www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

Use of Electronic Means of Payment as Ways of Crime Commission: Features of Investigation and Protection Routes

V. Vasyukov[1]; Elena F. Tsokur[2]; Evgeniy V. Kirichenko[3]; Valentina Romanovna Bugrova[4]; Natalia Grigoryevna Bondarenko[5]

[1]Moscow State Institute of International Relations (University), Russia.
Orel Law Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov, Russia.
[2]Southwest State University, Russia.
[3]Kuban State Agrarian University named after I.T. Trubilin, Russia.
[4]Russian State University of Tourism and Service, Russia.
[5]North Caucasus Federal University, Russia.

Abstract
The article deals with electronic payment systems and means as methods of committing criminal encroachments on material and other objects belonging to citizens and organizations. Electronic payment systems and means which have become widespread in recent years have proven vulnerable to various types of criminals using this vulnerability for various purposes, including personal gain. The purpose of this article is a comprehensive analysis of criminal encroachments on electronic payment systems and funds carried out for personal gain to determine the way for law enforcement agencies to counter them. The authors outline the concept of such systems and means according to the norms of the current legislation, as well as the methods of committing crimes in this area identified in forensic science. There is a description of elements of such crimes contained in the criminal legislation of Russia and several countries. Some problems associated with difficulties in qualifying crimes using electronic payment means have been identified. The authors' conclusions about the need for the further scientific and practical study of qualification of criminal liability for theft using electronic payment means are presented.

Key-words: Theft, Fraud, Material Gain, Computer Equipment.

1. Introduction

With the scientific and technological progress, the information environment inevitably expands and gradually begins to cover almost all areas of a modern person's life, including commodity-money relationships and the market economy. Currently, the parties increasingly often

pay for transactions with deposit or credit cards or the contactless payment method, as well as using mobile devices with pre-installed software [21, 23]. For example, the Android operating system and IOS for smartphones, tablets, and watches contain software that allows one to pay for goods and services by bringing a mobile device next to a cash register. Criminal actions using electronic means of payment (EMP) do not lag behind, trying to develop and keep up with the information and computing environment of a modern, comprehensively developed society. The latest trend in modern society is the improvement of the forms and types of theft aimed at bank cards, electronic wallets, and other electronic payment systems (EPS), among which fraud is in the lead.

The number of cases of fraud and theft related to electronic payments is growing steadily [1]. Moreover, at the present stage, there are already cases of cyberattacks that have led to very serious consequences for consumers. For example, in 2016 in the UK 9,000 accounts of Tesco bank customers were hacked and £2.5 million was stolen [2] (another source mentioned 20 thousand accounts [3]). Furthermore, due to the cyber attack, the bank's clients were unable to carry out online transactions for 48 hours [3]. In India, 3.2 million debit cards were also attacked in 2016. As a result, it was necessary to change the security codes of all hacked cards since clients could lose their money due to the fraudsters' actions [4].

In recent years, the Bank of Russia has also recorded a sharp increase in unauthorized transactions with bank customers' accounts. In most cases, these operations occur through spoofed telephone numbers using social engineering [22].

Crime makes progress and quickly responds to the innovations introduced in society while improving the methods and means of committing theft, the subject of which is electronic, non-cash money, money in Internet wallets, and other EPS. The means of committing fraud using EPS are becoming more sophisticated, and the methods of such attacks are also diverse, developing in parallel with the information-computer, electronic-digital environment of modern society.

Therefore, the issue of personal security and protection of personal data remains an urgent problem today. An increasing number of people are involved in fraudulent schemes, and the number of victims from the less protected layers of the population – the retired – is growing. This issue has long been the subject of debate in scientific circles and, as a result, requires careful research. The problems associated with combating crimes committed using electronic payment means have been considered by many scientists. Among the many studies available in the public domain, it is worth noting the works by E.D. Pidusov [5], N.V. Olinder [6], and E.A. Markova [7]. However, the emergence of more payment methods and schemes, the use of high-tech payment solutions accompanied by the emergence of new criminal schemes requires constant monitoring by regulators,

caution from users, and the search for both technical protection opportunities and legal protection of the relevant relationships from the scientific community. Thus, there is no doubt about the demand for and the relevance of new scientific developments in the legal security of EPS and funds. Research hypothesis. Currently, the establishment of specific elements of the crime that entail criminal liability for theft committed using computer technology in EPS does not seem justified.

