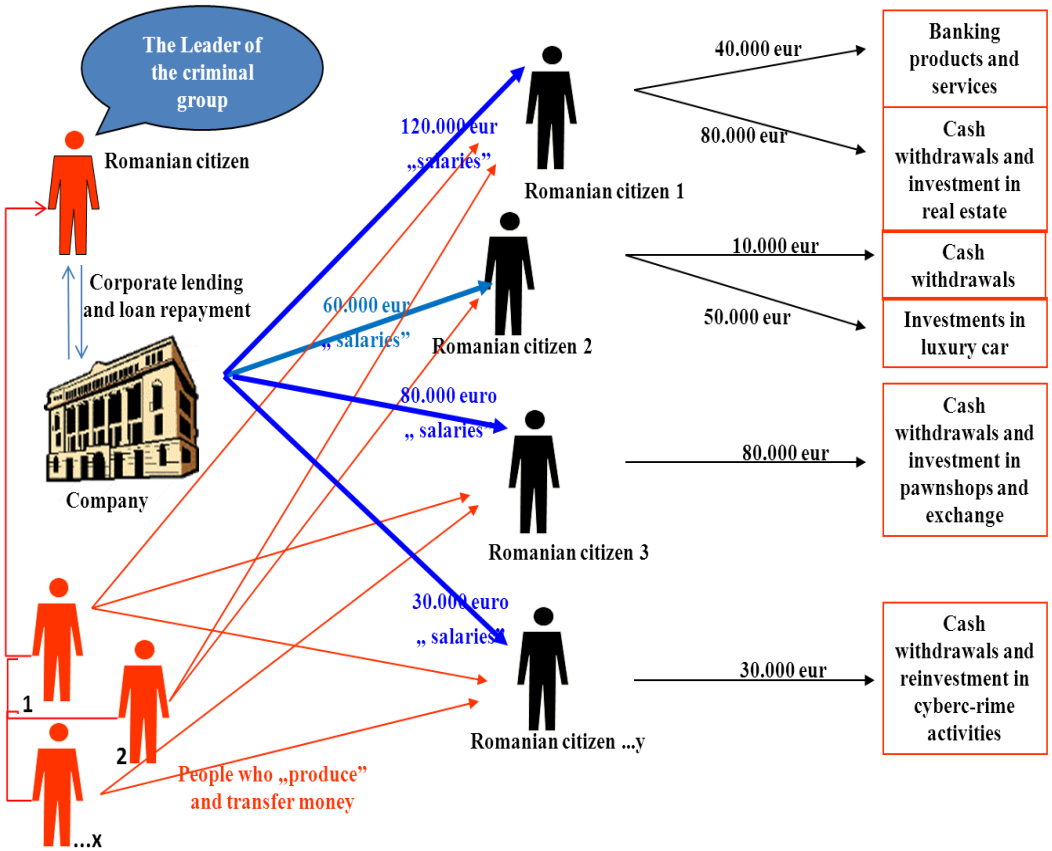
This means that for now, even if Bitcoin is not accepted as a regulated payment currency it's value as a unit of account is recognized and therefore subject to a financial instruments of payment which should have a license and be regulated as an entity, especially since many individuals and businesses have expressed their support online and started to accept payments via Bitcoin (Internet hosting companies, public food services, security services, consultancy and non-profit…). Some companies even facilitate in the limelight the Bitcoin conversion to other currencies.

Actual international perspectives with tendencies of handling the legality of virtual currency present a picture in compliance with which the competent authorities share the opinion that they are not considered automatically illegal but, the businesses that could be carried out with their help could be difficult to monitor and would elude any budget payments, taxes, and department fees. Virtual currencies can be a disruptive financial technology but in a world becoming increasingly digital they are building their own economic and social sense. Instead of increasing regulatory and predictability, it might be best to increase the understanding of new technologies and policies to adopt better decisions, and sanctions in case of violations of civil or criminal nature.

3.3. Methods of money laundering

3.3.1. Money laundering resulted from frauds with cards

An example of money laundering that resulted from cybercrime is shown in the figure above, in which the leader of the group practically performs the whole action.

