TECHNIQUES TO SIMULATE THE LEGAL ORIGIN AND TO DISGUISE THE ILLICIT ORIGIN OF MONEY

Gruia Petrişor, PhD Student
Valahia University, Târgovişte

Abstract: *Today**, money laundering techniques** are much more varied and more numerous, ranging from the use of bank accounts of individuals or companies to life insurance contracts, luxury goods purchases or "maneuvers" on the capital market or on the real estate market. The authorities' efforts to diminish the criminal phenomenon, by enforcing legal provisions, including those on money laundering, forced offenders to find new ways to shelter the law. That's why money laundering techniques are in constant motion and they do not know limits (perhaps only the imagination of offenders) and criminals are constantly trying to find new ways of washing. The goal is to identify the vulnerable segments of the financial system to generate fast, anonymous and efficient flows, extremely difficult to track. In the past, banks were the launderette's favorite institutions, but lately the situation has begun to change. The banking system has become increasingly supervised and pursued by the supervisory authority involved in the fight against money laundering, and the professional training of bank officials with responsibilities in the application of WBT / CFT legislation has increased considerably. Under these circumstances, offenders are trying to take advantage of the weak link in the chain of the global regulated financial system and law enforcement bodies by moving transactions, communications or assets to the least regulated jurisdiction with the most corrupt authorities law enforcement, with the highest degree of banking or professional secrecy, with the most ineffective seizure system, or the most inefficient banking supervision system*[28].

Keywords: *Regulation and Business Law; business economics; Financial Markets and Institutions*
JEL classification*:* K23, M21, N24

Money Laundering and Anti-Money Laundering Laws have imposed stringent regulations to control the recycling phenomenon through banking institutions. Firstly by imposing customer knowledge standards and by making reporting to the competent authority. Romanian legislation requires banks,

28 Savona, E. U., De Feo M. A. – „Money trails: internaţional Money Laundering Trands and Prevention/Control Policies"

financial institutions, and other non-financial entities (including accountants / financial auditors) to submit three types of reports to the authority, such as suspicious transaction reports, transaction reports with cash over the equivalent of EUR 15,000 in any currency and reports on external transfers over the equivalent of EUR 15,000, expressed in any currency.

As legislation narrows the maneuvering space of offenders, they tend to focus their activities on other sectors, less regulated or more difficult to control, such as the securities market, the precious metals market, the legal advice sector, and fiscal-accounting, etc.

The money laundering techniques we are going to address in the following are the following[29]:

A. Counterfeit cash / cash;
B. Use of bank transfers;
C. Using Company Accounts;
D. Using „ghost"Folosirea firmelor „scoică"
E. The use of the capital market;
F. Money-laundering (Trade based laundering);
G. Use of insurance companies;
H. Internet payment services;
I. Digital or electronic currency;
J. Use of exchange houses.

A. Counterfeit cash / cash

Counterfeit cash is represented by the physical transport of cash across national borders. It usually involves hiring couriers to transport money to countries where there are no restrictions in the field (or where they are less severe). The FATF qualifies as cash couriers individuals who physically transport money from one jurisdiction to another, along with personal luggage[30].

In some situations, cash smugglers have demonstrated a high complexity of operations, even taking control of expedition companies, and then hiding dirty money inside the parcels for export.

A typology for cash smuggling is the directing of the cash flowing from the current activity of some transport companies to the states of origin of the employers' companies through the drivers. Not many times they were found at the crossing of the Romanian border, carrying small sums (10,000-20,000 EURO) in cash that they did not declare and could not justify. At first glance

29 Nicolae Ghinea, Dita Bondarici (2005), Fraudulent Use of Payment Instruments - Publishing House. LUCMAN, Bucharest, p. 67

30 FATF Guidance – internațional Practices – Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments – 19 February 2010;

it does not seem too much, but if we take into account the fact that these races are regular, running at least once a week, a simple calculation leads us to the conclusion that, once a year, a single driver of a single transport companies can take out of the country over 520,000 EURO.

Many national authorities have found an increased incidence of cash accumulations in border areas or in ports. Generally, this is an indication that cash smuggling is taking place in those regions. Consequently, the most drastic measures were taken to reduce the phenomenon[31].

From a geographic point of view, areas of high risk are the territories where offenders can move freely between jurisdictions, such as, for example, the European Union space as well as large countries with long, easy to cross borders and numerous ports. Airports also pose a potential risk, and for this reason, jurisdictions pay particular attention to these border crossing points.

Transparency associated with bank transfers and (more recently) and money-surrendering or other value-added services are factors that have led criminals to reconsider the importance of cash smuggling as a key element among the "move" disguising their origins and hiding traces.

Cash appears in all profit-oriented crimes, from drug trafficking to cyber-crime. A recent study[32] shows that cash remains an important part of the chain of recirculation operations in the case of cyber-crime, which can be identified in all three phases of money laundering as it has the enormous advantage of contributing to the loss of traces of dirty money.

