DEPÓSITO LEGAL ZU2020000153
Esta publicación científica en formato digital
es continuidad de la revista impresa
ISSN 0041-8811
E-ISSN 2665-0428

Revista de la Universidad del Zulia

Fundada en 1947
por el Dr. Jesús Enrique Lossada

Ciencias Sociales y Arte

Año 13 N° 38
Septiembre - Diciembre 2022
Tercera Época
Maracaibo-Venezuela

DOI: http://dx.doi.org/10.46925//rdluz.38.11

Foreign experience in legal regulation of fraud investigation

Mykola Yefimov *
Natalia Pavlova **
Volodymyr Fedchenko ***
Viktor Pletenets ****
Oleksandr Kryvopusk *****

ABSTRACT

The purpose of the research. The purpose of the article is to clarify foreign experience in legal regulation of fraud investigation. Main content. Considered are methods of detecting abuses performed by personnel at foreign enterprises and methods of combating such abuses. Methodology: Review of materials and methods on the basis of analysis of foreign experience concerning legal regulation of fraud investigation. Conclusions. It has been observed that despite legislative and regulatory documents, fraud and other types of crimes committed by employees of various branches are a widespread problem both in Ukraine and abroad. Highlighted the main areas of economic activity where fraud losses account for the largest amounts.

KEY WORDS: Corruption, crime, criminal law, Law, jurisprudence, police.

*Assistant Professor, Doctor of Science in Law, Assistant Professor at the Department of Criminalistics and Premedical training, Dnipropetrovs'k State University of Internal Affairs, 49005, Gagarin Avenue, 26, Dnipro, Ukraine. ORCID: https://orcid.org/0000-0003-3964-798X E-mail: efffimovnick@gmail.com

**Assistant Professor, Candidate of Science Law, Assistant Professor at the Department of Criminalistics and Premedical training, Dnipropetrovs'k State University of Internal Affairs; 49005, Gagarin Avenue, 26, Dnipro, Ukraine. ORCID: ORCID https://orcid.org/0000-0002-1572-4648 . E-mail: Pavlova_Natalia_vvv@ukr.net.

***Assistant Professor, Candidate of Science Law, Professor of the Department of Criminal Procedure and Strategic Investigations of the Dnipropetrovs'k State University of Internal Affairs; 49005, Gagarin Avenue, 26, Dnipro, Ukraine. ORCID: https://orcid.org/0000-0003-4006-3535 . E-mail: mixayluz@ukr.net

****Assistant Professor, Doctor of Science in Law, Assistant Professor at the Department of Criminalistics and Premedical training, Dnipropetrovs'k State University of Internal Affairs; 49005, Gagarin Avenue, 26, Dnipro, Ukraine. ORCID: https://orcid.org/0000-0002-3619-8624 . E-mail: Viktor_plet@i.ua.

*****Assistant at the Department of Criminalistics and Premedical training, Dnipropetrovs'k State University of Internal Affairs; 49005, Gagarin Avenue, 26, Dnipro, Ukraine. ORCID: https://orcid.org/0000-0003-4889-5205. E-mail: krivopusk.and@ukr.net

Recibido: 02/06/2022 Aceptado: 22/07/2022

DOI: http://dx.doi.org/10.46925//rdluz.38.11

Experiencia extranjera en regulación jurídica de investigación de fraudes

RESUMEN

El propósito de la investigación. El propósito del artículo es aclarar la experiencia extranjera en la regulación legal de la investigación del fraude. Contenido principal. Se consideran métodos para detectar abusos cometidos por personal de empresas extranjeras y métodos para combatir tales abusos. Metodología: Revisión de materiales y métodos sobre la base del análisis de la experiencia extranjera en materia de regulación legal de la investigación del fraude. Conclusiones. Se ha observado que, a pesar de los documentos legislativos y reglamentarios, el fraude y otros tipos de delitos cometidos por empleados de varias ramas son un problema generalizado tanto en Ucrania como en el extranjero. Se resaltan las principales áreas de actividad económica donde las pérdidas por fraude representan los mayores montos.

