343.72-058.53
COBISS.SR-ID 32593673
DOI 10.5937/fb_godisnjak0-29663

SELECTED CRIMINOLOGICAL ASPECTS OF FRAUD COMMERCE THROUGH FALSE MANAGERS

Michaela Jurisová*
Academy of the Police Force in Bratislava, Slovakia

Miroslav Comorek**
Bureau of the Criminal Police of the Presidium of the Police Force

Elena Nikolajová Kupferschmidtová***
Academy of the Police Force in Bratislava, Slovakia

* michaela.jurisova@akademiapz.sk
** miroslav.comorek@minv.sk
*** elena.nikolajova@akademiapz.sk

SELECTED CRIMINOLOGICAL ASPECTS OF FRAUD COMMERCE THROUGH FALSE MANAGERS

Introduction

Serious organized fraud can be considered as one of the development trends and accompanying signs of crime. It is appropriate to apply crime control, both in the form of prevention and repression, from a national and international point of view. In 2014, at the initiative of France, Europol launched a new so-called Focal Point focused on serious organized fraud.[1] Later on, the Focal Points were transformed into the Analysis Projects (APs). Working with these Analysis Projects, Europol specialists can prioritise resources, ensure purpose limitation, and support EU law enforcement authorities and other partner organisations to tackle organised crime and terrorism through:

- analysing related information and intelligence, to obtain as much structured and concrete information as possible for law enforcement authorities to "hit" targets with;
- facilitating operational meetings between partners involved in cases;
- providing expertise and training to law enforcement authorities to support cases and share knowledge;
- deploying Europol mobile offices to the field for operations, giving live access to Europol's secure information exchange network and databases;

1 Analysis Projects (APs) are within the Europol Analysis System – an information processing system – and focus on certain crime areas from commodity-based, thematic or regional angles, e.g. drugs trafficking, Islamist terrorism, Italian organised crime.

- providing support for judicial cooperation and for the tackling of other related criminal activities uncovered in the course of investigations, such as money laundering.[2]

The main reason behind the initiative of French authorities as well as the authorities of other Members States of the European Union (hereinafter referred to as the 'EU') was an increase in the number of so-called CEO frauds in recent years. The Slovak Republic joined the forces with France, Spain, Belgium and Romania in 2015 thanks to (then) Focal Point APATE by participation through the National Criminal Agency of the Presidium of the Police Force (hereinafter referred to as 'NAKA P PZ').

Due to the seriousness of the issue, the Criminal Police Office of the Presidium of the Police Force (hereinafter referred to as 'ÚKP P PZ') also pays attention to CEO frauds as the reports on the development of CEO frauds in the Slovak Republic (resulting from the reports of individual Departments of the Criminal Police of the District and Regional directorates of the Police Force) and the analysis of the criminal activity of the CEO of fraud in the Slovak Republic are continually processed and passed on to the relevant authorities at national and international level. The Financial Intelligence Unit of the National Criminal Agency of the Presidium of the Police Force also pays attention to this issue. The up-to-date information (among others) on CEO frauds forms an integral part of the Annual Report of the Financial Intelligence Unit for the respective year. The above-mentioned documents give information on analysis of the current state of the CEO frauds committed in the territory of the Slovak Republic, its development through the recent years and proposed measures *de lege ferenda*.

For the purposes of the current contribution, the CEO frauds are looked upon from a multidisciplinary perspective.

Selected Criminological Aspects of CEO Frauds

"**CEO fraud**", also known as "Business Email Compromise" (BEC), is a scam in which high level executives (also known as C-level executives) are impersonated, giving employees urgent and confidential orders to make financial transactions in a way that does not follow the company's standard

2 Information was adapted from the Europol website: https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects [cited 2020-11-11].

procedures.[3] A CEO scam is a targeted attack whose point is to deceive an employee, usually from the finance or accounting department. During the implementation of fraud, there is pressure on the company's employees to transfer significant amounts of money (abroad). These scams are associated with so-called social engineering. Fraudsters use the classic tricks of social engineering, through publicly available websites, but also through 'hacking' into the e-mail communication of the company, finding out all the necessary information about ongoing business, contacts, methods of communication and the identity of the CEO or employee responsible for money transfers.

The fraudsters subsequently pretend to be the CEOs (usually by e-mail or telephone) by contacting the relevant employee due to the need to complete a financial transaction. In the context of such communication, they do not give 'their subordinate' a choice and this is guided in the form of strict instructions (often also in connection with the threat of a sanction for non-compliance). After the transfers (particular sum of money) end up in another country, the money is further 'laundered'.

This is a relatively new form of crime. This type of fraud began to be discussed in 2007–2008. Initially, it focused primarily on French companies. Later, around 2013, such cases were reported also in other countries such as the United Kingdom, Belgium and Romania. However, France was and still is the place with the highest rate in the CEO frauds and the highest number of victims and damages cause by this particular type of crime.

CEO fraud is basically a 'payment order fraud'. It is characterized by a sophisticated, harmonized and calculated attack, especially against companies, but also private individuals or state institutions. Attacks are usually organized by a single steering group. The basic fraud model involves at least two countries (often Member States of the European Union).

