Theoretical basis for detection of legalisation of proceeds of criminal activity

Teoretická východiska odhalování legalizace příjmů z trestné činnosti

JOZEF STIERANKA
STANISLAV BACKA

Abstract

If we intend to prevent the negative impacts of legalisation of proceeds of criminal activity on the legal financial system and entire economy of a country, it is necessary to safeguard the efficient detection of specific crimes involving legalisation of proceeds of crime. In this respect, knowledge of the theoretical basis of detection dealt with in the first part of the paper, which represents specific criminalistic and security activity, is essential. Detection of legalisation of proceeds of crime has specific features that are based on several determinants. One of those determinants is the legalisation indicator that is deeply encoded in the mode used to commit this kind of crimes. The second part of this paper deals with the modus operandi involved in legalisation of proceeds of crime.

Keywords

legalisation of proceeds of criminal activity, crime detection, criminalistic and security activities, crime identification, indicator of legalisation of proceeds of criminal activity

JEL Codes

K14, K34, K42

Abstrakt

Pokud chceme zabránit negativním vlivům legalizace příjmů z trestné činnosti na legální finanční systém a celé hospodářství státu, je zapotřebí zajistit efektivní odhalování konkrétních trestných činů souvisejících s legalizací příjmů z trestné činnosti. K tomu je nevyhnutné poznat samotné teoretické základy odhalování jako specifické kriminalisticko-bezpečnostní činnosti, které jsou obsaženy v první části příspěvku. Odhalování legalizace příjmů z trestné činnosti má však svá specifika, jež vycházejí z vícera determinantů. Jedním z determinantů úspěšného odhalování případů legalizace příjmů z trestné činnosti je samotný indikátor legalizace, který je zakódován ve způsobech páchání tohoto druhu trestné činnosti. Způsobům páchání legalizace příjmů z trestné činnosti je věnována druhá část příspěvku.

Klíčová slova

legalizace příjmů z trestné činnosti, odhalování trestné činnosti, kriminalisticko-bezpečnostní činnosti, rozpoznávání kriminality, indikátor legalizace příjmů z trestné činnosti

Introduction

From the criminalistics point of view, legalisation of proceeds of criminal activity, so-called money laundering, may be defined as a process of the transformation of income obtained through criminal activities into legal assets via a legal financial system. Legal definitions of these terms are contained in international documents dealing with these issues and the legislation of individual countries. In the Slovak Republic, this is Act no. 297/2008 on the prevention of legalisation of proceeds of crime and terrorism financing.

The objective of offenders committing crimes, especially organised crime, is to obtain the income (profit, property) generated through criminal activities. Profit is both the driving force behind criminal activities and their main objective. The effort to benefit regardless of the price and the effort to maximise profit regardless of the means come to the fore. Unlike traditional forms of criminal activity, organised crime very often involves the transfer of proceeds of crime into a legal financial system and its subsequent capitalisation through, for instance, investment into profitable sectors of the economy. The aim is not to consume the profit immediately but to legalise it and secure its growth through subsequent capitalisation. The financial transactions used to incorporate the profit obtained via criminal activities into a legal financial system are mostly not that obvious and they often differ very little from regular transactions. The purpose of legalisation of proceeds of crime is to conceal the origin of the income (property) obtained through criminal activities, its "laundering" via a legal financial system and the subsequent use of such income (property) in a manner indicating that its origin is legal. This means transformation of proceeds of crime into legal assets giving the impression that they have been obtained legally. Each of such cases involves an effort to legalise the income (property) obtained via criminal activities. Legalisation of proceeds of criminal activity represents a substantial aspect of each significant "criminal operation", because the purpose of the majority of crimes is to generate income. Legalisation of proceeds of criminal activity is frequently separated from the original criminal activity, i.e. the crime that has generated the proceeds or served to obtain them, which makes it even harder to detect it. The proceeds of organised criminal activities are often legalised by persons with no criminal history (experts or launderers).

The enormous income generated by organised crime is associated with the task for organised groups and their "launderers" to create the impression of legal character in respect of such income and to create adequate conditions for the incorporation of proceeds of crime into a legal financial system. Handling of the assets obtained through criminal activities and their placement within the financial sector represents a very vulnerable activity as regards possible detection, and therefore "launderers" frequently transform such proceeds into other assets that can be placed within a legal financial system much more easily. This can be done in various ways, e.g. creation of a fictional financial debt or obligation that can be made use of much more easily than cash. All transactions connected with legalisation of proceeds of criminal activity must be executed so that they differ as little as possible from regular business transactions and create the impression of lawfulness, thanks to which their detectability and vulnerability is reduced to a minimum.

Due to the limited extent of this paper it is not possible to deal with all the activities carried out within individual stages of detection that represent a cognitive process focusing on legalisation of proceeds of criminal activity.

The main objective of this paper is to present, in a shortened and simplified form, the theoretical basis for the detection, as a specific cognitive process, of crimes involving legalisation of proceeds of criminal activity. A partial goal is to describe the genesis of methods used to legalise proceeds of criminal activity in order to be able to identify the indicators associated with individual legalisation methods. We will abstract this from other elements of the first stage of detection, i.e. places of occurrence, subjects from which indicators are obtained, and the ways serving to detect indicators.

1 Theoretical basis for crime detection

Basically, crime detection is a process associated with cognitive activities focusing on the detection of latent criminal activities and carried out based on the theoretical and methodological basis of "detection", which may be defined as an operational learning process. When defining the term "crime detection" in the context of the above specification, the characteristics of this activity are substantial and determined by the fact that detection is:

- a cognitive,
- procedural, and
- cyclical

activity working with information.

Detection of offences and crime may be characterised as a purposeful systematic process pursued by state authorities in order to collect, gather, classify, evaluate and analyse information about crime, offences, offenders and victims, to create preconditions for law enforcement bodies to initiate criminal proceedings and bring charges against specific persons. Learning about crime elements may be carried out using the criminalistic and security-related actions that form part of the security activities performed by the police. The security-related activities of the police may be understood as a system of tasks and measures fulfilled and applied by the police and security authorities, specifically criminal investigation, administration, organisation and management in the area of security based on constitutional laws, legislation, other legal regulations and/or international treaties, ethical principles and scientific knowledge. The aim of these activities is to combat crime and other anti-social activities and protect public order, life, health, and property.[1] The security-related activities of the police include criminal investigation, administration, organisational and management activities in the area of security, where the criminal investigation activities are further divided as follows:

- search (linked with persons and items searched for in connection with criminal activities or missing persons)

1 *FILÁK, A. a V. PORADA. Pojem, obsah a hlavní organizačně taktické formy policejně bezpečnostní činnosti. Policajná teória a prax, 2006, č. 4, pp. 5–17.*

- investigation (linked with already registered crime)
- detection (linked with latent criminal activities)[2]

Within the above classification of criminalistic and security-related activities, **search** represents activities aimed at finding specific persons or items who/that exist and may be identified and distinguished from other persons/items of the same kind. A successful search is connected with detention, arresting, bringing in the person or the item searched for, etc.[3] Criminal **investigation** is a process relating to a known and registered crime. This process starts upon the commencement of criminal prosecution and the registration of individual cases via a crime report form completed for the purposes of the statistical registration of detected crimes. In general, **crime detection** is linked with latent criminal activities, not with reported ones. Detection involves activities through which a latent crime becomes obvious. The methodological basis for crime detection is associated with the theory of reflection "because to detect a crime means to establish, discover, and find an act classified by the law as criminal".[4] The learning carried out through the revelation of latent criminal activities basically means the process of collection, analysis and assessment of the information encoded in a specific actual situation that is linked with a criminal activity and its subject (detectable and decodable changes caused by a crime represent traces of the crime). Crime reflection is based on the ability of material systems and items to reflect characteristics of other material systems and items and demonstrate them in another form. The reflected system causes changes in the reflecting system. Such changes show and reproduce, to a certain extent, characteristics of the reflected system. A criminal event is one of the material phenomena of objective reality, and during its course, crime elements and events affect each other mutually, which predominantly means interactions between offenders, the means and tools used by them, the material environment (primarily the crime scene), the subject of the attack and the knowledge of people – witnesses, for instance. Such mutual interactions result in a reflection manifested as changes in the material environment (material traces) and changes in the knowledge of people (memory traces).[5]

From this point of view, detection typically focuses on:

- the offender,
- the subject of the attack,
- the tools used (also financial tools),
- the injured person, and
- a number of other objects.