B. Use of bank transfers

The use of bank transfers is particularly useful for money laundering. It is a fast, efficient and highly anonymous process (due to the huge number of transactions that take place on a daily basis). Once you enter the system, money can be easily transferred anywhere in the world, sometimes even without having contacts with bankers, in the case of Internet Banking operations.Most money transfers in the contemporary world, by talking about significant amounts of money, are made through bank accounts. Criminals do not want to, and do not want to avoid, this process, which offers great operating facilities, as well as the possibility of simulating commercial or lending operations, masking the fund[33].

31 At Amsterdam Airport there is a police unit specializing in detection of cash smuggling (and drugs), with dogs trained to detect banknotes;

32 Criminal MoneyFlowson the INTERNET – MONEYVAL research 2011, http://www.coe.int/t/dghl/monitoring/moneyval/default_EN.asp?

33 Popa S, Dragan G. – Money laundering and terrorist financing - planetary threats on financial routes - page 45

The advantages offered by this method are related to the speed of the operation and the irrelevance of the distance element, the funds being usually sent to a remote location (where the investigators are unlikely to travel to follow them). On the other hand, the disadvantage lies in the fact that the method leaves traces in the system because all these transfers and the identity of the persons who carry them are recorded by the banking institutions operating them and the records are kept for at least five years after the termination of business relations with that customer[34].

Although new technologies such as on-line payment platforms or digital money are gaining ground in the contemporary economic and social environment, criminals and "laundries" still depend on the financial-banking system. Bank transfers can be a quick and effective tool for money laundering in a series of "fashionable" cyber-attacks such as cyber attacks at the beginning of the recycling process, especially if fraud is the removal victims' money from their own bank accounts. At the next stage, the money is quickly transferred to the carrier accounts and withdrawn in cash or redirected to other destinations If sent to other jurisdictions, transfers are often made in amounts below the reporting threshold (€ 15,000 or equivalent) to avoid making the origin of those funds compulsory.

Regardless of the method of payment, international fund movements have a number of characteristics and vulnerabilities in terms of money laundering, as if borders disappear for goods and funds movements (especially within supra-state entities such as the European Union) , they remain a barrier for the policeman and the judge, slowing down and complicating the discovery of criminal pathways, obstructing the effectiveness of repressive actions.

International money dispatch is usually part of the stratification step and follows other operations previously performed, such as the use of cash handlers. In transnational operations, more than one state is usually transited, making it more difficult to identify the offender who is "leading the game", the one who invented the scheme and coordinates all transfers across thousands of kilometers. Undoubtedly, involvement in such schemes of companies established in offshore territories or in distant states of one another complicates things even more.

C. Using Company Accounts

A more and more common way in practice is to launder money illegally (usually from tax evasion) by introducing them into company accounts. Criminals store cash in the bank accounts of some companies or their cashier

34 According to international standards

as a "firm creditor" to then receive the amounts back - sometimes with interest - with the title "credit repayment".

In some cases, when the creditor is not the associate of the firm (or a minority associate), the situation in which, following the maneuver described, it may also take over control of the firm credited by transforming the credit into shares or shares. Their value or greater value can be obtained in the case of a firm's divestiture or its dissolution. In the latter case, criminals prefer cash-based businesses such as restaurants, bars, nightclubs, hotels, currency exchange offices, and so on. Thus they have the possibility to mix the illegal money in the form of a false income with the legitimate receipts that alone can not sustain the business[35].

D. Using „ghost"

The use of ghost companies for laundering illicit funds is a relatively new method used in those jurisdictions where the commercial company registration system allows the provision of false data at setting up, fakes that can not or can not be verified in a timely manner and in a manner efficiency.

As suggestively illustrates the assigned name, "phantom" firms do not work anywhere, and their associates and administrators usually can not be identified, they are very young, very old or restricted, but have the necessary legal and tax records in relationships with other companies. There is also the situation of "professional" associates and administrators who simply sell their identity for money, relying on the inability of the authorities to identify or investigate them. The purpose of setting up these companies is linked exclusively to real-estate accounting. The "ghost" companies provide false documents to real companies for their recording in the accounts and facilitate the making of bank transfers through their accounts, transfers that constitute a "buffer" between the real firm's account and cash withdrawal or other money-laundering operations. The "phantom" companies are registered at addresses that either do not exist (number 149 of a street that has only 140 numbers), or have altogether another destination, registering based on fictitious sales / renting documents.

There are many situations where these "phantom" companies with registration number at the trade register and fiscal code have been used for periods of 1-5 years and then introduced into insolvency and radiated. Under these circumstances, the company's administrator and associate / association are "absolved" of any payment obligations. Faced with this practice, in the last years, the delisting file also requires the tax certificate stating that there are no debts that the state budget and the social security budget.