A very important feature of CEO fraud is action, which at the same time pushes this type of crime into the realm of so-called 'cybercrime'. An overview of the selected companies alone is not enough. In principle, to create the impression of the actions of an authorized CEO manager is an essential step in breaking the security of e-mail communication of the CEO manager himself, provided that his mailbox contains information about ongoing

3 Adapted from: https://www.google.com/search?source=hp&ei=9ea6X5mQKc6IaYLfuqAK&iflsig=AINFCbYAAAAAX7r1BYG9hPPCpSgPPsJW9z55UihG-x8P&q=cEO+frauds&oq=cEO+frauds&gs_lcp=CgZwc3ktYWIQAzIFCAAQyQMyAggAMgIILjICCAAyAggAMgIIADICCAAyAggAMgIIADICCAA6CAguEMcBEKMCOggILhDHARCvAToKCC4QxwEQowIQClCIB1iqFWDEFmgAcAB4AIAB3gWIAZ8TkgELMS4yLjEuMS42LTKYAQCgAQGqAQdnd3Mtd2l6&sclient=psy-ab&ved=0ahUKEwjZ3qi1mpftAhVORBoKHYKvDqQQ4dUDCAY&uact=5 [cited 2020-11-20].

business activities, but also about e-mail addresses of individual employees. Thus, the highly sophisticated new technologies ensuring the anonymity of perpetrators are increasingly used by the hackers today. This form of fraud has proven and still proves to be a very lucrative for organized groups in terms of quick income gains. Due to this fact, it is important to assess the CEO scams from multiple, different perspectives.

In terms of the criminal law dimension, recorded cases of CEO fraud in the Slovak Republic are classified as a criminal offense of fraud under Section 221 of the Criminal Code (hereinafter also referred to as 'TZ'). Depending on the method of committing the crime or causing the damage, the qualified factual nature of this crime comes into play. As it was already mentioned above, in these cases the concurrence of the crime of fraud (according to § 221 of the Criminal Code being in force in the territory of the Slovak Republic) and the crimes of computer crime according to § 247 of the (same) Criminal Code et seq. or also being the criminal offense of money-laundering pursuant to Section 233 of the respective Criminal Code.

From the perspective of phenomenology, it is appropriate to draw attention to the positive change in the sense of adding code 858 in code no. 2 Evidence-statistical system of crime (hereinafter also referred to as 'ESSK') – Fraud in connection with a false transfer of money on the instructions of a fictitious manager. The change in question has been in force since 1 October 2017 and its purpose is the statistical monitoring of CEO fraud. It is breathtaking to add that a retrospective examination of these data revealed that the cases reported under this item were/are filled in incorrectly, probably due to human error.

In accordance with information from individual regional directorates of the Police Force (hereinafter also referred to as 'KR PZ'), 27 cases of CEO fraud were recorded in 2018. Of these, fifteen cases were committed at the trial stage and twelve cases were completed. In 2018 (compared to 2017) CEO fraud in the Slovak Republic shows a declining trend. In terms of the development trend, 18 cases fewer were recorded in 2018 than in 2017. Based on the available information (since 2013), it can be stated that in the years 2013 to 2016, the detected CEO frauds showed a stagnant trend (up to 20 cases per year). In 2017, an upward trend was recorded, more than double compared to previous years, and in 2018 a downward trend was again recorded. In 2019, again a downward trend was present through the monitored period. Thus, from a longer-term perspective, a stagnant or declining trend of recorded CEO frauds can be observed, with the exception of 2017. In the observed period (2013–2019), the number of attempts was

higher than the number of completed acts (see Table 1). From the point of view of criminal geography, the highest number of detected CEO frauds was recorded again, in 2017 in the Bratislava region and the lowest number in the Prešov region.

Table 1. The average amount of damage in cases of CEO fraud according to individual Regional Directorates of the Police Force.

Year	2019	2018	2017	2016	2015	2014	2013
Damage in €	CD	CD	CD	CD	CD	CD	CD
BA region	101140	18711	28373	22125	0	26155	0
TT region	20607	45900	17863	0	0	0	0
TN region	28932	35128	21916	0	0	0	0
NR region	25000	26066	14021	0	2855	0	0
ZA region	28789	17368	12756	43734	19936	45000	0
BB region	44393	12440	12250	0	0	0	0
PO region	6022	0	0	0	0	0	0
KE region	0	53837	5718	0	0	0	0
Overally in the SK	41223	27023	17251	30769	15666	29924	0
Damage in €*	28195	–	–	–	–	–	–

CD – Caused Damage

*is the average amount of damages without two specific cases of CEO frauds

In 2019, it was found that the most frequently challenged entities remain legal entities (commercial companies) established in the form of limited liability companies and joint stock companies (36 subjects in total). It is precisely these two types of entities that we can rank among the most vulnerable due to easily publicly accessible data on their structure and their insufficient access to information security. There were a total of 9 public institutions attacked by CEO fraud in 2019, namely Senior Park in Rohovce, Chynorany Municipality, Priepastná Municipality, Primary School with Kindergarten in Mikušovce, Straník Social Services Center in Žilina (also in 2018), Regional Cultural Center in Žilina, the Social House ANTIC in Bardejov, the Municipality of Veľká Lomnica and the Municipal Office of Rožňava. In addition, 2 state-owned enterprises and 2 natural persons operating a trade (self-employed person) were attacked. Comparing the

development of this crime, it was found that the most frequently attacked subjects are still limited liability companies and joint stock companies, while their number has doubled compared to 2018, and a new object of attack by perpetrators has also been added, namely natural persons operating a trade.