2. Methods

When conducting research within the framework of this study, the dialectical method of cognition of reality became the fundamental method. Moreover, we used the methods of analysis and synthesis, statistical, formal legal, and comparative legal methods. The theoretical framework of this study was the works by researchers in the field of criminal law and forensic science. The regulatory framework included the criminal legislation of Russia and the developed countries of the world, regulations governing the use of EMP. The study used statistical data presented, among other things, on the official websites of Russian government agencies.

3. Results

Currently, the service of credit, financial, and banking institutions allows one to carry out payment transactions remotely, manage accounts from any part of the planet using the Internet (Internet banking, mobile banking, etc.), a contactless payment method, and specialized software installed on mobile devices. The concept of "EMP" is used both in relation to payment cards and computer services, such as programs "Yandex.Money", "Webmoney", "Qiwi", etc., Internet banking systems, various electronic media using technologies of contactless payment, etc. The term "EMP" was enshrined in Article 3 of the Federal Law № 161-FZ dated 27 Jun. 2011 "On the National Payment System" [8] (hereafter – Payment System Law) and understood as "an instrument and/or a method that allows a money transfer operator's customer to prepare, certify, and send funds transfer instructions within the framework of applicable forms of cashless transfers using information and communication technologies, electronic data media, including payment cards, and other technical devices". However, the current legislation does not regulate all types of payments using electronic instruments and EMP. In particular, payments in online games, as well as the use of cryptocurrencies, remain outside the scope of legal regulation. The activity of EPS and the performance of legal actions of clients there is formalized by the adoption of regulations and the signing of agreements in

electronic form, which are equivalent to those drawn up in a simple written form and certified by the client's signature. The low level of control over such operations by the state leaves this system vulnerable to illegal encroachments. Among them, thefts committed in the field of electronic payments hold a prominent place [5].

One of the most important elements of the forensic characterization of crimes committed using EMP is how the crimes are committed. In the considered category of crimes, two main ways of their commission can be distinguished: - exploitation of the vulnerability in EMP not associated with illegal use of the legitimate user's account data; - unlawful (illegal) use of the account that belongs to a legal user of EMP. Considering the first method, vulnerability is a property that characterizes the likelihood of damage to the payment system by various external factors (means) [5]. The possibility of using (exploiting) the EMP vulnerability arises because this software and hardware system is formed by numerous subsystems and interacting computer networks, which creates an extremely complex operating environment where developer errors, the effects of incorrect interaction of subsystems, etc. are possible. Criminals successfully use these identified features of the functioning of EMP, preparing and directly committing their criminal acts [9]. For example, to commit one of the crimes, cybercriminals conducted extensive research, examining more than 50 payment gateways (services that authorize transactions, for example, "Yandex.Checkout") in an EPS [10]. As a result, the way of committing a crime using EMP becomes extremely complex and consists of several stages: preparatory, working, and final. At the preparatory stage, hackers search for vulnerabilities. To do this, the offenders must have sufficiently deep knowledge in the field of both the general technology of EMP functioning and its software and hardware features. Once vulnerabilities are discovered, these vulnerabilities are tested. Another feature of this type of crime is that, having discovered vulnerabilities in the operation of the EPS and developed the appropriate software that allows them to be exploited, criminals often sell their results as an instrument of committing crimes to other interested parties using specialized closed forums of hackers. At the working stage, the identified vulnerability is exploited without the illegal use of a legal user's account data [5]. Digital currency from the user's account is transferred to temporary accounts in the same or different EPS. After that, there is a chance to cash these funds. The purpose of the final stage is the withdrawal of funds from the EPS by members of the criminal group, who subsequently distribute the money among themselves. However, as N.V. Olinder notes, in most cases, criminals anonymously resell stolen funds at an undervalued rate to hide the traces of their criminal actions [6].

The second way is the unlawful use of the access details that belong to the legal user of the EPS. This method is most common due to insufficient attention of EMP owners to the safety of their