During an event relevant from the criminalistic point of view, such objects meet, various contacts take place, and information is exchanged. The information transfer may take place at various levels of intensity and the disclosed information does not have to be always detectable by technical or other means. The changes in the environment caused

2 *NESNÍDAL, J. Neodvratnost trestního postihu a operativně pátrací činnost. Praha: Kriminalistický ústav VB, 1989, p. 80*

3 *STIERANKA, J. a kol. Spravodajská činnosť. A PZ Bratislava, 2013, p. 27.*

4 *PORADA, V. Teorie kriminalistických stop a identifikace. Praha: Academia, 1987, pp. 17–24.*

5 *PORADA, V. a J. STRAUS. Kriminalistická stopa. Kriminalistika, č. 3/1999, p. 187.*

by the personality and acts of the offender may be determined based on specific signs (indicators) and their sets. A number of natural relations apply, e.g.:

- interconnections among objects and phenomena within the material world (acts of the offender – their personal features are naturally reflected by the surrounding environment),
- existence of the inevitable relationship between a cause and its effect (a specific phenomenon occurs under specific conditions in one specific way and not otherwise),
- causality – typical processes giving rise to specific changes that should naturally occur upon the existence of analogical conditions,
- unique character and individuality of each manifestation (the opportunity to identify crime indicators is manifested, more or less, as a trend resulting from research; many latent crimes remain undetected) and the possibility to perceive the differences among them, etc.[6]

There is no such event important from the criminalistics point of view during which individual objects would not exchange any information related to them, which means that changes occur naturally in the environment in which the subject (offender) carries out certain activities when committing a crime.

In general, crime detection is identified as actions performed in order to establish the existence of an act that may be classified as a crime and has as yet neither been reported to the police nor registered in police statistics.[7] As concerns its contents, crime detection involves the collection and use of information. Detection may be characterised as a system consisting of structured elements that share one common feature – proactive actions aimed at discovering unknown information characterising an illegal or criminal event. Individual elements have their own specific subjects of detection and unknown pieces of information that are to be detected through such proactive actions.

When defining crime detection, the second important point is that it is **a procedural activity**. Crime detection is not a single action, a single activity, but a process consisting of relatively independent activities and operational actions that are carried out in a certain sequence. We can say that detection is a process within which various activities and operational actions are carried out in a certain sequence and with certain interconnections with their final objective to learn the facts that have been unknown and characterise unlawful activities, a crime or its perpetrator. Detection has the character of **a learning process** – it starts at the point of knowing nothing and ends with a specific piece of knowledge. Primarily, within this process it is necessary to capture the changes caused by a crime, i.e. those to which it has given rise within the relevant environment – to capture signals or indicators of the crime. Subsequently, these indicators are complemented by other pieces of information, focusing on all the aspects and facts of a specific case, which will either confirm or disprove the initial signals of a crime being committed. The

6 *LISOŇ, M. and J. STIERANKA. Organizovaná kriminalita v Slovenskej republike. Bratislava: Akadémia PZ v Bratislave, 2004, p. 95.*

7 *NESNÍDAL, J. Neodvratnost trestního postihu a operativně pátrací činnost. Praha: Kriminalistický ústav VB, 1989, p. 92.*

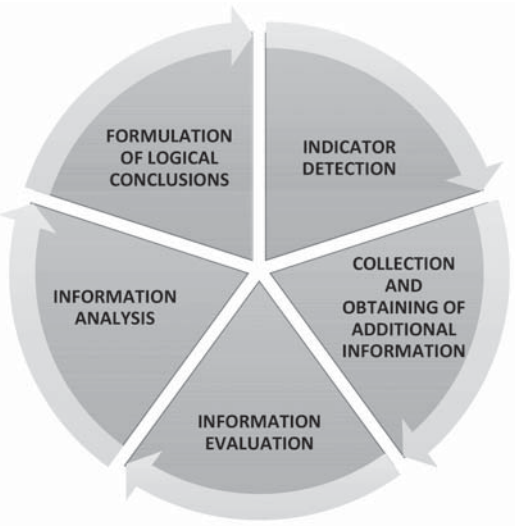
fundamental feature of the detection process is the fact that the detection starts at a point when no investigation is carried out yet based on which a well-grounded suspicion of a crime being committed could be defined because manifestations of such an activity are latent. This type of procedure is part of an extensive strategy of latent crime detection.

Implementation of the entire detection process is conditioned by the detection of an initial signal (indicator) indicating that a crime is being either prepared or committed or has already been committed. Discovery of an indicator determines the further procedure and objectives within the learning and detection processes. If we proceed based on the above defined theory of crime traces and identification, which also includes the process of collecting, analysing and evaluating the information encoded in a specific actual situation, then detection may be characterised as an operational process involving interlinked activities, in particular:

1. obtaining of initial information (a piece of knowledge, indicator, signal) on the preparation, committing or perpetration of a tax evasion or tax crime,
2. collection and obtaining of additional information,
3. information evaluation,
4. information analysis, and
5. formulation of logical conclusions.

The important features of detection, as a learning process, include the fact that it consists of stages and is **cyclic**. Detection, as a process within which the above-specified activities are carried out, is conducted in stages within a cycle. Several detection stages may be carried out simultaneously. Furthermore, within the detection process the learning may return to a previous stage. The process of crime detection is carried out in a similar way as the intelligence cycle. The information cycle forms the basis of both crime detection and intelligence.

Figure 1: Sequence of activities performed within crime detection (information cycle)



Source: authors

Due to the limited extent of this paper, we will focus on one aspect of the first detection stage (determination of indicators), i.e. the ways in which proceeds of criminal activity are legalised

2 Methods of legalisation of proceeds of criminal activity

Detection of crime indicators represents **the first stage of the entire detection process**, which is very important and determines the further steps and development. Therefore, it is necessary to find the indicators that qualify as concerns their "quality" and are able to secure the detection of a crime. **A crime indicator is to be understood as an initial piece of information about a phenomenon or fact that diverts from the normal situation that we are familiar with and means compliance with laws and regulations.** It represents the initial finding concerning a crime that is either being prepared or committed or has already been committed. The term "indicator" is multi-dimensional and this is manifested through possible approaches towards its definition. First of all, it is a piece of information about a certain phenomenon and it initiates the process of gathering knowledge concerning that phenomenon. Similarly, it may be understood as a signal indicating the occurrence of a certain event giving rise to an interest or suspicion on the part of the observer or as "a deviation from the normal situation that we are familiar with and means compliance with laws, regulations, and other social standards".[8] In addition, it may represent a specific external manifestation of a specific phenomenon, which means that we learn about phenomena through their external manifestations. This applies *vice versa* – external manifestations indicate the existence of certain phenomena. We do not always succeed in finding or correctly interpreting the combination of the indicator and the phenomenon that we are looking for. Offenders make use of various legal gaps. Because they carry out activities that are in contradiction with society´s interests, it is only logical that the methods and means used by offenders to achieve their intentions are concealed and frequently also well-worked out. As concerns the general detection methodology, we can state that each action, including a committed crime, leaves some "traces" within its environment, and we may consider such traces to be crime indicators.