The phenomenological concept undoubtedly includes the reference to clarity (of the selected type of crime). The level of clarity of this crime is limited by the fact that it is an international crime (and the presence of elements such as money mule or foreign bank accounts to which there are fraudulently lured funds are subsequently transferred). In cases of suspension of criminal prosecution, the main reason is the failure to identify a specific person of the perpetrator who communicated from abroad and mainly in electronic form. In living cases, the results of investigations depend to a large extent on the results of international cooperation and assistance. The main reasons for not clarifying such cases can clearly include their international aspect and modern ways of covering up the identity of the perpetrator through electronic communication. Given these aspects of CEO fraud, local options for clarifying individual are most likely insufficient.

It is obvious that the damage caused by CEO frauds amounts to large extent, while in 2018 in the Slovak Republic the damage caused by this type of crime amounted to more than € 405,000, the previous year the damage found was higher, both for completed acts and for acts in the experimental stage. The total amount of damage is, of course, mainly affected by the number of cases. For this reason, for a more objective assessment, it is also appropriate to evaluate the so-called claims (i.e. the average amount of damage in one case). As a result of the above, in 2018, in the attempt of the CEO fraud, a loss of less than € 39,000 per case was found in the attempt of the CEO fraud and in completed CEO frauds slightly exceeding € 27,000 per case. In 2017, the number of attempts to perform even for completed CEO frauds showed lower amounts compared to 2018. From the above-mentioned information, it can be concluded that in the last year the perpetrators performed fewer attempts and completed less number of acts of CEO frauds compared to 2017, but the damage rate increased in experiments as well as in completed cases.

As a result of reports from individual regional directorates of the Police Force and NAKA P PZ, 49 cases of CEO fraud were recorded in the Slovak Republic in 2019. Unfortunately, more than half of this number was completed acts – there were 20 cases committed at the trial stage and 29 com-

pleted acts. Compared to 2018 (27 recorded CEO frauds), this is a relatively significant increase in the number of recorded acts. There was also a change in the number of trials and completed acts. In 2018 more acts were recorded at the trial stage than completed acts. In terms of available data on the state of CEO frauds in the the Slovak Republic (since 2013), it can be stated that in the observed period (2013–2019) in 2019, for the first time, the number of completed acts exceeded the number of acts in the trial stage. Taking into account the geographical arrangement of the Slovak Republic, the highest number of cases was recorded in 2019 in the Bratislava Region and the lowest number of cases in the Košice Region. The phenomenological concept of crime undoubtedly includes the appropriate detection rate of the particular act/type of crime. As in the previous period, unfortunately in 2019 in the Slovak Republic, not a single case of CEO fraud was solved. This confirms many of the accompanying features of these frauds, such as their international dimension or the sophistication of perpetrators in the form of modern ways of concealing their identities through electronic communication.

The amount of damage is also monitored statistically, both in the case of completed acts and in attempted cases. In 2019, the damage caused by CEO fraud in the Slovak Republic was almost one million two hundred thousand euros and the damage in attempted cases more than one million euros. Compared to 2018, the damage found increased both for completed acts (more than twice) and for attempted acts (almost twice). This shows a clear year-on-year increase. In 2019, in the case of damage caused (completed case), it was a fraud with a damage amount of 406,000 euros (within the competence of the Regional Directorate of the Police Force in Bratislava) and in the case of endangered damage (an attempted case) it was a fraud where more than 300 000 euros in damages were at stake (within the competence of the Regional Directorate of the Police Force in Nitra). In terms of a more objective comparison of the amount of damage caused by such fraud, it is appropriate to evaluate the damage itself which is represented by the average amount of damage per one case. The specific cases mentioned above are automatically taken into account when assessing claims, although it is appropriate to add with one breath that they significantly distort the resulting figure. In the Slovak Republic, in 2019, the attempted CEO frauds resulted in a loss of € 54,195 per case and in case of the completed CEO frauds it was € 41,223 per case.[4]

4 Report on the development of criminal activity of the CEO of fraud in the territory of the Slovak Republic in 2019.

In the past, perpetrators of CEO fraud have focused on a larger number of entities with a lower amount requested, probably in order not to attract attention. Recently, it can be stated that this development is beginning to change – perpetrators act in such a way that even when deceived by a smaller number of entities, they obtain a larger amount of fraudulently lured funds. Following the analysis of Slovak documents, in connection with the *modus operandi*, it can be noted that recently the perpetrators of this crime used basically only electronic communication (e-mail), in which they communicated with victims. Cases of CEO fraud in the form of a phone call or a fax message were not recorded. As a result of the analysis of such frauds, data on the way the perpetrator communicated with the injured party indicate that in several cases it may have been the conduct of one perpetrator, focusing primarily on facilities within the Slovak Republic, due to language barriers.