account data. At the preparatory stage, cybercriminals infect a user's computer with malicious software. Then the process of the secret collection of confidential computer information begins, including data on the password and login of the account of the EPS. The received data on the details that belong to the legal owner of the EMP and the stolen account data of other clients of this system are arranged in a special array. Such arrays are sold to other members of the criminal group who carry out the withdrawal of money from the system through the direct commission of a cybercrime [11]. At this stage of committing a crime by the considered method, there is no need for in-depth knowledge of the technology of EPS operation, especially of their server part, since the user's computer is attacked, and not the payment system itself. It is from the user's computer that the access details for the electronic account are entered, and it is on this computer that key files are stored containing the specified details in the encrypted form [12]. In the process of preparing to commit a crime, criminals only need to obtain the most basic information about the functioning of the most common operating systems and applications. Due to the use of counterfeit software by many EMP owners, which is never updated (or is updated rarely, from time to time), it becomes extremely vulnerable to a wide range of malware. At the preparatory stage, criminals remotely diagnose the computer's software environment. After that, considering the identified features of this environment, criminals select suitable malicious programs that will be used at the next (working) stage to commit criminal acts or as a basis for the development of a new malicious program capable of performing the required functions. At the working stage, with the help of a malicious program (programs), criminals receive the access details of a legal user of the EPS [5]. It should be noted that hundreds of computers can be infected by malware. As a result, criminals have access to a whole array of account data for various EPS, which are usually sold on closed hacker forums. Anonymous purchasers of information about the username and password of a user account use this data to illegally transfer digital currency on a legal user's behalf to temporary accounts in this or another EPS. After that, criminals can cash the stolen funds at any time [5].

Criminal law considers the issue of qualification of the above methods of theft using EMP as follows. Thus, for example, if the data could be obtained as a result of hacking technical means and used to obtain funds, then the legislator defines this act as fraud in the field of computer information (Article 159.6 of the Criminal Code of the Russian Federation [13]). Fraud will also occur when the person who stole non-cash funds used any confidential information, thanks to which the person managed to get access to these funds (Article 159.3). It is also considered fraud when an attacker gains access thanks to a bank employee. If the criminal act was committed with the help of any data

of the account holder, then the act qualifies as theft. This is the position expressed by the Supreme Court of the Russian Federation in the Plenum resolution dated 30 Nov. 2017 № 48 [14].

It also indicated that the fraud should be recognized as completed from the moment when the stolen property came into the possession of the perpetrator and the latter received a real opportunity to use or dispose of the property as their own. Moreover, the Plenum also indicated that a person received such an opportunity only when electronic funds were credited to their or another person's account. With the combination of these circumstances, the fraud was considered completed.

In this case, the wording of Article 159.6 of the Criminal Code of the Russian Federation seems unclear. Article 159 defines fraud as "theft of someone else's property or the acquisition of the right to someone else's property by deception or abuse of trust". Article 159.6 describes an activity that does not contain elements of the act specified in paragraph 1 of Part 1 of Article 159 – this is a hacking of the payment system and theft of property without any communication with the victim, there is no deception or abuse of someone's trust. Therefore, such an act is theft, and the corresponding wording is more suitable for Article 158 (theft). Furthermore, the disposition of Article 159.6 competes with some dispositions of articles of Chapter 28 where the interest in personal gain is indicated as a qualifying feature (part 2 of Article 272, part 3 of Article 273). These inconsistencies may contribute to improper enforcement and should be eliminated by the legislator.

4. Discussion

Due to the noted shortcomings in the qualification of theft with the use of EMP in Russian criminal law, the criminal law regulation of similar theft in international practice is of interest.

In the United Kingdom, various statutes establish liability for computer crimes: the Computer Misuse Act, the Telecommunications (Fraud) Act, the Electronic Communications Act, and the Personal Data Protection Act, the Television Licenses (Disclosure of Information) Act, and the Social Security Fraud Act [15]. However, none of the statutes above directly establishes responsibility for theft in the field of computer information. The Computer Misuse Act provides for liability for unauthorized access to computer material; unauthorized access with the intent to commit or facilitate the commission of further offenses; unauthorized actions with the intent to cause damage in relation to a computer malfunction, etc.; unauthorized actions that cause or create a danger of significant damage; manufacture, supply or receipt of products for use in the above offenses. In other words, in different cases computer information could be the subject of a crime, the object of a crime, finally, a means, a method of committing a crime.

In 1986, the United States passed the Computer Fraud and Abuse Act. Section 1030, Chapter 47, Title 18, of the US Code which established liability for fraud by accessing a computer became part of that Act [16]. According to this norm, criminal liability arises for access to a computer carried out with fraudulent intentions, and its use to obtain anything of value through fraud, including illegal use of computer time worth more than 5 thousand dollars during the year, that is, without paying for use computer networks and services. Thus, by US legislation, computer fraud is delimited from traditional fraud. Its essence is access to a computer and the use of a computer.