35 T. Seah - Anti-Money Laundering 101 2006 – pag. 40

In Romania, the "phantom" firms or the "pocket-sized" companies formed the basis of the great tax evasion, through which the state lost billions of lei[36].

E. Using „shell"

The use of "shell" companies is one of the most common methods by which organized crime networks wash money all over the world, especially if a laundrette has access to a professional in the field (such as a notary, a lawyer, an accountant or financial adviser) is all the easier for him to set up and then to use a company, corporation or "shell" partnership.

Such a firm is usually set up in a fiscal paradise, having a mailbox as a mailing address, and as associates and administrators difficult to identify.

Sometimes behind these companies are individuals who have offshore businesses and use offshore firms for fraud, hiding behind other companies to make it harder to identify them. Specifically, the system works like this: the X person who has the interest to hide his identity sets up two offshore Q and P. Afterwards, he incorporates another company R (possibly another off-shore!), Whose associate is Q and administrator P. Company R is used in business partnerships in on-shore territory, in the sense that it provides different "services" to other companies, receiving counterparts of impressive amounts of money.

Moreover, through the complicity of a professional, it is possible to create a tangled chain of transfers through a network of such firms to mask the origin of the funds resulting from the crimes, and by dividing them into several jurisdictions one can also take advantage of the lack of communication and collaboration between law enforcement agencies in different states.

Faced with this company registration system, the Romanian banking system requires all companies registered in Romania to operate abroad and open bank accounts, carry out the procedure for identifying the beneficiary of the funds and submit all the legal certificates issued by the trade register in the country where registered affiliates have been registered, attesting to this real beneficiary, the natural person, as a majority associate (may be one or more, over the 25% limit of the number of social shares).

F. Use of the capital market

With the sophistication of the financial market, the level of complexity of recirculation operations has also increased. Thus, sometimes black money is used to acquire shares, bonds or other securities traded on the capital market, through which subsequent capitalization can be made of amounts of money of apparently licit origin. The capital market is a possibility to quickly invest

36 Melinescu I., Talianu I – Investigatiile financiare în domeniul spălării banilor pag. 83

large sums of money and is therefore often used by criminals who want to escape the money of fraudulent origin[37].

The capital market also has the advantage of banks' high confidence in operations where one party is a financial investment services company. Thus, a transfer by a person (either physical or legal) in relation to such an intermediary is at the outset considered less risky.

A strong point of the capital market (and a weak point for money laundering) is the high degree of client knowledge by the intermediary company.

Since the capital market, together with the banking and insurance industries is a key segment by which individuals and businesses can access the financial system, in 2009 the FATF published a report on money laundering typologies using securities. Case studies and other information gathered in this research have shown that using the capital market for money laundering is a real threat. Moreover, industry itself can be used to generate illicit profits from licit funds.

When they are generated, these dirty profits are virtually almost automatically washed. This phenomenon is relatively new and contrasts with the traditional situation in which, through the capital market, funds from crimes committed in other areas[38].

G. Money laundering through commercial operations

The international trade system is clearly the object of money laundering vulnerabilities that can be exploited by criminal organizations and terrorist financing. The attractiveness of the system for offenders is related to:

- the enormous volume of commercial flows that can hide individual transactions that can offer criminals opportunities to transfer values across national borders;
- the complexity of financial transactions generated by the use of a large number of foreign exchange operations and the use of different financial arrangements;
- the complexity of transfers that leads to easy merger of illicit funds with those from perfectly honorable sources;
- limited possibilities for authorities to exchange information between jurisdictions;
- limited resources available to customs to detect suspicious business operations.

37 Popa S. Dragan G. – Spalarea banilor şi finantarea terorismului – amenintari planetare pe rute financiare – pag. 47

38 IDEM pag. 58

From the company's accounting perspective, this money-laundering technique is particularly important, as commercial transactions behind which dirty money transfers are camouflaged, are apparently recorded fairly in the accounting of the firms involved in the commercial operation in question, and the professional accountant detects a possible suspicion may be particularly relevant.

In fact, money laundering is done by manipulating the accounting documents of the importer and / or the exporter, resulting in over or under-invoicing, multiple invoicing of goods or services, alteration of the quantities entered in the transport documents and false description of the quality goods and / or services in question.

H. Use of insurance companies

The insurance industry has a special place in preventing and combating money laundering, most of it being in the "heads" of recycling operations. In other words, assurances are used either in the integration phase, as a final good for the use of the offender, or as a ground for committing the predicate offense, in a manner similar to what was done on the capital market. As with securities, insurance fraud provides dirty money, which is then subjected to the recycling process using industry segments, at least in the immediate aftermath.