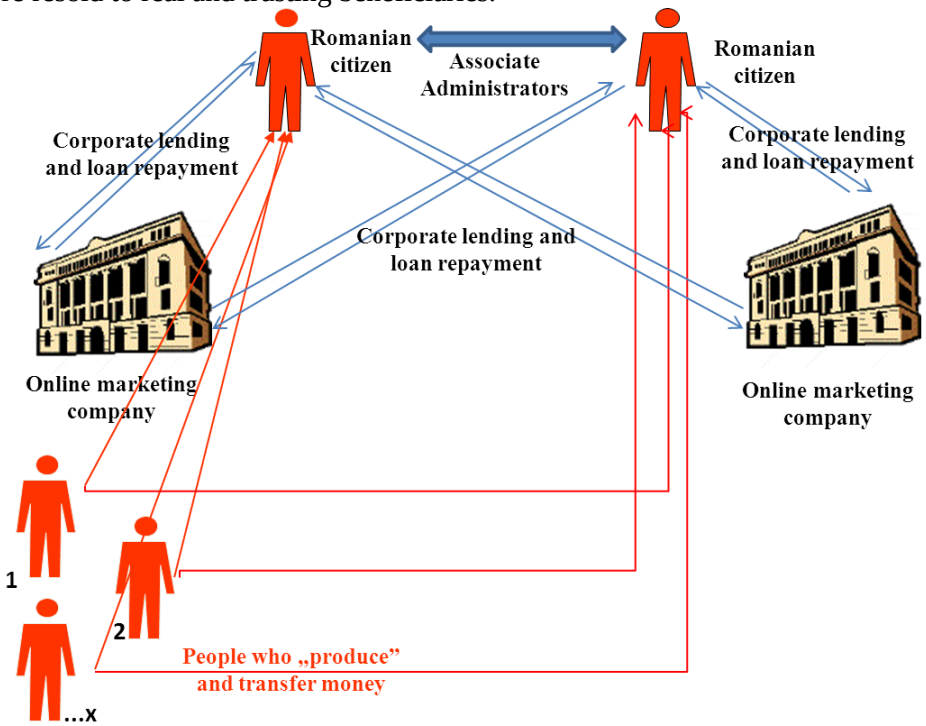


The money obtained fraudulently is transferred to third persons „engaged” in a real lucrative business that pays generous fictional wages, thus uploading expense. In exchange for a fee paid to „employees”, the money is placed in banking products and services, investment property, luxury car, pawn shops and money exchange, etc. Part of the money is returned to the criminal circuit by investments in high-end devices and software. Apart from these amounts, all initial investments are liquidated later to remove their tracks as much as possible. If we consider that the person who coordinates this can be one of the company's shareholders and could „lend” fictitious (as a personal contribution or loan from a person/entity - third party that is part of a fraudulent scheme) amounts from all of cybercrime to be able to withdraw amounts (personal contribution refund or credit contracted) paid to fictional third parties, we might begin to understand the full picture.

3.3.2. Money laundering through e-commerce activities

Another example is to invest money from cybercrime in companies that sell products online. Managers and associates credited newly established firms in

successive stages with small amounts dirty money, by purchasing products that were resold to real and trusting beneficiaries.



Shopping websites allowed redirection exactly to those who were „responsible" for collecting information, as well as the production and transfer of funds obtained fraudulently. Turnover increased while lending to companies and administrators continued over several years. In a maximum peak of sales period there were major delays in delivery to customers of items ordered and paid for, seeking reimbursement from loan companies, followed by cash withdrawals by administrators. Money laundering was corroborated with fraud; the goods that had to reach customers were not in reality in the company's stores. Thus, the „business" was prepared for liquidation and then, the „scheme" was subsequently resumed in another geographical area.