Revealing crime indicators, in other words, their detection, is a very demanding activity that represents the first stage of the detection process and requires, *inter alia*, the thorough coordination of activities. When detecting a crime, it is necessary to consider individual elements linked with the detection process, especially:

- crime indicators themselves,
- place of occurrence of indicators,
- subjects from which indicators are obtained,
- ways of finding indicators.

Crime indicators alone represent an important element within crime detection and are contained and "encoded" in the ways in which crimes are committed. Therefore, it is vital

8 LÁTAL, I. Příznaková analýza a možnosti jejího užití v policejní praxi. Kriminalistika, 1996, roč. XXIX, č. 1, p. 73.

to know the modus operandi of specific crimes, including crimes involving legalisation of proceeds of criminal activity.

There are a great number of methods used to legalise proceeds of criminal activity. A legalisation method means the steps taken by an individual or organised group to achieve a goal involving creating an impression of the legal origin of assets obtained through criminal activities. The choice to apply a specific method depends on two factors. **The first factor is defined by the character of the initial crime**, i.e. the crime that served to generate proceeds, and answers as to whether the initial crime was committed by an individual or an organised group, relates to drug crimes, general crimes, economic or financial crimes, and whether the initial crime was simple or highly sophisticated. **The second factor represents the form of assets (proceeds) obtained through criminal activities.** Proceeds in the form of money will be legalised differently from those movable items, real estate, intellectual property, etc. Because of all these aspects, we can state that it is not possible to provide an exhaustive list of methods of legalisation of proceeds of criminal activity. The occurrence of new methods is caused especially by the increasingly sophisticated character of initial crimes and increasing flexibility of "criminal organisations". One reason that cannot be neglected involves new methods of business transaction execution, which are faster and keep on improving through the application of new banking transaction methods. Based on the cases registered until now, we can discuss the following and most frequently used methods of legalisation of proceeds of criminal activity.

2.1 False increase in the turnover of a company using cash

This ranks among the oldest methods of legalisation of proceeds of criminal activity. It is a relatively simple method within which an offender or an organised group owns or otherwise controls a legally existing company in an area within which handling of cash is usual (e.g. services such as coffee shops, accommodation and catering facilities, gaming machines, facilities providing various services, etc.). Even if this method is rather simple, it does not mean that it is easily detectable. On the contrary. This method is applied where the proceeds of criminal activity are in the form of cash (e.g. drug dealing on the streets, procuring, people smuggling, etc.) and such proceeds are subsequently commingled with the legal income generated through the activities of a legally existing company. The process of legalisation of proceeds of crime starts at the point where the cash obtained through criminal activities is deposited into an account of a legally existing company and declared as income generated through the business activities of that company. In another words, this means mingling the legal income of a legitimate company with the proceeds of crimes committed by an organised group. The operator of the company then declares the combined amount as profit and pays the tax. Thus, the proceeds of crime become legal within the first stage and may proceed to the next stage – layering. Mingling of the income obtained through criminal activities with legal income and subsequent declaration of profit means a false increase in the company´s turnover. The profit created in this manner creates an impression of legality and the legally existing company has the reputation of a prospering firm. Thus, the tax authorities do not focus their attention on

the company, because the company is fulfilling its tax obligations. After complying with the tax obligations and payment of the tax on the income generated through criminal activities, such income becomes legal *de facto*. When applying this method, the first stage is the riskiest, i.e. the phase within which the proceeds of criminal activities are deposited into an account. If an organised group does not increase the turnover of a legally existing company to a significant extent, it is more than likely that the tax authority will overlook this form of legalisation of proceeds of criminal activity. A certain disadvantage of this method of legalisation of proceeds of crime is that only a limited amount of such proceeds may be declared, and income tax has to be paid.

Practical example: *Diana, a businesswoman, established and registered the Oak Ltd. company where she was the sole member and owner. The company, registered as an entity developing activities in the timber industry, hired Donna who acted as a business agent. Both Donna and Diana were in fact involved in extensive criminal activities and used the company only as a tool for money laundering. They deposited the capital obtained through criminal activities into the company´s account in cash. Despite the fact that cash transactions in such amounts were not usual in the timber industry, the bank did not report them. As the result of various activities carried out by both women, the Oak Ltd company declared profit amounting to USD 100,000 for the first year of its activities. In February of the next year, Diana died. But her passport remained within the company´s premises. Donna, pretending to be Diana, used her passport and withdrew USD 100,000 in cash from the account. Shortly after this transaction, the bank decided to draw the attention of the Financial Intelligence Unit to the fast growth of the company and high cash withdrawals. After checking the transactions in the account and the register of inhabitants that contained the date of Diana´s death, it was obvious that Donna used the Oak Ltd. company to launder money*.[9]

2.2 False increase in the turnover or profit of a company through excessive invoicing

Within this method, an offender or organised group owns or otherwise controls one or several legally existing companies and through those companies y create an excessive profit. They increase the profit either through supplying goods with a value lower than the invoiced price or they reduce the invoiced price and part of the price is paid outside the books, using income generated through criminal activities. This is conditioned by mutual cooperation between the companies that do business with one another and invoice one another. They are usually aware of the illegal character of such transactions. This legalisation method is mostly used with goods in respect of which it is hard to determine the actual value (e.g. antiquities, artworks, items subject to intellectual property rights, etc.). A modified alternative involves a supplier delivering goods to one company and issuing invoices to two companies, where the second company pays the supplier using income generated through criminal activities and temporarily deposited in the company´s account. In order to hinder information collection, the second company is often registered in another country and its accounts are also kept in that other country. This method means

9 *Finanční zpravodajské jednotky v akci,100 případů Egmontské skupiny, p.12.*

that the supplier makes an increased profit and their accounting records are regular, so there is no reason to suspect them of any unfair practices. The company declares a profit and thus becomes attractive for both business partners and banking institutions. Even when applying this method, problems with the tax authorities may occur if the organised group increases its profit to too high a level.

Practical example 1: *Within a global operation entitled "Green Ice" led by the Drug Enforcement Administration (DEA, USA), it was proven that Italian and Colombian criminal organisations had been using the method of excessive invoicing. A Colombian company was selling leather containers to an Italian customer. The transported containers actually contained leather. The purchase invoice listed top-quality leather, thanks to which a high amount could be invoiced. In practice, the leather had almost no or only a minimal value. In this way it was possible to kill two birds with one stone. The Italians were able to make a settlement with the Colombians in respect of cocaine under the cover of a legal business transaction. On the other hand, thanks to this excessive invoicing, the Colombians made extraordinarily high profits and thus they included their income generated through the sale of cocaine in the legal revenues of the company*.[10]

Practical example 2: *A businessman (client) from Western Europe kept several accounts denominated in foreign currencies with a Swiss bank. The total balance in all accounts amounted to approximately 600,000 Swiss francs. This client, who was also the director of a smaller company in Switzerland, declared that his revenues were generated through fees paid for investment consultancy services. He transferred part of the funds to the USA. Soon afterwards, the bank found out that one of his subordinates had resigned from office because he most likely suspected that the client had been involved in criminal activities. Not long afterwards, the bank received an order to transfer another part of the funds to the USA for the purposes of purchasing a house. But the bank established, in cooperation with the Financial Intelligence Unit, that the client was suspected of a crime (there were no consultancy agreements) and therefore he was trying to transfer the assets abroad in stages. He had already succeeded in transferring part of the assets abroad*.[11]

2.3 Borrowing method

The principle of the borrowing method is based on the fact that the offender or member of an organised group borrows *de facto* their own funds obtained through criminal activities so that neither other entities nor the state authorities are able to check the details of this transaction. This is often a loan from abroad provided by a natural person who is forced, in various ways and for various reasons, to sign a loan agreement. The loan agreement terms and conditions are unusually advantageous for the entity or person to whom the loan is provided. The loan may also be obtained from a legal entity registered in a tax haven. The managing director of such a company is a citizen of that country, authorised to act on behalf of the company, and they provide a loan to the organised group member

10 AKSE, T. A farba je špinavá, Zoetermeer 2003, p.29.

11 AKSE, T. A farba je špinavá, Zoetermeer 2003, p.30.

who legalises illegal proceeds and is the beneficial owner of this so-called "shelf or paper company" within which they have temporarily deposited proceeds of criminal activities. The loan is often repaid through a consideration that is hard to value, e.g. through payments for intellectual and industrial property rights.