As far as the integration phase is concerned, we are dealing with the purchase by the scrubbers of life insurance products for them and their families, a matter of great certainty and worthwhile if the insured event occurs (for example, reaching a limit age of the insured person).

On the other hand, even in the case of the offender's death, his family may benefit from important amounts paid in the form of insurance premiums, sheltered by the state authorities or by potential offenders who may claim the wealth gained illegally.

Apparently, the above theory may seem ridiculous, but in practice there are not many cases of confiscation of insurance policies concluded by criminals with insurance companies, even if the offender was convicted for the predicate offense or for washing of money, and some, or even all, goods from offenses (other than that insurance) were confiscated.

From this perspective, the insurance industry is indeed insuring for offenders and their policy recipients.

In Romania, insurance companies have reported to the Financial Intelligence Unit specialized in combating money laundering with very few cases. And when they did, it turned out to be attempts to defraud the insurance company and not to actually launder the money from the offenses. The situation is explained both by the relatively modest development of the insurance

business and by the insufficient concern of these companies regarding the activity of preventing and combating money laundering[39].

I. Internet payment services

The term "Internet Payment System" (SPI) is generally used to describe bank transfers (payment services based on the existence of a bank account, the Internet being the only operating environment for payment orders from the ordering party to the payee), as well as other payment methods offered by non-bank financial institutions operating exclusively on the Internet and indirectly associated with a bank account.

In the case of SPI based on the relationship with a bank account, the transfers are made in the same way as any banking transaction, the only characteristic being related to the physical positioning of the client, namely in front of a computer connected to the INTERNET and not at its bank's premises.

Non-bank SPIs (such as the Pay Pal service) offer their clients a range of services such as: transferring domestic or international funds, making online shopping, using their auction sites on -line, etc.

A number of SPIs allow their clients to hold accounts, in which case all client funds are aggregated into a single bank account opened on behalf of the financial service provider. In this situation, the bank where IPS has an account will not have a direct relationship with each of the individual suppliers of the supplier and therefore will not be able to run the client knowledge procedures in relation to them. Although SPI offers an inexpensive, anonymous and quick way to make international transfers, they are not always subject to the same CSL / CFT control and surveillance measures imposed by the authorities of other "classical" financial institutions, which may make them vulnerable to risks money laundering.

Due to the recent development of SPI, they are increasingly linked and interconnected with various other settlement systems (new or classical). Today, funds can be transformed by a variety of methods, from cash, fund transfer, digital money, bank transfers, or using cards. Furthermore, some SPI providers have begun to issue pre-paid cards that they offer to their customers, thus giving them unlimited cash access through a global ATM network[40].

J. Digital or Electronic Currency

Electronic money is an encrypted code representing the value attached to a particular account, as ordinary banknotes are pieces of paper bearing certain characteristics that make them a symbol of value.

39 Popa S. Dragan G. – Money laundering and financing of terrorism - planetary threats on financial routes - page 54

40 Money Laundering Using New Payment Methods – FATF Document, October 2010

Some experts claim that electronic money is "real money" like banknotes, but it is not (as yet) as liquid as cash as it can only be used under certain circumstances (such as the availability of electronic equipment) , while cash can be used by anyone at any time in any payment transaction.

Globalized e-money services are accessible to all customers all over the world and make it possible to move values from one country to another almost simultaneously, sometimes without leaving any trace. Few of these international fund transfer operations are monitored as it happens with bank operations. Using the digital currency, both individuals and businesses can send and receive virtual money in real time. Payments can be made 24 hours a day, 7 days a week, quickly, anonymously and at minimal cost, without operators leaving their office or home.

As mentioned above, electronic money and quasi-anonymous payment systems are divided into two categories: "trusted" and those based on the value of some precious metals. The first category is based on the mutual trust established between the seller and the buyer. There is no "exchange rate" for such coins and they are of no value to others, except individuals and companies that use them[41].

The second category has a precious metal warranty that determines the exchange rate for these electronic coins (Egold, Pecunix). Once the conversion is made, funds and accounts are unattainable. In addition, some companies offer the possibility of establishing a link between the electronic money account and a debit card that can be used in shops and ATMs.

Cyber criminals and money laundering start to use these systems that offer a high level of anonymity (depending on the issuer) and immediate compensation (conversion), all at a discounted price.

In some legislation on money laundering, electronic money payment systems are not included in the list of entities with obligations in the matter, which is why their operators are not obliged to identify their customers, to keep supporting documents for their operations, or to report possible suspicious transactions.

Bibliography

1. Savona, E. U., De Feo M. A. – „Money trails: internaţional Money Laundering Trands and Prevention/Control Policies".
2. Popa S. Dragan G. – Money laundering and financing of terrorism - planetary threats on financial routes - page 54.
3. Melinescu I., Talianu I – Investigatiile financiare în domeniul spălării banilor pag. 83.

41 http://www.ukash.com/fr/fr/home.aspx