PALABRAS CLAVE: corrupción, delincuencia, Derecho penal, Derecho, jurisprudencia, policía.

Introduction

In the up-to-date world, fraud takes almost the first place among the most common offenses. Despite legislative and regulatory documents, fraud and other types of crimes committed by employees of various branches have become a widespread problem both in our state and abroad. In particular, the Association of Certified Fraud Examiners (ACFE) in its 2022 report estimated that American organizations lost 5% of their annual income due to economic crime of various types, which is 2% more than in 2021 and 5% more than in the previous report of ACFE in 2020. In view of the rapid development of information technologies over the past decades, it is possible to single out a separate group of fraud - Internet fraud. Every day, citizens of absolutely all countries bear huge losses, becoming victims of fraudsters on the Internet. Yes, hardware and software are improving every day becoming more secure, but at the same time, offenders are also improving their skills and overcoming newly created network barriers. Unfortunately, the law enforcement system does not always keep up with technological development, and previous action protocols are losing their relevance not later than today.

The purpose of the article is to clarify foreign experience concerning legal regulation of fraud investigation.

1. Literature review

A.O. Yeremenko and A.M. Klochko note in their research that among all types of fraudulent acquisition of other people's funds on the Internet, the most prominent and insufficiently researched ones are phishing, vishing, and farming and they are qualified as hacker actions (Klochko & Yeremenko, 2016). It should be noted that the problem of cyber fraud was considered by the researchers at the time of publication of their works, and characteristics of this type of offense lose their relevance every day due to the rapid development of IT technologies, and as a result, methods, techniques, and awareness of fraudsters are being improved. In the article we will perform a criminal analysis of modern types of fraud on the Internet with the help of statistical data of different countries concerning this category of offenses.

M.S. Oktiabreva notes that the term "carding" refers to fraudulent transactions with payment cards (card details) not approved by their card holders. Carding includes the following various methods of deceiving legitimate owners of material assets: a) theft or illegal acquisition of a card - it is either a physical influence on the owner, or search for a vulnerability in the process of issuing, delivering or issuing a bank product and use of the stolen card by an evil-doer; b) compromise of card data for further production of a counterfeit. First of all, it is about copying data of the magnetic strip of the card and theft of the PIN code. This type of fraud was most widespread before the mass transfer of cards to chip technologies. Today, this scheme is rare, since almost all over the world "Chip Liability Shift" is in force, that is, the acquiring bank's obligation to service a chip-based card exclusively with the use of its chip; c) compromise of card details for carrying out operations without actual presence of the card. An outstanding example is payment for purchases or services on the Internet. The ultimate goal of offenders in all cases is to obtain access to money. In order to implement their plans, fraudsters invent extremely cunning schemes, often taking advantage of gullibility and inattention of citizens (Oktiabreva, 2014).

Another group of authors emphasizes that it is of great importance to determine criminalistic features of the initial stage of investigating frauds with financial resources in cyberspace, essence of such frauds, their analysis and justification as one of the types of cybercrime that is dangerous for everyone, as well as proving the need to take urgent measures aimed at preventing and countering such criminal offenses (Reznik ect, 2021).

2. Materials and methods

The research is based on the works of foreign and Ukrainian researchers, as well as on theon the empirical material of national and international legal acts and juridical (forensic) practice.

Comparative analysis and a dialectical method of cognition made it possible to comprehensively research foreign experience in the sphere of legal regulation of fraud investigation. With the help of a synthetic method, peculiarities of the foreign experience in legal regulation of fraud investigation.

3. Results and discussion

Professional frauds are serious and growing problems (Kamlyk, 2005). With the help of experts in economic crimes, it is possible to identify main features of frauds, establish the guilty parties and even recover assets. American experts from the ACFE suggested to distinguish three main categories of fraudulent schemes:

1) misappropriation of assets through false billing, payment information, fraud and skimming;

2) corruption, by means of receiving or offering a bribe or demanding funds from third parties;

3) financial reporting provided fraudulently, i.e. preparing a report showing fictitious income or concealing expenses or liabilities.