Practical example 1: *In 2000, it was established based on reported suspicious transactions from Hong Kong that a Chinese citizen living in the Netherlands received a loan to purchase a Chinese restaurant. The money came from a company account kept in Hong Kong but immediately before that a similar amount had been transferred from Luxembourg to the account in Hong Kong. A deeper investigation was conducted and it was proven that the same Chinese citizen was transferring his own funds generated through criminal activities to the account controlled by him in Luxembourg*.[12]

Practical example 2: *A bank provided a client with credit. The client had already experienced repayment problems in the past. Suddenly, he repaid the credit through a single payment. The client was evasive when asked questions by a bank clerk in respect of the origin of the money. Based on those facts, the bank clerk reported his actions to the Financial Intelligence Unit. Through investigation it was established that the money had been generated through criminal activities*.[13]

2.4 Back-to-back loan

With this type of so-called "back-to-back" loan, a famous banking institution is involved in the loan provision but the institution is not aware of the fact that it is being abused to legalise illegal proceeds. While the borrowing method may be executed absolutely independently, this type of loan requires the engagement of a bank or other provider of financial services that provides loans only against adequate security. Loan security provided by a financial institution to members of an organised group legalising illegal proceeds is created by another company that deposits cash and is seemingly not connected with the company receiving the loan, but in fact, it is controlled by the organised group. The advantage of this method of legalisation of proceeds of criminal activity is that a renowned financial institution is engaged in the legalisation process, thus making the entire process look trustworthy.

Practical example: *An investigation carried out by the investigation unit in the Rotterdam-Rijnmond region showed that credit had been arranged by an attorney of a Swiss bank for a client who was involved in cocaine trafficking in the Netherlands. An amount of four million guilders deposited in a deposit account was used as security. The credit was used to finance a legal business belonging to the cocaine trafficker. The funds came in cash to the Netherlands and were deposited in cash into the deposit account. Thus, everyone could see the actual credit provided by the bank but not the security*.[14]

12 AKSE, T. A farba je špinavá, Zoetermeer 2003, p.57.

13 AKSE, T. A farba je špinavá, Zoetermeer 2003, p.57.

14 AKSE, T. A farba je špinavá, Zoetermeer 2003, p.62.

2.5 False winnings

This method of legalisation of proceeds of criminal activity is based on the following: an offender or a member of an organised group comes to a casino along with other persons from the same group and they purchase chips paying either in cash, via a cheque or credit cards. They play low stakes at tables and create the impression that they are three independent players who do not know each other, to prevent any suspicion. Players do not play actively and to a great extent because they want to preserve as high as possible an amount for legalisation. After some time, all the players give their chips to one of them and the person goes to the cash desk to exchange them for cash or asks to deposit the cash into an account while pretending that it is winnings. The majority of casinos offer the opportunity to open a deposit account for clients in which clients deposit their winnings and are able to place orders with the casino for wire transfers thanks to which funds may be relocated in a short time. Of course, this is possible provided that the casino is private, the state supervision is benevolent, and the internal supervision fails to detect the false winnings. In this way, the proceeds of criminal activity may be legalised only when there is a sufficient period of time, because if the casino finds that a player wins too often, the risk of detection increases. Moreover, some casinos check the provability of high winnings. If the player fails to prove that they have won, the casino refuses a transfer to a deposit account and asks the player to take the winnings in cash. Technical equipment and administrative means allow reverse determination and checking whether winnings are fake or not. Another form applied within lotteries and similar games is the purchase of the prize from the actual winner, who receives a "commission".

Gambling via the Internet **using player accounts** represents a new method of legalisation of proceeds of crime. Player accounts execute mutually interlinked transactions, the aim of which is to legalise illegal proceeds. This scheme of transactions among player accounts allows player accounts to be used to create a legal framework for transactions, with the funds coming through anonymous payment channels without their origin being proved. Subsequently, the funds are transferred into the bank accounts of player account holders. The typical signs of this legalisation method include:

- creation of two-player accounts pretending that these are two different persons as the rules require,
- use of player accounts by persons other than those who opened/registered the accounts; in online gambling, the same IP address is used and one player plays in favour of the other player and this even at their own expense,
- organised use of player accounts associated with the risk that the final beneficiaries, as concerns player accounts and participation in gambling, are not the players under the names of which player accounts are registered but other unknown persons, or at least one the players is such a person,
- funds are deposited to player accounts through the PAY SAFE CARD payment channel for instance, i.e. via prepaid cards that may be purchased without customer identification in shopping centres, gas stations in the SR and abroad, and via the Internet,
- organised participation of several persons in gambling who violate the relevant game rules and gambling ethics, do not play against another but in accord so that one person loses in favour of the other,

- the player gives up/throws their hand in within a gambling game despite the fact that there is a high probability of winning and thus secures winnings for the other player,
- the result of participation in a gambling game is usually winnings that equal the deposited amount, and the players act systematically so that the deposited amount returns regardless of the probability of winning. Even if the probability of winning is high, they give up the chance of winning and proceed so that the deposited amount returns with certainty,
- payment of winnings to a bank account.

Practical example 1: *Roland worked as a secret agent within a police investigation focusing on money laundering in casinos. During the investigation, Roland was introduced to Theodor who lived in the same country as Roland. Theodor claimed that he was a casino employee in a neighbouring country and offered Roland the opportunity to launder money. He claimed that it would be very simple, because he was employed by the casino. If Roland gave him cash, Theodor would give him a casino receipt amounting to the same value as the cash provided by Roland, reduced by Theodor´s commission. Roland would be able to claim that he had won the money in the casino and the police would not be able to disprove it. Furthermore, the casino would know nothing about the transaction because it will seem that Roland had won the majority of the deposited money back. Roland wanted to get more information about the money laundering method and therefore accepted Theodor´s proposal. Following Theodor´s instructions, he deposited 25,000 dollars in cash into the casino´s account. In return, he received a receipt for the same amount reduced by Theodor´s commission amounting to 9%. The commission was divided among Theodor and Armin, the man who introduced Theodor to Roland. The first transaction was executed without any problems – Theodor laundered money for Roland as he had promised. But he did not know that the 25,000 dollars that he laundered was not illegal money, but money provided by the police authority for which Roland worked. Soon afterwards, Roland contacted Theodor again and asked him to execute a similar transaction but this time it was supposed to amount to 500,000 dollars. Theodor was happy to help him again but during the transaction the police arrested him for a crime involving money laundering*.[15]

Practical example 2: *The Financial Intelligence Unit received simultaneously from two obliged entities – Bank A and Bank B – reports on unusual business transactions involving the personal accounts of Person X, Person Y, and Person Z. Specifically, the transactions included recurring payments credited either personally in cash or transferred in smaller amounts to accounts of those persons, which were followed by cash withdrawals from the accounts kept in Bank A and Bank B.*

A detailed analysis of the data and information contained in both reports showed that the personal accounts of Persons X, Y, and Z were credited with funds in cash and/or via transfers in tens of euros with payment descriptions indicating that those funds represented various winnings of material or financial nature obtained through a competition run via Facebook. The pieces of information from the payment reports relating to the competition were partially confirmed by the information from the Facebook profile of the Police Force of the SR where the