The general tendency to reduce the language barriers within the organizations, especially the international ones can help the perpetrators to commit the CEO frauds. The language related mistakes are easy to spot in case a native speaker of a language is reading the instructions, however, in case of international companies where there is a high degree of multilingualism, employees of different cultures melt together and the working language is usually adapted to the needs of such an environment. To increase efficiency, productivity and quality, many linguistic mistakes are accepted, thus considered not being suspicious even in case a foreign fraudsters hack the communication systems of the respective company. It is worth mentioning that while language proficiency may also promote a safer work environment, to employ foreign-born workers with a perfect (native level) command of working language being used as communication platform within the company is more than desirable as it is naturally a way how to spot fraudulant communication/e-mails/instructions and consequently prevent such crimes.

However, the ways of obtaining relevant information vary through the time and countries. It is also possible to draw attention to the so-called social engineering as a way of obtaining confidential information through manipulation. This method commonly uses Internet or telephone communication, abusing people's trust by pretending to be known in existing companies or institutions. Attacks using social engineering can be heterogeneous, from bulk phishing emails to targeted, multi-layered, and sophisticated multi-technique attacks. However, they all have in common that they focus on manipulating normal human behavior, and there are only a limited

set of technical measures that can help to protect companies/individuals against these types of attacks.

The objects that are most often attacked by perpetrators committing the CEO fraud are legal entities. In 2018, most of the contested companies were established in the form of Ltd. company (Limited Liability Company). Joint-stock companies as well as public institutions (such as the municipal offices, the social services centers or the agricultural cooperatives) were also attacked, but not in such frequency as Ltd. companies. Two of the most frequently attacked objects (Ltd. companies and public institutions) can be classified as the most vulnerable due to easily publicly accessible data on the structure of society and possibly insufficient access to information security. In terms of the legal form of business of legal entities in the form of companies (such as limited liability company and joint stock company), the share of injured entities is given both by their highest numerical representation in the Slovak Republic and also by their ordinary and relatively frequent trading, especially with goods. In the case of public institutions (or state-owned enterprises), it was also possible for the employee to fail (due to insufficient experience). The fact that the trading of these entities is rather exceptional may also have played a role. The effect of an economically active region (e.g. Bratislava, Nitra or Žilina) and a greater concentration of companies with business potential suitable for perpetrators of this type of fraud manifested itself in the CEO's fraud facilities.

In general, CEO frauds are directed mainly towards private companies and state institutions or public organizations due to the fact that electronic bank transfers are commonly performed on the instructions of superiors. One of the commonly used forms is that a perpetrator who has internal information about the structure of the organization and its working processes, manipulates his/her way through these processes and pretends to be the CEO manager and addresses directly the object (accounting officer or accountant) with a request to transfer particular amount of funds.

On the basis of information obtained from already committed CEO frauds abroad, it is possible to observe several methods/ways (acting individually or even intertwining) used by the perpetrators:

a) *an amended invoice* – is used for companies that cooperate mainly with suppliers from abroad. Impersonating the client (supplier), the perpetrator contacts the (damaged) company (by phone, e-mail, fax) asking its employee to change the account number to which the payment for the invoice is to be sent. This is an existing invoice for a trade that is currently in progress.

b) *fake manager* – the perpetrator who impersonates the CEO manager instructs (for example by phone or e-mail) an employee of the aggrieved company to transfer funds to a designated account due to the acute and urgent need to perform such transaction.
c) *fake e-mail* – the perpetrator creates a fake e-mail address identical to the e-mail address of the CEO manager, from which fake invoices are subsequently sent to potentially exploited and in case of successfully completed crimes aggrieved companies, these are companies with which the company of the fake CEO manager trades or traded – the invoices for transactions that in reality were not executed.
d) *fake lawyer* – a way in which the offender contacts an employee/CEO manager, pretending to be a lawyer representing their company, with a request for immediate reimbursement of the costs that are due for the legal services required by the company (e.g. court fees, amount due, arrears on compulsory payments). There may also be cases where the perpetrators impersonate lawyers representing the CEO's company and assert a right (for example, in the form of an execution order) against another company on his behalf.

Within 2018, in the Slovak Republic, the CEO frauds *modus operandi* stabilized in two basic forms:

a) email masking is the technique of altering **email** addresses, usually in order to protect the real data from mistakenly (or intentionally) being misused. Usually, an **email** address that's **masked** keeps its original format and can't be easily traced back to the original address.[5] However, for the purposes of the CEO frauds, the information provided within the e-mails intended for this type of crime are almost identical to the original ones but differs in small details that are not easy to spot, thus, being taken by the employee for the original e-mail.

b) phishing as a type of social engineering **attack** often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim

5 Information adapted from: https://www.google.com/search?rlz=1C1GGGE_skSK515SK520&ei=Tmy7X5ecO4iwa-zMl7AP&q=email+masking&oq=email+masking&gs_lcp=CgZwc3ktYWIQAzIFCAAQyQMyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAMgIIADICCAA6BwgAEEcQsAM6BwgAEMkDEEM6BAgAEEM6AgguOggIABDJAxCRAjoFCAAQkQI6CAguEMcBEK8BULHsCVj2jwpggJEKaAJwAHgBgAHZAYgB0ROSAQcxMC4xMC4ymAEAoAEBqgEHZ3dzLXdperABAMgBCMABAQ&sclient=psy-ab&ved=0ahUKEwiX-5_LmZjtAhUI2BoKHWzmBfYQ4dUDCA0&uact=5 [cited 2020-11-15].

into opening an email, instant message, or text message.[6] Phishing allows the offender to enter into business/work communication between the CEO and the accountant using the true e-mail address of the CEO.