3.3.3. Money laundering within the same group of companies

X SRL Company headquartered in City B has been identified as a suspect in money laundering, the element of suspicion being given initially by transfers between companies belonging to the same group. The amount received in the account opened at bank M of SC Y SA reached a detouring bank circuit in the account of SC Y SA from Bank N. On dd1.mm.yyyy, by discounting a ticket order, SC X SRL with accounts opened at Bank O received an amount bbb.bbb,00 ron from SC Y SA, with accounts at Bank M. On dd2.mm.yyyy at Bank O was

presented the payment order No. ppp1 of the same value of bbb.bbb,00 ron, and the payer being SC X SRL, and beneficiary SC Z SRL, with accounts opened also at Bank O, the payment representing the counter value contract of cooperation No. ccc1/dd3.mm.yyyy. The same day dd2.mm.yyyy, SC Z SRL pays with payment order No. ppp2 the same amount bbb.bbb,00 ron to the beneficiary SC Y SA, in the account from Bank N, the payment being done based on the cooperation contract No. ccc2/dd4.mm.yyyy. As we have mentioned, all those companies were part of the same group and subsequently it was discovered that the money resulted from cybercrime.

3.3.4. Money laundering and the Nigerian letters

Customer X based in city S requires the issue of a bank guarantee in foreign currency of a value of b.bbb.bbb usd for guarantying the payment to a lawyer Y, who intermediates the taking operation of the amount bb.bbb.bbb USD from the fortune of a doctor Z deceased, offered to person X by W from country N, the widow of person Z. The transaction identified initially as fraud due to the way it was carried out (messages via Internet) was fatherly confirmed as money laundering. After accessing the site Internet-Fraud.com the e-mail messages were identified, using the same name (Y, W) used for fraud attempts. The suspicious document shown as an evidence of the existing funds in Nigeria and the communication between parts (e-mail) led investigators to the conclusion that those goods for which the issuing of the guarantee were voluntarily pledged by person X and recovered after a period of time in order to hide the amounts resulted from real frauds.

3.3.5. Money laundering by means of ATMs

The method of money laundering may seem improbable because we are accustomed to the idea that ATMs are exclusively owned by banks, but in some areas it is considered quite a cheap, simple and safe method of money laundering because the device can be bought and placed in an area that can be monitored and controlled by criminals, or even placed in a legitimate business. The phenomenon is studied carefully, Association of Certified Fraud Examiners (ACFE) showing a very solid point of view. The ATM is loaded with money from cybercrime and the bank debits the card of every user in good faith, crediting the bank account of the legitimate owner of the ATM. The card reading device can retain data from the cards so that they can be cloned later and re-enter new amounts in the criminal circuit, or maybe just act as a normal card reader. The method is preferred by some groups because there are some areas where operating procedures of private ATMs are not regulated, no request for history background of the buyer are issued, and there’s no obligation of reporting procedures or rules of registration of sales management (ACFE, 2015).

3.3.6. Money laundering and the Prepaid system

Some of the areas with potential for money laundering from payment systems refer to gift cards offered by retailers, prepaid debit cards, prepaid phone cards, payroll cards with overdraft (wages given by the employer incompliance with the issuing bank, in advance to the working hours performed by the employee), transport cards, etc. Many businesses offer the possibility of using prepaid cards, beneficial for both merchants and consumers. Prepaid system vulnerability is the most attractive element for criminals engaged in money laundering and arises from anonymity of the holders, often lacking the regulatory environment. In addition, the cards / prepaid cards are easily manufactured, transported and used. All methods are centered basically on the same principles. Money from cybercrime is loaded and can then be transported or placed based on the offenders needs. Millions of prepaid phone cards can be used by customers, the money going into the criminal groups' bank accounts. The same method can be applied to gift cards preloaded with amounts that end up in the criminal scheme administrators' bank accounts.