15 Finanční zpravodajské jednotky v akci,100 případů Egmontské skupiny, p.37.

police drew attention to the Facebook site with the competition and warned that it was a fraud. Within the competition, the persons interested in offered winnings – material prizes – executed payments that conditioned the winning of the prize; the account holders were Persons X, Y, and Z, i.e. the persons who organised the competition but never handed over any prizes. Based on the reports, it was established that the funds in the accounts of Persons X, Y, and Z consisted mostly of cash deposits made by various persons and transfers from the account of a company organising lotteries and other gambling games in the SR (a "betting company"). The modus operandi of the fraudulent obtaining of funds from persons interested in the competition was based on the fact that the interested person could win various items as prizes after giving a "like" to the competition page and sharing it. After giving a "like", the interested person was called upon via the Messenger application to pay a handling fee or postal fee amounting to up to 10 euros. Where the interested person had a prepaid mobile phone programme from Mobile Operator M, they received a message via Messenger saying that they had a chance to win if they sent a message via Messenger to the account administrator. After sending such a message, the interested person received a reply with information about the prize and the request to send a confirming SMS to the short number 3,000 within 5 minutes. Payments from such confirming SMS subject to fees were subsequently transferred to the accounts of Persons X, Y and Z kept by the betting company, but the person interested in the prize was not aware of that. The accounts of Persons X, Y, and Z were credited in this way in fact. When the person interested in the competition/prize did not have a mobile phone programme from Operator M, the interested person was informed via Messenger that they should pay a handling fee via a transfer or through a cash deposit to one of the accounts of Persons X, Y, and Z from which those persons were withdrawing cash subsequently. Persons X, Y, and Z proceeded jointly and most likely, they knew each other because mutual transfers of funds generated via the incriminated competition were identified among their accounts and they had permanent residence in the same city in the Slovak Republic.

Within an analysis of the data from both reports it was established that Persons X, Y, and Z acquired funds amounting to at least 9,000 euros in this manner. The Financial Intelligence Unit referred the information to the competent investigating officer.[16]

2.6 International money transfers

This method of legalisation of proceeds of criminal activity is based on the existence of organisations that offer international money transfers and provide the opportunity to transfer cash to anywhere in the world. The advantages of this method include the speed at which funds are relocated. Because the contact between the sender and the institution arranging international money transfers is only temporary, unlike in the case of banks, the use of forged identity documents is much simpler. The advantage is that there is no "accounting track", i.e. a trail based on which it would be possible to establish further movements of money, because the money is deposited in cash and then withdrawn in cash as well. The disadvantages include the limit on the amount that may be transferred. Those limits differ by institutions and countries subject to the legislation concerning unusual

16 Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2017.

transaction reporting. In the majority of countries, amounts exceeding EUR 10,000 cannot be sent, which necessitates the use of the services and activities of hired and usually irreproachable senders and couriers, so-called "smurfs". Such steps may be established only based on long-term monitoring of deposits and transactions and identification of regular elements within them.

In the Slovak Republic, this service is offered by Western Union, a global company, through various agents such as banks, post offices, etc. Transactions within the Western Union system are carried out at the rates defined by Western Union independently from the rates determined by the bank through which money transfers are available and independently from the rate determined by the National Bank of Slovakia. The daily limit is 10,000 US dollars. The limit for one transaction is 5,000 US dollars. Within a few minutes of depositing funds within the system, the money may be withdrawn practically anywhere in the world, because this international money transfer service has representation in 150 countries of the world in more than 150,000 cities. Money transfer may be abused to legalise proceeds of criminal activity because it allows the preservation of anonymity to a great extent of both the sender and the recipient due to the fact that the transaction is carried out with no bank accounts involved and sometimes an identity document is not even required. The sender of funds is asked to provide their name, surname, address, and telephone number and the amount that they wish to send. No other data is required, which means that the financial profile of the client is not subject to any examination that might reveal whether it is realistic for the client to send such an amount of money. In the end section of the relevant form serving to send funds, there is a question asking whether the recipient will have a valid identity document upon acceptance of the funds. If the sender enters NO, the sender and the recipient agree a password based on which the transfer is executed. This means that the recipient is absolutely protected against being identified.

Practical example: *An investigation of a criminal grouping exporting ecstasy to England commenced in Utrecht, the Netherlands. After delivery of the drug, persons were detained in both England and the Netherlands. The investigation revealed that the payment for ecstasy was supposed to be executed at a certain time and was supposed to amount to GBP 30,000 (approximately EUR 45,000). Through telephone tapping it was established that no transfer mode had been agreed yet. Finally, the payment was divided into ten money transfers that were to arrive to the Netherlands via a well-known money transfer system with branches in England and the Netherlands. The transfers were executed and amounts ranging from GBP 1,000 to 4,000 were transferred. In England, the money was deposited in favour of a member of the criminal group in the Netherlands and then withdrawn in the Netherlands*.[17]

2.7 Bank cheques, bills of exchange, letters of credit, capital deposits

Bank cheques and bills of exchange serve as tools within the process of legalisation of proceeds of criminal activity, especially within the second stage of legalisation,

17 AKSE, T. A farba je špinavá, Zoetermeer 2003, p.41.

i.e. the layering of illegal proceeds. Three types of bank cheques may be used within legalisation: the first is a personal cheque where the amount stated on the cheque may be paid only to the person whose name is stated therein. A cheque to order represents another type where the person presenting the cheque may transfer the amount in favour of any person. Bearer cheques represent a popular alternative for legalisation as well – a bearer cheque does not contain the recipient´s name and thus secures anonymity. The cheque is paid out to the person presenting it. The advantage of using cheques within the process of legalisation of proceeds of crime is that they may even be purchased from a financial institution by a person who is not a client of that institution and there is no limit to the number of purchased cheques. Cheques may be purchased for cash as well. Organised groups prefer bearer cheques or cheques to order within the legalisation process where anyone can be a recipient. The great advantage is that there is no need to apply conversion because if they buy cheques for dollars, someone else can have them paid out in euros. A certain disadvantage is that cheques leave "traces" in banking documentation through which it is possible to establish to whom the funds have been transferred via endorsed cheques (cheques to order). The cheque remains with the bank used by the person delivering it for payment. The time-consuming updating of accounts represents another disadvantage. Updating is the process carried out by two financial institutions (two branches of the same institution or two different banks) where the bank to which a cheque has been submitted for payment asks the bank that sent the cheque for settlement. Within this settlement, the relevant amount is transferred to the account kept by the bank to which the cheque was presented. The account is used to pay the person who has presented the cheque. Updating may take several days when it comes to international transfers and this represents the risk to the organising group of the possible seizure of the funds.

Practical example 1: *A married couple from another European country opened a savings account with a Dutch bank. One spouse was an employee of a commercial bank in their home country where he worked with letters of credit featuring high amounts on a daily basis. Making use of the experience, he opened a false standby letter of credit amounting to USD 500,000 in the name of his wife and subsequently sent the money to the savings account in the Netherlands. After crediting the amount to their account, they executed several wire transfers to another account of theirs and third-party accounts. Since this activity did not comply with their usual transactions involving a similar type of account, the commercial bank reported their case to the Financial Intelligence Unit. The subsequent investigation carried out with international cooperation revealed that the husband was already suspected of carrying out criminal activity in his country – bankruptcy fraud and embezzlement*.

Practical example 2: *A client opened an account with a bank in order to establish a joint-stock company. At the same time, he stated that funds amounting to USD 100,000 would be transferred to that account. The bank already knew the client´s history, describing him as an unreliable and indebted person. The advised funds were transferred to the account from an Eastern European country. After 8 days, the client asked to withdraw USD 50,000 in cash from his account. The bank did not pay the money to the client and reported the transaction to the Financial Intelligence Unit. The Unit established that the client had similar accounts with other banks as well. Further investigation revealed that the client had connections with the underworld and the money had been generated through crimes involving prostitution*.