The difference between these two forms lies mainly in the extent of the perpetrators‘ expertise and the actual implementation of the expertise. Creating a masked e-mail address requires less computer skills compared to executing CEO phishing fraud. In addition, there are many instructions for implementation within the Internet. The perpetrator then selects from the available resources of the institution that has the necessary e-mail addresses published and also uses the addresses of the (potential) victims. Then the request for a quick transfer of funds abroad is submitted. In case of phishing attack, the perpetrator is expected to break into the computer and communication system of potential victim (individual or company). As a result, the data about personal/company communication, business activities, internal functioning of the company and, in several cases, the data from available social networks are obtained and subsequently being used as a source data for execution of the attack. The perpetrator uses the data for the purpose of targeted and timely coordinated attack (e.g. at the time when the CEO of the company is absent – having days off, being at holidays, or simply out of office). In most cases, the change of the account number on the invoice in an ongoing business operation was requested from perpetrators. This method, on the one hand, increases the chances of the CEO frauds being executed successfully, on the other hand, it requires much more expertise, compared to the form of a masked e-mail, as the latter is a targeted sophisticated attack. Phishing as well as an amended invoice (or account number) is usually used in terms of an ongoing business operation.

Of the total number of cases recorded in 2018 in the Slovak Republic, the majority was carried out in the form of a masked e-mail and only in two cases the phishing method was used. Compared to the previous year, when the method of CEO fraud in the form of phishing and only subsequently by the method of masked e-mail dominated, there has been a change. The premise of the reason for the change is that potential objects pay more

6 Information adapted from: https://www.google.com/search?rlz=1C1GGGE_skSK515SK520&ei=-s2u7X8PfHMWPlwSBirHoBw&q=phishing+attack&oq=phishing+attack&gs_lcp=CgZwc3k-tYWIQAzIFCAAQyQMyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAMgIIADICCAA6BwgAEEcQsANQ-ZQJWNWyCWC5tAloAXAAeASAAeADiAGIFJIBCTYuNi4xLjEuMZgBAKABAaoBB2d3cy13aXqwAQDIAQjAAQE&sclient=psy-ab&ved=0ahUKEwiDhY2BmZjtAhXFx4UKHQFFDH0Q4dUDCA0&uact=5 [cited 2020-11-15].

attention to securing their software against unauthorized entry into commercial communications, thus preventing the perpetrators from committing such frauds.

The *modus operandi* of perpetrators of such fraud goes hand in hand with the etiology of CEO fraud. The fact that individuals as well as companies cannot defend themselves so effectively against receiving fraudulent e-mails is alarming even now as in most cases the CEO frauds were committed due to the failure of human factor. There are also other factors influencing the way of crime being committed as well as the success rate of the CEO frauds. Insufficient and ineffective preventive measures from the company's perspective can facilitate the crime itself. Also the standard administrative procedures within the company should be tailored to the needs of each company/individual. The transfer of funds should not be the responsibility of only one person. There should be a system of several stages including double/triple checking, verification and approval of individual transactions set at the particular financial limit (especially larger amounts of funds).

The Slovak Republic belongs to a group of countries (together with, for example, the Czech Republic, the Republic of Poland or the Republic of Hungary), through which the transfers of funds from abroad is quite frequent. From the etiological point of view, this situation is a consequence of legislative gaps (especially in regard to the financial market), which are used by the perpetrators in the framework of transfers of funds between the states of the European Union.

While committing the CEO frauds, in most cases, the offender needs a bank account that he will be in control of, even if he does not own it. For this purpose, various intermediaries are organized who, whether for remuneration or fraud, open an account and subsequently grant access rights to the perpetrators or carry out the relevant transactions on their instructions. Purposeful opening of accounts has thus (but not only) become a lucrative source of income for many '*straw men*' in the Slovak Republic, especially for foreigners, and at present it is not possible to speak of effective measures to significantly prevent the current situation.

In connection with CEO fraud and with regard to the subsequent actions of perpetrators, it is appropriate to state that it is also a predictive crime for the subsequent legalization of the proceeds of crime obtained by execution and completion of such crimes. Thus, CEO frauds are largely related to money-laundering across the states of the European Union. The Annual Report of the Financial Intelligence Unit for 2018 confirms that money-laundering is related to the most of the cases of the CEO frauds

being committed in the territory of the Slovak Republic for the period of 2018. It is the crime of money laundering that is the element that connects cases showing signs of CEO fraud, because the way in which the offender transfers funds and their subsequent collection is also the biggest weakness in the complex structure of CEO fraud. An important role in the above-mentioned cases is played by the time starting by the act of funds withdrawal to their gradual transfer to the offender's account, or subsequent transfer to other accounts.