3.3.7. Money laundering and Mobile Payments

Online payments as an area that integrate mobile payments broaden the access to money launderers. They use channels that are designed to be secured so that the service provider takes as many steps as possible to mitigate risk. However, there are risks that are generated by the user. If the client fails to protect details of his secure access or if a virus infects his phone, it is automatically exposed to risk. The debate on the issue of activating communication data reveals different points of view from users. Mobile phones can act as tracking devices to help locate the owner. If the phone is used for financial services, the data collected is enriched with additional information on payment methods and transactions (Louis de Koker, 2013). Investigators concerns stems from a premise under which there's the possibility of taking control of several peoples' mobile phones or even groups of individuals enrolled in the same network or different networks. Multiple low value transactions can avoid reporting and monitoring systems, covering their tracks and hiding money. The paradox is that if the customer does not often check his transaction history, he doesn't knows he was used as a relay because he doesn't see any obvious disparity in his receipts and payments balance. However, the situation is completely different if the account holder of the phone owner and beneficiary of mobile payment service is defrauded, but the purpose of the criminal group in this case is not to fraud. The goal is to have as many layers as possible, as to avoid being detected. The advantage of online payments made on computers is given by the mobility, possibility of dynamic routing, crossing from one phone to another network and phone payments directly to retailers without the need for card. The transportation of money in this case is quite simple and in addition, if the money

from cybercrime are accessed on a mobile device, they can be diverted without any impediment to the destination desired by the offender.

3.3.8. Money laundering and the virtual assets

Virtual assets are similar to virtual money or to the digital coins. They benefit from the same characteristic of anonymity and lack reglementation, but the domains of applicability are more reduced even if they also transitioned on-line. Internet casinos and games provide the ideal money laundering schemes. Criminal organizations may exchange assets in return for their later use of virtual currencies or to engage and support the gamer to achieve best results in order to take possession of as many shares (assets). Another feature of the assets is that they began to be used as currency between criminal groups. Value per share may differ depending on the area of interest of the seller and the buyer. As mentioned, if in the case of virtual money there are algorithms pretty well established, in the case of virtual assets there is a much wider flexibility.

4. Conclusions

SMART technology is a reality. Online payments, electronic money and digital money, „Internet of things" and market information systems are an integral part of the financial compensation. Mobile payments represent a great promise in terms of financial inclusion but also pose financial integrity issues. Virtual currencies have created a bridge certified and accepted by users as an alternative to currencies and securities backed by governments. It is unlikely that the international law or the national laws will include all changes occurring in the emerging technologies market and adapt to them to real time. The points of contact between the public and private sectors can become balance points for solid construction or they can contribute to the deepening conflict between the new and old or between traditional and futuristic. The result of such clashes is difficult to predict.

REFERENCES

[1] **ACFE**, ***Fraud Examiners Manual* (2015),** *International Edition*;
[2] **Ajibola Adetilewa Ogunbadewa(2013),** ***The Bitcoin Virtual Currency: A Safe Haven for Money Launderers?;*** *University of Wales System - Carddiff Law School, September 2013*;
[3] **Cristian Păun**, ***Cours I, International Financing, Introduction in the Problematic of International Financial System***;
[4] **Cüneyt Dirican(2016),** ***Will the Central Banking be the Center of Banking?***; *International Journal of Economics, Commerce and Management, Vol. IV, Issue 5, 2016, United Kingdom*;

[5] **Danton Bryans (2014),** ***Bitcoin and Money Laundering: Mining for an Effective Solution;*** *Indiana University School of Law, 89 Ind.L.J. 441, 2014*;
[6] **Emil Dinga (2008),** ***Theoretical Considerations on Tax Evasion vs Tax Fraud,*** *4/2008Financial Studies, theoretical and modeling approaches*;
[7] **FATF**, ***Terrorist Financing FATF Report to G20 Leaders***, *November 2015*;
[8] **FATF Report**, ***Money Laundering Through the Physical Transportation of Cash,*** *October 2015*;
[9] **Louis de Koker (2013),** ***The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity RisksWithin the New Standards Framework***, *Washington Journal of Law, Technology & Arts Volume 8, ISSUE 3Mobile Money Symposium 2013*;
[10] **Rutger Leukfeldt & Jurjen Jansen (2015),** ***Cyber Criminal Networks and Money Mules: AnAnalysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands***; *International Journal of Cyber Criminology, Vol 9 Issue 2 July – December 2015*;
[11] **The FATF Recommendations**, ***International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,*** *February 2012*;

I. Internet resources:

[12] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf;
[13] http://www.egmontgroup.org/
[14] https://regulation.revues.org/7473?lang=en;
[15] http://www.riksbank.se/en/The-Riksbank/Research/Historical-Monetary-Statistics-of-Sweden/.