Practical example 3: *In a case involving 2,200 kg of cocaine mixed with charcoal investigated by the police in the Netherlands, a certain number of cheques were issued by the cooperating administration office. An account was opened with a Belgian bank for a company from Aruba of the AVV type and the proceeds from the sale of drugs were deposited into this account. After a deposit, blank bearer cheques were drawn up in respect of the account and forwarded to a Colombian organisation. After endorsement, the cheques were paid out in favour of accounts in Panama. The administration office used two companies of the AVV type represented in Aruba by a trust company. The companies provided a cover for this structure and the companies´ accounts served to execute a number of transactions. Payments were officially executed against delivered goods but in fact, they paid for supplied cocaine*.[18]

2.8 Real estate transactions

This method makes use of the purchase of immovables to legalise proceeds of criminal activity. Immovables represent one of the most attractive investments. Investing in immovables is nothing unusual when it comes to foreign companies, because real estate prices are quite stable and in addition often secure an increase. The second advantage of investments into immovables is that they usually have very high values and thus the proceeds of criminal activities may be legalised in high amounts and repeatedly. This legalisation method may be applied in several ways. The first is based on purchase of immovables using the borrowing method. The second option is the self-lease of immovables via companies domiciled in tax havens. Another possibility is to purchase neglected immovables and renovate them using the proceeds of criminal activities. The next step involves the sale of the renovated property for a significantly higher price. The profit obtained through the sale represents a legalised amount. The most complex alternative of this real estate transaction method is the so-called "A-B-C-D structure". It is based on the existence of several companies controlled by an organised criminal grouping. The sale of immovables among the companies is carried out as follows: Company A purchases a piece of real estate using the borrowing method and subsequently sells it for an increased price to Company B, Company B sells the property again for an increased price to Company C but for a short time only. Company C sells the property to Company D but the property is already overpriced. The legalised income is, in this case, represented by the profits achieved through the sale transactions executed by the companies while as early as the purchase using the borrowing method, part of the illegal proceeds are legalised. Subsequently, the property's owners may have legal income thanks to leasing it.

Practical example 1: *A client opened an account with a medium-sized bank. He informed the bank employees that the money that would be deposited to his account would be commission for the sale of real estate situated on Caribbean islands. A significant amount of money accrued in the account over two years. After some time, the client requested immediate cancellation of his account and transfer of funds to another bank. The bank asked the client to provide a more detailed explanation and to submit brokerage contracts. The submitted contracts were drawn up unprofessionally and the bank found out that his other explanations were also untrue.*

18 AKSE, T. A farba je špinavá, Zoetermeer 2003, p. 91.

Therefore, the bank reported the client to the Financial Intelligence Unit, which established that the money transferred to the account kept with the bank had originated from land frauds.

Practical example 2: *A Pakistani organisation was interested in purchasing a hotel in the Netherlands. Using both regular bank transfers and illegal transfers, money was transferred from Pakistan to a bank to finance the purchase of the hotel. The Pakistani organisation claimed that family capital based in Pakistan served as the source. The investigation revealed that after the transaction, the investment was repaid using proceeds of criminal activities. The investors in Pakistan received back their funds along with an interesting profit. A very short time elapsed between the investment and its repayment*. [19]

Practical example 3: *The Financial Intelligence Unit received a report from an obliged entity – Bank A – on an unusual business transaction involving repeated wire transfers between the business accounts of Companies A and B in respect of which Bank A deemed especially the repeated transfers between their business accounts to be suspicious*.

Immediately after receiving the report on unusual business transactions ("UBT") from Bank A, the Financial Intelligence Unit received a UBT report from another obliged entity – Bank B – on unusual business transactions concerning the personal account of the statutory representative of Company B, where Bank B deemed to be unusual the combination of those transactions with cashless payments deposited into Account 2 belonging to Company B. From open sources it was established that Companies A and B had participated in a voluntary auction, i.e. Company A as the auctioneer, and Company B as the party that initiated the auction and participated in it. The auction involved lucrative immovables. Analysis of the data from both UBT reports revealed that funds had been transferred repeatedly and several times between the accounts of Company A and Company B, involving identical amounts ranging from EUR 400,000 to EUR 500,000 and those transfers resulted in an overall turnover amounting to EUR 2,000,000 in the account of Company A and EUR 2,000,000 in the account of Company B; the payments from Company B to Company A were declared as settlement of the "price achieved through bidding" and payments from Company A to Company B were declared as settlement of the "auction proceeds". In this manner, turnover amounting to EUR 2,000,000 was seemingly achieved in the account of Company A and this represented the total amount received for the immovables subject to auctioning.

From open sources it was established that in this case Company B acted as the pledgee and the party initiating the auction and simultaneously as the sole bidder within the auction where Company B actually purchased immovables through bidding. The pledge over the immovables subject to the auction was registered in favour of Company B. An expert opinion determined the value of the real estate pieces as EUR 4,000,000. Subsequently, after the unsuccessful first auction round, a second round was announced, but the value of the subject-matter of the auction, the real estate, was reduced to EUR 2,000,000 exactly 50% of the value of the real estate subject to the auction.

Within the initial analysis it was not possible to determine the origin of the funds used within the described scheme and their further flow because at the beginning and end of the scheme

19 AKSE, T. A farba je špinavá, Zoetermeer 2003, p. 117.

involving the above-specified repeated transfers, the cash deposits and withdrawals were executed by the statutory representative of Company B.

In both UBT cases, the contents of which were interrelated, the established facts indicated that the auction might have been manipulated by Companies A and B to obtain a property for a price that did not reflect its market value and it might have been accompanied by causing an injury to the property owner because the owner pledged the property in favour of Company B most likely with a value corresponding to the expert opinion.[20]

2.9 CEO transactions

The mechanism of so-called CEO frauds is based on attacks against email communication among business partners concerning standard payments between them in order to re-route the payments to an account prepared in advance. Such an account is usually opened with a bank domiciled in a country other than the country in which the account of the payer or business partner is situated. The business partner paying for goods is informed about the change in the payment details of their business partner via a fake email message, the data of which seem to be highly authentic. Such emails are sent from someone pretending to be the business partner notifying a change of the account that serves to settle business deals due to various technical or organisational changes, or by someone who is seemingly part of the business partner´s organisational structure. Competent representatives are informed about the change of the business partner´s account and most likely at this level no thorough checking or verification of accounting data is carried out. After a payment is executed by the business partner to the account that has been opened and prepared by the offender, the funds are usually transferred almost immediately after their crediting to:

- other accounts prepared by the offender and kept with banks domiciled in offshore countries or countries with more problematic enforcement of law, e.g. Nigeria, Ghana, China, Hong Kong,
- accounts kept with banks domiciled in Great Britain where there are indicators that the accounts were opened for the persons who have been granted asylum within third-country inhabitants´ migration to Great Britain and are used by offenders as so-called dummies.