There are many ways in which the proceeds of crime can be legalized. The legalization method is the process of an organized group or individual to achieve the goal of creating what appears to be a legal origin of property that has actually been obtained through crime. The use of a particular method depends on two factors, namely: 1. *source of crime* and 2. *form* used for the purposed of obtaining the property/income through the crime. The source of crime is directly related to the nature of property/income obtained through the crime. Thus, the question of who committed the crime (organized group or an individual) plays a vital role when analyzing the crime. Also the information about related criminal activities and consequently additional leads to drug crime, ordinary crime, economic or financial crime, highly sophisticated crime or the opposite are important and need to be taken into account. Given these contexts, we can state that it is not possible to provide an exhaustive list of methods of money-laundering. The reasons for the emergence of new methods/ways of money-laundering are mainly the sophistication of source crime and the increasing flexibility of organized groups. It is also worth mentioning that new ways of conducting business transactions – they are accelerating and improving, using new methods of banking transactions can modify also the ways the crimes are committed today. Thanks to the information shared by the officers from the current application practice, it is possible to sum up, that most frequently used methods of money-laundering in the Slovak Republic for the recent period of time are the following: artificially increasing the turnover of companies working with cash; artificially increasing turnover or profits by over-invoicing; repayment method; back-to-back loan; fake winnings; international money transfers; bank checks, bills of exchange, letters of credit, capital contributions; real estate transactions; 'identity theft' (from identification documents, payment cards, skimming, phishing; and also the CEO frauds.[7]

7 STIERANKA, J. a kol. 2018. Legalizácia príjmov z trestnej činnosti a financovanie terorizmu, právna a inštitucionálna ochrana v Slovenskej republike (authors' translation: Laundering of the Proceeds of Crime

An important factor that precedes the CEO fraud in many ways is the existence or establishment of a bank account where fraudulently lured funds will be remitted. This account is opened in a bank domiciled in a country other than the one in which the account of the sender of the payment – business partner – is located. So-called *money mules* are generally used for this purpose. These persons are most often addressed in electronic form, not often under the pretext of a job offer or in the form of a service for consideration. Thus, in the case of CEO frauds committed in the Slovak Republic, the most common practice is that funds are transferred to accounts established abroad. The use of this method significantly affects the possibilities of securing funds. At the same time, it serves to thwart the identification of the attacker, or the final recipient of funds. In most cases, funds are also transferred several times until they end up in the account from which they are subsequently withdrawn in cash – by the final beneficiary (perpetrator) or another money mule, who then passes them on to the perpetrator or again sending the funds to the perpetrator through services such as Western Union and others.

In the phase of non-cash transfers, transactions are executed (to the money transfers themselves) to other pre-prepared accounts owned/controlled by offenders in banks domiciled in offshore countries or countries with difficult law enforcement cooperation (from the Slovakia's perspective due to limited number of bilateral/multilateral agreements or no possibilities to establish any agreements or cooperation), such as Nigeria, China, Ghana or Hong Kong. Cashless transfers are also often made to accounts held in banks domiciled in the United Kingdom, and it is possible to draw attention to the indications that these accounts are established for persons who have been granted asylum in the United Kingdom as part of the migration of the population from third countries and are used by perpetrators. In most cases the owners of such accounts are third-country nationals being granted the asylum in Britain and the above-mentioned owners are thus in the position of 'straw men'. The analysis of CEO fraud (in which data on bank accounts were found) in the Slovak Republic in 2018 provided detailed information about the cases of CEO frauds. It was reported that in 69% of cases the funds were directed to accounts established in the United Kingdom. The second most frequently used country for this purpose was Ukraine. Among the countries in which funds derived from the crime of CEO fraud have been or should have been legalized, the following

and Terrorism Financing, Legal and Institutional Framework of Protection in the Slovak Republic), p. 27 and following.

countries can be included: Spain, Turkey, the Netherlands or the People's Republic of China.

In terms of the application of prevention, the best way to protect companies or individuals against CEO frauds at present appears to be the increase of the security awareness of natural and legal persons (potential victims) against the possibility of such crimes and specific conduct of perpetrators in the matter. Fortunately, the failures of perpetrators trying to commit CEO frauds are also frequent. The failures are detected in most cases thanks to the real CEOs of the company or the accountants of the potentially aggrieved companies as they pay attention to every detail and every amount being transferred from and to the company accounts. However, Slovakia is one of the smaller countries, thus the volume of transactions and trade within the country is not really comparable to economically stronger countries such as France or United Kingdom. The size of the country and the number of business transactions within the country thus may be detected earlier and on time (compared to larger countries in size and volume of transactions). A draft of preventive measures was also prepared and published as a way of warning against attacks by perpetrators of CEO fraud in relation to available mass communication tools. In October 2018, the Police Force in the Slovak Republic was informed about a warning in the form of a short message appearing on the social network Facebook and was circulated in Slovakia. The Slovak Police Force informed general public about the case of CEO fraud that happened in Slovakia – it was a case similar to one that happened in reality in August 2018 and the message circulated by the Police Force was an example that was supposed to be informatory and preventive. Two months earlier, in August 2018, the section „Fraudulent money transfers" was added to the website of the Ministry of Interior of the Slovak Republic (www.minv.sk), in which a warning against the attack of perpetrators of CEO frauds has been published.[8]