Of these three categories, misappropriation of assets is the most common one; it accounts for nearly 89% of all reported cases in the research. In fact, hostile takeovers are often performed for this purpose. According to ACFE, this category of fraud has the lowest amount of losses - the average cost is $ 150,000.

Economic offenses related to financial reporting are the least common. However, their losses are the highest: in the result of such offences companies lose about $2 million.

The most common types of fraud from the first category (misappropriation of assets) are presented as payment schemes; the purpose of payment schemes is to create fictitious companies and to issue employer's accounts for non-existent services. Skimming (transactions with bank cards) occurs when an employee accepts client's payments without confirming sales documents. Other common fraud schemes include theft of monetary funds and property, falsifying inventory results, leaking trade secrets or confidential customer

information, submitting false expense reports. Of the 1388 economic offenses investigated, 1379 ones contain information about fraudulent schemes and, as a result, the average amount of losses in USD. The latter amount to 140,000 dollars, and more than one fifth of cases related to losses in the amount of 1,000,000 dollars.

Rapid revealing of fraudulent schemes is often the most critical aspect in the process of crime detection. Decisions must be made quickly in order to provide evidence, reduce losses, and effectively investigate fraud strategies. By means of investigating fraud methods a company can prevent similar schemes in the future, gain experience and test similar types of abuse (Nikolaiuk, 2005).

Average fraud losses detected through internal audit ($81,000), document review ($105,000), IT control ($110,000), management control ($123,000), and account control ($124,000) were significantly lower. This last group of detection methods reflects proactive measures taken by organizations to stop fraud.

The risk of auditor's identifying significant reporting irregularities due to frauds performed by management personnel is higher than due to frauds performed by lower employees. The reason is that higher-level workers have more authority. This gives them an opportunity to bypass control procedures designed to prevent similar frauds performed by lower-level employees. Using their official position, management personnel can induce employees to perform certain illegal actions or require them to help in committing fraud (Krutov, 2008).

There is no doubt that there is a great advantage in detecting fraudulent schemes just before they are implemented, in particular this advantage consists in an ability to limit the financial and reputational damage caused by offenses. When analyzing duration of professional frauds, one can have an idea of possible areas of company's activity where cases of economic offenses occur. Average duration of an offense is the amount of time from the moment when the possibility of a fraud was considered until it was discovered - in all cases of the research it is 18 months. However, duration of cases in each category of fraud was ranging from 12 months (for cash schemes of payments and non-cash payments) to 36 months (for salary projects).

To identify the most common prevention methods, a specially designed system is needed to assist individuals in finding information (Kamlyk, 2005).

DOI: http://dx.doi.org/10.46925//rdluz.38.11

Such tools as anonymous hotlines or online portals that give people an opportunity to report abuse without fear of reprisal or being identified can help to facilitate this process. There are several reasons why a person may want to be anonymous when providing information to prevent a fraud; and available data indicates that a significant number of alerts were sent anonymously (12%).

The presence or absence of a hotline has an interesting effect on frauds. For example, organizations with some form of hotline organization at the local level are much more likely to detect fraud (51%) than those without such arrangements (35%).

Another major difference between these two classes of organizations is observed in frauds discovered by chance. The share of incidentally detected fraud in organizations with a hotline is less than 3%, compared to 11% or more in organizations without a hotline.

About 40% of the affected organizations considered in the research were private companies, and 28% of researched organizations were public companies, meaning that more than two-thirds of the victims considered in the research were non-profit organizations. This division corresponds to the previous ACFE reports. Non-profit organizations are the smallest part of the data set; they account for slightly more than 10% of all registered cases.