Practical example 1: *The Financial Intelligence Unit in the SR received a report from an obliged entity (Bank A) on an unusual business transaction involving two fraudulent payments from abroad, from the foreign business entity X in France, using two foreign accounts; the transfers amounted to approximately EUR 320,000 and EUR 140,000 respectively. Both these transfers from abroad amounting to EUR 460,000 in total were credited to the same account kept with Bank A for Company S. Company S was domiciled in the Czech Republic and its statutory representative and managing clerk with access to the account of Company S kept with Bank A was a French citizen ("Representative of Company S"). The foreign bank requested the return of the funds to the foreign account of the owner of Company X due to fraud and sent Bank A the criminal complaint filed in France by the injured party – Company X. An analysis*

20 Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2017.

of the unusual business transaction report revealed that the above payments from abroad were executed from foreign accounts through so-called CEO fraud, i.e. the electronic business communication of the holder of foreign accounts of Company X was "hacked" and original payments were re-routed to an incorrect account belonging to Company S. By comparing the invoices sent electronically to Bank A by the Representative of Company S in order to release the funds from the account of Company S, it was established that both invoices share a simple graphic form that does not make them trustworthy and were supposedly drawn up in order to document two payments from abroad to Bank A. The supplier data in both invoices of Company S did not comply with the data concerning the recipient of foreign payments stated in SWIFT messages – the data was only similar, which is one of the main indicators of CEO frauds. Based on those facts, Bank A assessed the situation as the intention of the Representative of Company S to use the funds in the account, suspended the unusual business transaction, and submitted the information to the investigating officer of the Police Force. The Prosecutor's Office seized the funds in the account of Company S, amounting to EUR 450,000.[21]

Practical example 2: *The Financial Intelligence Unit in the SR received from an obliged entity (Bank A) an unusual business operation report concerning a payment from abroad amounting to EUR 1,400,000 which was executed from an account in Chile belonging to a local company. The amount had been transferred in a fraudulent manner into the account kept by Bank A for Czech company X. After crediting the funds amounting to EUR 1,400,000 from abroad to the account of Czech company X, two urgent wire transfers to another country were executed from the account – EUR 150,000 and EUR 20,000 were transferred to two accounts in a bank in Poland. Furthermore, Bank A received from a foreign corresponding bank the first SWIFT report requesting the return of the payment amounting to EUR 1,400,000 transferred from Chile to the account of Czech company X. The Chilean bank stated that the Chilean company had fallen prey to so-called CEO fraud. Subsequently, Bank A applied technical measures to the account of Czech company X to prepare for possible seizure due to an unusual business transaction under Sec. 16 of the Act on prevention of legalisation of proceeds of criminal activity in order to prevent further use of the account balance. The FIU immediately informed its partner – the Financial Intelligence Unit in Poland – about the two above-specified payments amounting to EUR 170,000 in total transferred to two Polish accounts based on a CEO fraud. Immediately after sending the information, both payments were returned from the Polish accounts back to the account of Czech Company X kept with Bank A. Subsequently, the Financial Intelligence Unit forwarded the information to the investigating officer of the Police Force and the Prosecutor´s Office seized the funds amounting to EUR 1,400,000 that remained in the account of Czech company X.*[22]

Practical example 3: *The Financial Intelligence Unit in the SR obtained, within international cooperation with a partnering foreign financial intelligence unit, information on the accounts kept by a French bank for Company A domiciled in France because funds accumulated in those accounts in a short time from several cases involving most likely fraudulent re-routing of payments (so-called CEO fraud) amounting to EUR 2,500,000 in total. The funds were supposed to be legalised as proceeds of criminal activity so were to be layered in parts and integrated via a network of bank accounts already opened in several European countries. In*

21 *Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2017.*

22 *Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2017.*

cooperation with all the banks in Slovakia, the Financial Intelligence Unit in the SR checked Companies B and C, with a special focus on the accounts kept by those two companies in banks in the SR. Subsequently, it was established that one of the banks seated in the SR maintained accounts for both Companies B and C which were newly opened accounts X and Y in respect of which there was no history of previous transactions. Based on the above-established facts, the Financial Intelligence Unit initiated measures in the bank involving monitoring accounts X and Y. Subsequently, the bank recorded a foreign payment from France credited to monitored account YouTube amounting to over EUR 670,000. The Financial Intelligence Unit, in cooperation with the obliged entity, blocked this unusual business transaction in compliance with the Anti-Money Laundering Act and seized the funds. The competent French authorities asked the SR for legal assistance in this case.[23]

Practical example 4: *Funds amounting to almost EUR 460,000 were transferred via three payments to the account of Company A – a Slovak legal entity acting through a Spanish citizen, from an account of a Slovak governmental institution. As was established later, the Slovak governmental organisation had executed the payments based on an email message in which their business partner informed them of change of bank account and asked them to send all future payments to the new account. After transferring the above funds, the Slovak governmental organisation established that the account to which they had transferred the funds did not belong to their business partner who had allegedly notified them about the change of account but was kept with a bank in Slovakia for Company A which had only pretended to be their business partner. The entire transaction was executed by Company A in a very sophisticated way and was preceded by precise preparation which was evidenced by a number of accounts that had been prepared for that purpose in advance in order to make it as hard as possible to seize the funds. Immediately after the governmental organisation credited the funds in favour of the company´s account, Company A executed transfers of several smaller amounts to already prepared accounts – an account of Slovak company B acting through the same Spanish citizen as Company A and another three personal accounts that he had opened for this purpose with banks in the Czech Republic.*

Thanks to the prompt cooperation of the Financial Intelligence Unit with the Slovak bank that kept accounts for Companies A and B and cooperation with the Czech Republic, almost all the funds amounting to EUR 460,000 were seized in accounts in Slovakia and the Czech Republic.[24]

2.10 Identity theft (use of identification documents, payment cards, skimming, phishing)

The mechanism of this method is based on the abuse of identification documents, especially documents confirming the identity of natural persons, and abuse of payment cards. Offenders legalising proceeds of criminal activity open accounts with banks using stolen or forged documents and use such accounts to transfer the funds generated through various criminal activities. Funds are transferred from such accounts via Internet banking

23 Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2016.

24 Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2015.

to other accounts from which they are withdrawn mostly via ATMs using payment cards. To prevent verification procedures, an international element is used – cash withdrawals from ATMs abroad or transfers of funds to accounts opened abroad.

Practical example 1: *Based on an unusual business transaction report, the Financial Intelligence Unit in the SR launched an investigation concerning the account of a non-profit organisation domiciled in Slovakia and unusual business transactions executed using its account kept with a bank in Slovakia. In this case, it was established that higher amounts had been credited to the relatively new account of the non-profit organisation represented by a foreigner – an EU citizen – and those payments had been executed via a POS terminal leased to the non-profit organisation upon opening the account. For three months, the POS terminal served for payments with foreign payment cards, amounting to more than 400,000 euros. After crediting funds, the managing clerk authorised to use the account executed 45 wire transfers to various accounts abroad, amounting to more than 240,000 euros, and 60 cash withdrawals were made via ATMs abroad, amounting in total to more than 24,000 euros. Smaller amounts paid via payment cards abroad were recorded as payments for goods or services. The total amount of transferred funds withdrawn via ATMs amounted to more than 270,000 euros. Further investigation revealed that unknown persons copied at least 21 payment cards into a device that saves such information, so-called skimming, and, using the POS terminal leased by the non-profit organisation in connection with the account, abused the copied card data and credited the account of the non-profit organisation. Subsequently, the bank received 61 requests (complaints) from various card companies requesting them to check payments transferred to the account of the non-profit organisation, which amounted to more than 160,000 euros, since the holders of those cards had not executed any financial transactions via the POS terminal. The bank contacted the client repeatedly and requested documentation concerning the transactions subject to these complaints and submission of documents based on which the payments had been executed, but the representative of the non-profit organisation did not communicate with the bank at all. When the bank established that various payment cards issued abroad had been abused, the balance in the account of the non-profit organisation amounted to approximately EUR 136,000. In cooperation with the bank, the Financial Intelligence Unit seized the funds in the account of the non-profit organisation in compliance with the Anti-Money Laundering Act and referred the case immediately to the investigating officer of the Police Force. Because as of the date of account blocking, further fraudulently obtained funds were credited to the account of the non-profit organisation, the total balance seized for the purposes of criminal proceedings amounted to more than 200,000 euros. The investigating officer of the Bratislava Regional Investigation Bureau of the Police Force commenced a criminal prosecution procedure dealing with the case of especially serious crime involving legalisation of proceeds of criminal activity*.[25]