It is also necessary to focus on the overall approach of organizations to information security, strict adherence to security policies (rules) and, of course, to support the active participation of employees of individual institutions in the company's as well as employee's security. Also the processing of 'Analysis of the crime of CEO fraud in the Slovak Republic' and 'Report on the Development of Crime of CEO fraud in the Slovak Republic' helps to reduce the number of recorded cases, whether committed at the stage of trial or completed acts (CEO fraud). Undoubtedly, the Annual Report

8 Website of the Ministry of Interior of the Slovak Republic – www.minv.sk. [online]. [cited 2019-06-14]. Available at: <https://www.minv.sk/?podvodne-prevody-penazi>.

of the Financial Intelligence Unit for 2018 also has a partially preventive effect.

Undoubtedly, an information system would also have a preventive effect, which would provide individual components with a detailed overview of the occurrence of this crime across the entire territory of the Slovak Republic together with selected features (IP addresses, address text, account number, etc.) – absence of such system appears to be problematic in this area.[9]

It is necessary to note that the individual criminological indicators (phenomenology, etiology, *modus operandi* of perpetrators, damaged objects or prevention) of the crime in question, in this case the CEO fraud, intersect in both theory and application practice.

CEO Frauds in Application Practice

In September 2018, in the morning, a hitherto unknown perpetrator posing as the company's manager, via e-mail communication (e-mail) contacted the company's sales representative and instructed him to pay an invoice for an order from a Ukrainian company, in the amount of more than € 8,300. The funds were about to be transferred to a bank in Ukraine. In a subsequent communication, he ordered the immediate payment of € 3,300 to that account, stating that he had ordered the balance to be paid the following day. The company's sales representative, convinced that she had been asked to make the said payment, transferred the amount of € 3,300 from the company's account on the same day. During the subsequent communication with the manager of the company, it was found that the manager did not send an e-mail to the sales representative and did not ask for payment of any amount. Damage of € 3,300 was caused to the company by this action. In the event of a transfer of the remaining amount, the company in question would suffer damage in the amount of more than € 8,300.[10]

In January 2018, the Financial Intelligence Unit (hereinafter referred to as 'FIU') received from the liable person Bank A a report on an unusual business transaction concerning two fraudulent payments from two foreign companies B and C from accounts held in Germany in the total amount of € 178,000. Both foreign payments were in the same amount of

9 The absence of information system was reported in the Report on the Development of Crime of CEO fraud in the Slovak Republic and also in the Annual Report of the Financial Intelligence Unit for 2018.

10 Information is part of the Report on the Development of Crime of CEO fraud in the Slovak Republic in 2018.

€ 89,000 and were credited to the same account maintained by Bank A for person D. The foreign bank requested the return of the respective funds to the foreign accounts of companies B and C due to fraud and also sent a copy of the criminal complaint. As the bank learned about fraudulent payments in time, before handling the funds, it took technical measures on the person's account and after trying to manage the funds on the person's account via the Internet banking service, it subsequently proceeded with a delay pursuant to § 16 of the Act on protection against the legalization of proceeds of crime.

An analysis of the report on unusual business transactions revealed that the transfer of both of the above-mentioned foreign payments from foreign accounts was preceded by hacking of the electronic business communication of the foreign account holders of entities B and C and the original payments were redirected to the wrong account belonging to person D.

The FIU subsequently processed the information and passed it on to the competent law enforcement authority, which, on the basis of this information, initiated criminal proceedings for a particularly serious crime of money-laundering at the trial stage. The prosecutor's office subsequently secured funds in the total amount of € 178,000 in the account of person D.[11]

Conclusion

In conclusion, based on the relatively low number of detected cases and the declining trend of detected CEO frauds (compared to the previous period), it can be stated that the Slovak Republic is not directly and permanently endangered by this crime.

In terms of the effective application of crime control in the coming period, it is of vital importance to continue to monitor the development of CEO fraud within the Slovak Republic.

The cooperation at the international and national levels is indispensably important in the whole process of detecting and clarifying CEO fraud. In the Slovak Republic, within the framework of service cooperation, it is mainly the cooperation of the following departments: Criminal Police Departments of Regional and District Directorates of the Police Force, Criminal Police Office of the Police Force, NAKA P PZ, Computer Crime Department of the Criminal Police Office Presidium of the Police Force, etc.

11 Information adapted from the Annual Report of the Financial Intelligence Unit for 2018.

It is also important to acquaint the relevant departments with the current status and development of CEO fraud, which is implemented primarily by a report on the development of CEO fraud in the Slovak Republic (prepared by the Criminal Police Office of the Presidium of the Police Force). In terms of international cooperation in the matter of verifying the occurrence of bank accounts detected in cases of CEO fraud committed within the territory of the Slovak Republic, the direct cooperation and exchange of information with the Europol National Headquarters of the Office of International Police Cooperation of the Presidium of the Police Force continues to play a crucial role. The FIU, which intends to be interested (among others) in CEO fraud, is an active member of international bodies, such as the Moneyval Committee. This confirms the international dimension of the issue and, consequently, the need for international police as well as legal cooperation.