In the French Criminal Code, the rules providing for liability for computer crimes are contained in two books. Thus, the second book "On Crimes and Misdemeanors against the Person", containing the chapter "On Attacks on the Person", includes elements of such crimes as illegal actions with personal data in telecommunications systems. The third book "On property crimes and misdemeanors" contains the chapter "On encroachments on automated data processing systems", the norms of which provide for criminal liability for its illegal use. Therefore, personal data, as well as telecommunication systems, are subject to criminal law protection. The French Criminal Code does not contain special rules on thefts committed with the use of computer information [17].

In the Criminal Code of the Federal Republic of Germany, computer fraud is a separate crime, paragraph 263a establishes responsibility for actions to obtain unlawful material gains for oneself or a third party, which harm another person's property by influencing the result of computer data processing by creating incorrect programs, using wrong or incomplete data, unauthorized use of data or other unauthorized influence on the data processing. In this case, computer information acts as a way of committing theft [18].

Article 246-11 of the Penal Code of Japan includes liability for the unlawful gaining of profit by making an electromagnetic record that is contrary to the truth. Namely, it is established that a person who, by submitting falsified information or an illegal command to a computer used in another person's professional activities, has provided for use in conducting another person's affairs an electromagnetic record contrary to the truth regarding the acquisition, loss or change of property rights and thus acquired an illegal property benefit or allowed this to another person, is punishable by imprisonment with forced physical labor for a period not exceeding 10 years [19]. Moreover, in Japan, illegal hacking into computer systems and information networks for theft, damage to information, as well as use to generate income and cause damage to legitimate owners, is criminalized in the 2000 Law on Unauthorized Computer Access.

The application of the approach when criminal liability is provided for not only by the criminal code but also by a special law, according to O.S. Guzeeva, would be an efficient measure to combat crimes committed in the Russian segment of the Internet [20].

Therefore, at present, different approaches are used in the criminalization of thefts committed using computer information. Some countries, for example, the US, the UK, and France use general rules on property crimes in relation to theft through unauthorized access to EMP with the application of provisions reflecting the constituent elements of acts such as unauthorized access, interference with personal data, and other information security crimes. In other countries, such as the Federal Republic of Germany and Japan, thefts committed using computer information form separate elements in the system of property crimes. Most of such acts are recognized as theft in the form of fraud and are prohibited either by the main criminal law of the country, or special law, or both.

As for the qualification of theft committed by influencing EPS in the legal field of the Russian Federation, it seems appropriate to reason as follows. To steal someone else's property or obtain the right to it, a hacker penetrates computer systems, real data streams which are not a place for storing property but only allow access to the property when certain actions are performed. The property does not come to the perpetrator's disposal with the owner's consent but secretly from the owner. The fact of such transfer of property does not indicate that the victim is misled, deceived, and personally transfers their property. Illegal actions in information networks, the introduction of viruses, alteration of computer data "force" the program to function differently eliminate obstacles to turning other people's property into the hacker's possession and do not induce the victim to transfer what belongs to the hacker. Under such circumstances, actions aimed at illegally taking possession of property or acquiring the right to the property, carried out using computer information cannot be recognized as fraud but should be qualified as theft in the form of larceny. In this regard, it seems necessary to additionally qualify such an act as larceny. However, the legislator does not notice the erroneous design of the current criminal law, which establishes responsibility for thefts committed using computer information. To resolve issues of qualification of the relevant socially dangerous acts in the simplest way, it is proposed to exclude the provision of Article 159.6 of the Criminal Code of the Russian Federation and the criminal law prohibition to be formulated more abstractly.

5. Conclusion

Therefore, the following conclusions can be drawn. The development of EMP and EPS that ensure modern property turnover along with vulnerabilities in their technical security, create a

favorable environment for the actions of criminals who use the knowledge in the functioning of these systems and means to take possession of other people's property. In forensic science, the classification of such crimes has been carried out, the means of committing them have been disclosed, methods have been developed for detecting traces of the commission and searching for criminals. At the same time, criminal legislation cannot keep up with high-tech and innovative EPSs and, as a rule, does not reflect all the features of criminal encroachments on EMP and EPS. Therefore, the correct approach for the legislator to the formulation of norms on criminal liability seems to be more abstract, combining general norms on property crimes related to the use of EMP, with the formulation of general concepts reflecting the use of computer hardware and software to commit such acts. Thus, the hypothesis of the study appears to be proven.