Practical example 2: *Within a case involving several coordinated phishing attacks against bank accounts of smaller Slovak municipalities, funds were transferred from their bank accounts to several personal accounts prepared in advance from which they were withdrawn in cash via ATMs abroad, using payment cards or transferred to other already prepared*

25 Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2016.

accounts abroad. Those cases demonstrated identical elements indicating that it is most likely they were coordinated (phishing). The identical signs were the following ones:

- *all phishing attacks were targeted at accounts of smaller Slovak municipalities,*
- *all attacked accounts were kept with the same bank,*
- *all accounts to which funds were transferred after phishing, i.e. the funds generated through criminal activities, were kept with another bank in Slovakia,*
- *in all phishing cases, the accounts that served to deposit the illegal proceeds were held by the same persons*.[26]

Practical example 3: *In 2011, the Financial Intelligence Unit in the SR recorded a case involving the abuse of POS terminals through which 1 665 unauthorised payments of smaller amounts were executed at various vendors in the USA within two days. The transactions were unauthorised offline transactions – declared as so-called "returned goods", using VISA and MASTER CARD payment cards. The funds were credited to two accounts held by a company domiciled in the SR. Transactions of this type (return of goods) are executed when a client returns the goods for which they have already paid the vendor using a payment card and the client files complaints about the goods. In this case, no payments for purchase of goods from specific vendors in the USA had been executed. After crediting the funds coming from abroad to the company´s accounts, the managing clerk authorised to use the account tried to withdraw the funds in cash. Since the Financial Intelligence Unit already had information on similar activities by the managing director and members of his family in the past, the Unit blocked the transaction, and after the case was referred to the investigating officer, the Prosecutor seized the funds in the account. This case was interesting in regard to the preparation for the crime. The offenders found a socially vulnerable homeless person in advance and appointed them as a managing director of a company; subsequently, they opened bank accounts for that company in order to transfer the funds generated through criminal activities committed abroad which they wanted to legalise. The company´s managing director was supposed to pretend to undertake regular business activities, e.g. transfer payments from foreign customers for goods and services. Subsequently, he was to execute cash withdrawals in order to conceal the origin of the funds generated through criminal activities and thus hinder their seizure for the purposes of criminal proceedings. The company´s account was opened immediately before executing the fraudulent payments and no other business transactions were executed except for those during that period of time, which only confirms the fact that it was a criminal activity planned in advance. The company´s managing director was not able to provide bank employees with any explanation as to the origin of the funds credited to the company´s account. In total, 1,665 payments were executed using payment cards amounting to approximately 317,000 euros*.[27]

Practical example 4: *The Financial Intelligence Unit received an unusual business transaction report concerning the opening of several accounts with Bank A based on forged authorisations and personal identification documents; those accounts were subsequently used to obtain credit from Bank A for several natural persons. After analysing the relevant data, the Financial Intelligence Unit established that Bank A had opened at least eight personal accounts for various natural persons – some of the accounts were opened via a courier service without any*

---

26 Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2014.

27 Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2011.

authorisation and some were opened through employees of Bank A, who opened them outside the branch of Bank A based on the identification of a person using a personal identification document. Immediately after opening the accounts, their holders applied via Bank A's Internet banking application for credit amounting to EUR 150,000 in total. After the credit had been provided and transferred to the newly opened accounts, funds amounting to EUR 130,000 were transferred from the accounts to one account which had also been opened by employees of Bank A outside the branch of Bank A based on an authorisation. The funds generated through the credit agreements were gradually withdrawn via ATMs up to EUR 120,000. Later, Bank A found out that the data in the personal identification documents was not correct and the documents and authorisations had not been notarised, which gave rise to the suspicion that the case involved a cooperating group of unknown persons who solicited funds amounting to a total of EUR 150,000 from Bank A in a fraudulent manner and under false identities.[28]

3 Conclusions

In addition to the legalisation indicators encoded in criminal activities, other elements such as the place where the indicator occurs, the subjects associated with the indicators, and the manner in which the indicators are obtained also play an important role within the first phase of the detection of legalisation of illegal proceeds. The places where the legalisation of proceeds of criminal activities can be detected depend on the specific manner of the legalisation and the means (financial and business tools) used within the legalisation. In the majority of cases, it is the financial market, capital market, insurance market, real estate market, etc. As concerns the place where indicators occur, an important role is played by the entities present within such markets, the tasks and legal competencies of which include the detection of possible cases involving legalisation of proceeds of criminal activity. Any deviations from regular business and financial transactions represent indicators of legalisation of proceeds of criminal activity, and the Slovak legislation in the area of legalisation prevention defines them as unusual business transactions.

References

AKSE, T. (2003) *A farba je špinavá*. Zoetermeer.

FILÁK, A. a V. PORADA (2006) Pojem, obsah a hlavní organizačne taktické formy policejně bezpečnostní činnosti. (The term, contents, and main organisational and tactical forms of the security related activities of the Police). *Policajná teória a prax*, 2006, č. 4.

Finanční zpravodajské jednotky v akci, 100 případů Egmontské skupiny (2000) Publikace pro edukační účely pracovníků zpravodajských jednotek, další údaje neuvedeny.

LÁTAL, I. Příznaková analýza a možnosti jejího užití v policejní praxi. *Kriminalistika*, 1996, roč. XXIX, č. 1.

LISOŇ, M. a J. STIERANKA (2004) *Organizovaná kriminalita v Slovenskej republike*. Bratislava: Akadémia PZ v Bratislave.

28 Výročná správa finančnej spravodajskej jednotky Prezídia PZ v SR za rok 2011.

NESNÍDAL, J. (1989) *Neodvratnost trestního postihu a operativně pátrací činnost*. Praha: Kriminalistický ústav VB.

PORADA, V. (1987) *Teorie kriminalistických stop a identifikace*. (Theory of crime traces and identification) Praha: Academia

PORADA, V. a J. STRAUS (1999) Kriminalistická stopa. (Crime trace) *Kriminalistika*, 1996, roč. 3/1999

PREZÍDIUM POLICAJNÉHO ZBORU SR (2017). *Výročná správa finančnej spravodajskej jednotky Prezídia PZ v Slovenskej republike za rok 2017*.

PREZÍDIUM POLICAJNÉHO ZBORU SR (2016). *Výročná správa finančnej spravodajskej jednotky Prezídia PZ v Slovenskej republike za rok 2016*.

PREZÍDIUM POLICAJNÉHO ZBORU SR (2015). *Výročná správa finančnej spravodajskej jednotky Prezídia PZ v Slovenskej republike za rok 2015*.

PREZÍDIUM POLICAJNÉHO ZBORU SR (2014). *Výročná správa finančnej spravodajskej jednotky Prezídia PZ v Slovenskej republike za rok 2014*.

PREZÍDIUM POLICAJNÉHO ZBORU SR (2011). *Výročná správa finančnej spravodajskej jednotky Prezídia PZ v Slovenskej republike za rok 2011*.

STIERANKA, J. a kol. (2012) *Operatívne procesy a operácie (Vybrané problémy)*, Bratislava: A PZ v Bratislave.

STIERANKA, J. a kol. (2013) *Spravodajská činnosť*. Bratislava: A PZ v Bratislave.

STIERANKA, J. (2009) *Boj proti legalizácii príjmov z trestnej činnosti vo vybraných krajinách Európskej únie, Praha*: Policejní akademie ČR v Praze.

Contact address

prof. Ing. Jozef Stieranka, Ph.D. (corresponding author)
Academy of the Police Force in Bratislava, Department of Criminal Police / Akadémia Policajného zboru v Bratislave, Katedra kriminálnej polície
(jozef.stieranka@minv.sk)

JUDr. Stanislav Backa
Pan-European University, Faculty of Economics and Entrepreneurship / Paneurópska vysoká škola, Bratislava, Fakulta ekonómie a podnikania
(backa.stanislav@slposta.sk)