In 2018, not a single case of CEO fraud was solved in the Slovak Republic. Compared to 2017, the number of detected CEO frauds decreased in 2018. In the years 2013–2016, it was possible to observe a stagnant trend. In 2017, there was a relatively significant increase (more than double) in recorded CEO fraud (compared to 2016). *Modus operandi* of perpetrators was in most cases masked e-mail, compared to the use of a more demanding method of implementation – phishing, which was used in only two cases. The perpetrators focused on a smaller number of entities, but with a higher amount requested. Thus, the damage rate was higher. The objects of CEO fraud were mostly legal entities established in the form of limited liability companies and joint stock companies, with the exception of several state institutions. Funds coming from CEO fraud in the Slovak Republic were transferred abroad, most often to accounts in the United Kingdom. No financial investigation was conducted in any case of CEO fraud.

The Annual Report of the Financial Intelligence Unit for 2018 draws attention to the assumption of an increase in CEO fraud in 2019, as there are no (really functional) preventive measures in place. Such fraud can also be prevented (among other things) by trying to thoroughly and constantly check the data stated in the documents (e.g. verifying the transactions at the accounts) and with particular focus on verifying business activities between business partners. At the same time, the Annual Report of the Financial Intelligence Unit for 2018 draws attention to forecasts of further developments in the area of legalization of proceeds of crime and terrorist financing, which states that based on an analysis of past developments in legalization and terrorist financing, in the Slovak Republic, revenue genera-

tion can be expected in the next period: e.g. by committing property crime in the form of internet fraud and CEO frauds; committing various and new forms of tax crime; exploiting tax heavens and offshore companies and involving box and fictitious companies in complex business.

REFERENCES

Annual Report of the Financial Intelligence Unit for 2018. Available in Slovak only.

ČENTÉŠ, Jozef a kol. 2016. Penal Code – Extended Commentary available in Slovak only under the title: Trestný zákon – Veľký komentár, 3. aktualizované vydanie. Žilina: Eurokódex, s. r. o., 2016. 959 s. ISBN 978-80-8155-066-9.

Europol.europa.eu. [online]. [cit. 2019-06-11]. Available at: <https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects>.

Ministry of Interior of the Slovak Republic. Webpage: Minv.sk. [online]. [cit. 2019-16-14]. Available at: <https://www.minv.sk/?podvodne-prevody-penazi>.

Report on the Development of Crime of CEO fraud in the Slovak Republic for 2018. Available in Slovak only.

Report on the development of criminal activity of the CEO of fraud in the territory of the Slovak Republic in 2019.

STIERANKA, Jozef a kol. 2018. Laundering of the Proceeds of Crime and Terrorism Financing, Legal and Institutional Framework of Protection in the Slovak Republic. Available in Slovak only under the title: Legalizácia príjmov z trestnej činnosti a financovanie terorizmu, právna a inštitucionálna ochrana v Slovenskej republike. Bratislava: Wolters Kluwer SR, s. r. o., 2018. 193 s. ISBN 978-80-8168-912-3.

Law for public available in Slovak only under the title: Zakony pre ludi.sk. [online]. [cit. 2019-06-14]. Available at: <https://www.zakonypreludi.sk/zz/2005-300>.

Law for public available in Slovak only under the title: Zakony pre ludi.sk. [online]. [cit. 2019-06-14]. Available at: <https://www.zakonypreludi.sk/zz/2008-297>.

ОДАБРАНИ КРИМИНОЛОШКИ АСПЕКТИ ПРЕВАРНЕ ТРГОВИНЕ КРОЗ ЛАЖНЕ МЕНАЏЕРЕ

Михаела Јурисова
Полицијска академија у Братислави (Словачка)

Мирослав Цоморек
Биро криминалистичке полиције Президијума Полиције Словачке

Елена Николајова Купершмитова
Полицијска академија у Братислави (Словачка)

Сажетак

Циљ овог чланка је да укаже на такозвану превару извршног директора (од енглеског извршног директора – злочини превара учињени на основу упутстава такозваног „лажног менаџера“), као релативно нов и озбиљан облик кривичног дела. Анализа извештаја о необичним пословним операцијама показала је да су најчешћи случајеви прања новца и њихове повезаности са предиктивним криминалом у 2018. години укључивали (између осталог) и превару извршног директора, што је један од разлога за обраћање пажње на ову тему. Кривично дело о коме се говори посматра се из перспективе криминологије. Теоријски део рада указује на кривичноправну димензију, феноменолошку димензију, учиниоце и њихов начин рада, предмете такве преваре, али и могућу превенцију. Теоријски део рада допуњен је указивањем на стварне случајеве из праксе у облику извештаја о случајевима. За резимирање информација коришћени су налази финансијске обавештајне јединице и канцеларије криминалистичке полиције, као и стручна литература и правни документи. Са методолошког становишта, као приоритет су коришћени: анализа докумената и студија случаја.

Кључне речи: *превара, превара извршног директора, прање новца, необично пословање, Канцеларија криминалне полиције Президијума полицијских снага, Финансијско обавештајна јединица Националне криминалне агенције Президијума полицијских снага, Словачка Република.*