Small organizations (with fewer than 100 employees) are still the most common victims of fraud, although the overall difference between the categories is relatively small. In addition, small enterprises make up the majority of commercial organizations in many countries, so the distribution of cases is being skewed towards large organizations (Yefimov, 2021).

This difference is due to at least partly greater propensity of large organizations to create conditions for reduction of fraud, or to employ certified experts dealing in investigation of plundering (thievery) and officially investigating cases of fraud. However, ACFE's observations have shown that small organizations (with less than 100 employees) and medium-sized organizations (with 100 to 999 employees) have a constant increase in fraud losses in comparison with their counterparts with more employees. This reflects a significant share of fraud in small organizations. That is why they need to employ certified experts dealing in investigation of plundering (Leheza ect, 2020).

Due to limited resources, small businesses may be particularly devastated through the loss of money in the result of fraud. Unfortunately, in the result of restrictions most small

organizations often make a minimum of investment to fight fraud, and due to this fact these organizations are more vulnerable to economic abuses.

According to recently reported data, the US Federal Trade Commission received more than 2.1 million fraud reports in 2020, with impostor frauds remaining the most common type of fraud reported to the agency (Leheza ect, 2021).

Online shopping was the second most common category of fraud reported by consumers, and it was boosted by a spike in reports in the early days of the pandemic. Lotteries, contests, Internet services, prizes, telephone and mobile services have highlighted five most common categories of fraud.

Consumers reported losses of more than $3.3 billion in the result of online fraud in 2020 compared to $1.8 billion in the previous year. Almost $1.2 billion losses reported in 2019 were attributed to impostor fraud, while online shopping accounted for about $246 million of reported losses. Just over a third of consumers who filed a fraud report to the RTS (and namely 34% of consumers) reported about losing money, compared to 23% in 2019

In November 2020, a citizen of India was sentenced to 20 years in prison and 3 years of supervised release for his involvement in a fraud which resulted in losses to US citizens by millions of dollars. He was responsible for the operation and financing of a call center in India between 2013 and 2016. The District Court of the Southern District of Texas also ordered Hitesh Hinglaj (a citizen of India) to pay a compensation in the amount of $ 8,970,396 (Yefimov, 2021).

The global practice distinguishes the following main types of fraud using computers and the Internet: sniffing, vishing, phishing and carding.

“Crelan Bank” in Belgium became a victim of a fraud with commercial e-mail which cost the company approximately $ 75.8 million. This type of attack involved the fraudster compromising the account of a high-level executive in the company and instructing his employees to transfer money to an account controlled by the evil-doer. The phishing attack of the “Crelan Bank” was discovered during an internal audit and the organization was able to cover the losses because it had sufficient internal reserves (Leheza ect, 2018).

The Austrian manufacturer of aerospace parts “RASS” also lost a significant amount of money due to a commercial impersonation scam. In 2016, the organization announced an attack and found out that the attacker posing as the company’s CEO instructed an

DOI: http://dx.doi.org/10.46925//rdluz.38.11

accounting employee to send $61 million to a bank account controlled by the attackers. This case was unusual, as the organization decided to dismiss and take legal action against its CEO and CFO. The company demanded that the two executives reimburse the losses of $11 million due to their improper implementation of security controls and internal supervision, which could have prevented the attack. This claim demonstrated the personal risk to organizational leaders in case of their failure to perform proper cyber security checks (Leheza ect, 2021).

In 2015 "Ubiquiti Networks" (a US-based computer networking company) was the victim of a phishing attack that cost the company $46.7 million. The attacker posed as the CEO and attorney of the company and instructed the company's chief accountant to make a series of wire transfers in order to cover a secret acquisition. Within 17 days the company made 14 bank transfers to accounts in Russia, Hungary, China and Poland. The incident attracted attention of "UbiquitiNetworks" only when the FBI reported that the company's bank account in Hong Kong might have become a victim of fraud. This gave the company an opportunity to stop any future transfers and try to recover as much of the stolen 46.7 million dollars as possible (which amounted to approximately 10% of the company's cash position) (Yefimov, 2021).