References

Achord, S., Chan, J., Collier, I., Nardani, S., & Rochemont, S. (2017). *A Cashless Society: Benefits, Risks and Issues* (Interim paper), Institute and Faculty of Actuaries, 149.

Treanor, J. (2016). *Tesco Bank Cyber-Thieves Stole £2.5m from 9,000 People.* The Guardian.

Morrison, C. (2018). *Tesco Bank Fined £16.4m over Cyber Attack.* Independent.

Shukla, S., & Bhakta, P. (2016). 3.2 Million Debit Cards Compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit. *The Economic Times. E-Paper*.

Pidusov, E.D. (2020). Forensic analysis of crimes committed with the use of electronic payment systems. *Vestnik Voronezhskogo instituta MVD Rossii.* 4, 224-229.

Olinder, N.V. (2014). Typical means of committing crimes with the use of electronic payment means and systems. *Ekspertkriminalist, 1,* 13.

E.A. Markova, E.A. (2020). Issues of qualification of fraud with the use of electronic payment means. In the collection: Law enforcement activities of the internal affairs bodies in the context of modern scientific research. *Proceedings of the regional scientific and practical conference.* Compiled by A.A. Sarsenova, E.Kh. Mamedov. 139-142.

Federal Law "On the National Payment System" (as amended on 22 Dec. 2020) (in force from 1 Jan. 2021) - http://docs.cntd.ru/document/902286143

Repin, M.E. (2018). Ways of committing fraud with the use of bank cards. Forensic science in the context of the development of the information society (59th annual forensic readings): *proceedings of the international scientific and practical conference.* M.: Akademiya upravleniya MVD Rossii, 238.

Capturing data: how money is stolen from bank cards.

https://www.gazeta.ru/tech/2019/07/30/12543445/skimming.shtml

The Archive of the Sverdlovsk District Court of Kostroma. Criminal case № 1-448/2016. https://rospravosudie.com/courtsverdlovskij-rajonnyj-sud-g-kostromy-kostromskayaoblast-s/act-535682824/

Yu. V. (2016). Electronic payment security. *Proceedings of the 14th International scientific and practical conference,* Ufa: Aeterna, 208.

Criminal Code of the Russian Federation (as amended on 30 Dec. 2020. http://docs.cntd.ru/document/9017477

The Plenum resolution of the Supreme Court of the Russian Federation dated 30 Nov. 2017 № 48 *"On Judicial Practice in Cases on Fraud, Misappropriation and Embezzlement"*. https://www.garant.ru/products/ipo/prime/doc/71723288

Jahankhani, H., & Al-Nemrat, A. (2015). *Hosseinian-Far Cybercrime classification and characteristics.* Cyber Crime and Cyber Terrorism Investigator's Handbook. Waltham, 393.

Khilyuta, V.V. (2013). A theft using computer equipment or computer fraud? *Biblioteka kriminalista, 5*(10), 55-65.

The French Criminal Code. (2002). Scientific editing by L.V. Golovko, N.E. Krylova; translated from French by N.E. Krylova. SPb.: Yurid. tsentr Press, 650.

The Criminal Code of the Federal Republic of Germany. (2003). Scientific editing by D.A. Shestakov; translated from German by N.S. Rachkova. SPb.: Yurid. tsentr Press, 524.

The Penal Code of Japan. (2002). *Scientific* editing by A.I. Korobeev; translated from Japanese by V.N. Eremin. SPb.: Yurid. tsentr Press, 226.

Guzeeva, O.S. (2014). Criminal policy in respect of crimes committed in the Russian segment of the internet. *Zakony Rossii: opyt, analiz, praktika, 6,* 74-77.

Dudin, M.N., Frolova, E.E., Lubenets, N.A., Sekerin, V.D., Bank, S.V., & Gorohova, A.E. (2016). Methodology of analysis and assessment of risks of the operation and development of industrial enterprises. *Calitatea, 17*(153), 53.

Sekerin, V.D., Dudin, M.N., Gorokhova, A.E., Gayduk, V.I., & Volkov, V.I. (2019). Creation of a Virtual Image: Digital Technology of the 21st century. *Amazonia Investiga, 8*(20), 340-348.

Sekerin, V.D., Dudin, M.N., Gorokhova, A.E., Kondrashova, A.V., & Blinkova, E.S. (2019). Mathematical Modeling of the Analysis of Medical Services at the" Prevention" Stage through Quality Indicators. *Quality-Access to Success, 20*(173).