Conclusions

Thus, professional fraud is a global problem. Although some results vary from country to country, most of the trends in fraud schemes and the fight against them are similar regardless of where the crime occurred.

One of the key tasks of law enforcement agencies is to create an effective and stable system of training specialists who will possess technologies for investigating crimes related to the legalization (laundering) of illegal income, in particular, income obtained through fraudulent accounting schemes. Also, in order to prevent criminals from using incomes obtained fraudulently, it is reasonable to apply measures of timely seizure of assets in accordance with the cases.

In order to minimize fraud and abuse, a company needs to improve internal controls, independent audit, and it should also optimize and improve supervisory functions.

It has been found that the number and variations of Internet fraud methods are growing literally every second. Offenders use the latest technologies and equipment, adapting them very quickly to their criminal goals; they get adapted to the growth of progress by means of developing new fraud schemes. Among all types of Internet fraud, we can single out the main and most common ones including phishing, sniffing, vishing, and carding. Internet users, bank card holders and any ordinary citizens need to be familiar with modern methods of Internet fraud. In particular, you should be very careful when using online banking, mobile communication, making purchases in online stores; you should be careful when disclosing your personal data when entering information into forms on various web-sites.

References

Kamlyk, Mykhailo (2005). Economic security of business activity. Economic and legal aspect: education. manual Kyiv: Attica. Ukraine.

Klochko, Anatolii; Yeremenko, Anton (2016). Fraud using bank payment cards. Legal scientific electronic journal. No. 1, P. 82-86.

Krutov, Volodymyr (2008). Dictionary of non-state security system terms. KROK University, Kyiv. Ukraine.

Leheza, Yevhen; Tiutchenko, Svitlana; Stanina, Olha; Shatrava, Serhii; Rezanov, Serhii (2021). Uso y protección del suelo: regulación legal y experiencia extranjera. *Revista De La Universidad Del Zulia*, 12(33), P.70-81. DOI: https://doi.org/10.46925//rdluz.33.06

Leheza, Yevhen; Dorokhina, Yuliia; Shamara, Oleksandr; Miroshnychenko, Serhii; Moroz, Vita (2021). Citizens 'participation in the fight against criminal offences: political and legal aspects. *Cuestiones Políticas*, 39(69), P. 212-224. DOI: https://doi.org/10.46398/cuestpol.3969.12

Leheza, Yevhen; Filipenko, Tatiana; Sokolenko, Olha; Darahan, Valerii; Kucherenko, Oleksii (2020). Ensuring human rights in ukraine: problematic issues and ways of their solution in the social and legal sphere. *Cuestiones políticas*. Vol. 37 №º 64 (enero-junio 2020). P. 123-136. DOI: https://doi.org/10.46398/cuestpol.3764.10

Leheza, Yevhen; Savielieva, Maryna; Dzhafarova, Olena (2018). Structural and legal analysis of scientific activity regulation in developed countries. *Baltic journal of economic studies*. 4(3), P. 147-157. DOI: https://doi.org/10.30525/2256-0742/2018-4-3-147-157

Nikolaiuk, Serhii (2005). Security of business entities. Course of lectures. Kyiv. Ukraine.

Oktiabreva, Maryna (2014). Carding in Russian practice. Economics and management: analysis of trends and development prospects. 15, P. 99-103.

Reznik, Oleg; Fomenko, Andrii; Melnychenko, Andrii; Pavlova, Natalia; Prozorov, Andrii (2021). Features of the initial stage of investigating fraud with financial resources in cyberspace. *Amazonia Investiga*, *10*(41), P. 141-150 DOI: https://doi.org/10.34069/AI/2021.41.05.14.

Yefimov, Mykola (2021). Forensic analysis of certain modern types of fraud: problematic issues. Collection of scientific works "*Scientific Bulletin of Public and Private Law*". Issue 5. P. 116–121.