Advances in Economics, Business and Management Research, volume 138
2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)

The Experience of Foreign Countries in the Prevention of Fraud Using Electronic Means of Payment

Shavaleev B.E.

Kazan Law Institute of the Ministry of Internal Affairs of Russia, Kazan, 420108
Email: shavaleev.bulat@gmail.com

ABSTRACT
The article examines the experience of foreign countries in the field of preventing illegal transactions using electronic means of payment, analyzes criminal law, organizational and other measures aimed at eliminating the causes and conditions of the crime, and victim behavior of the population. Based on the studied foreign experience, we formulate some proposals for their integration into domestic law and other recommendations in order to effectively prevent the investigated illegal act.
Keywords: *warning, prevention, electronic means of payment, fraud, foreign countries*

1. INTRODUCTION

An increase in the share of non-cash payments using electronic means of payment in the total volume of transactions is typical for most foreign countries. According to the annual report on the state of commodity-money relations in the world, the World Payments Report, published by the world's largest management and information technology consulting company Capgemini, this trend is caused, first of all, by the positive dynamics of the integration of innovative technologies [1].
Cashless payments are the main method of payment for trading operations performed remotely, mainly on the Internet. The transition to non-cash payment of goods and services, according to retailers, can reduce the costs of entrepreneurial activity, increase the transparency of financial transactions [2].
Electronic means of payment have become the main tool for providing comprehensive services to economic entities due to their speed, relative security of transfers and ease of settlements. However, the dynamic development of the sphere of non-cash payments has contributed to the emergence of new forms of criminal encroachment, associated with the unlawful use of electronic means of payment, the purpose of which is the theft of electronic money.
We assume that studying the experience of foreign countries will have a positive impact on the effectiveness of preventing this category of crimes in the Russian Federation, since the implementation of preventive measures abroad stanted more than seventy years ago when the first payment cards appeared.

2. THE DEPTH OF RESEARCH

The experience of foreign countries in the field of crime prevention in general, as well as certain types of crimes, including fraud, was highlighted in the studies of the following domestic authors: V.D. Malkov [3], G.G. Shikhantsov [4], L.M. Prozumentov, A.V. Shesler [5], S.V. Sheveleva, A.A. Grebenkov, V.E. Novichkov [6], S.L. Alekseev, R.R. Salimzyanova [7], Y.I. Gilinsky, Yu.V. Morozova, P.V. Fedyshina [8]. However, the experience of foreign countries in the field of fraud prevention using electronic means of payment has not been sufficiently studied. Among the foreign scientists who investigated this phenomenon, the following should be noted: L. Fernandes [9], M.G. Rachavelias [10], M. Mazitova [11], Akshada K. Dhakade, K.K. Chhajed, A.S. Kapse [12], C. Tancock [13] and many others.
We have studied criminal law, organizational and other measures in the field of fraud prevention using electronic means of payment in foreign countries.

3. PAPER STRUCTURE

The text is organized as follows. Section 4 gives the analysis of international trends in the field of fraud using electronic means of payment. Section 5 addresses the basics of international cooperation to prevent illegal transactions using electronic means of payment are presented. Section 6 suggests the priority measures for the prevention of illegal transactions using electronic means of payment studied. Section 7 summarizes the findings of our study.

4. INTERNATIONAL TRENDS IN PAYMENT FRAUD

At the end of 2019, less than 2% of settlements were made in cash in the Kingdom of Sweden [14], a similar situation is observed in the Kingdom of Denmark, the Republic of Iceland and the Kingdom of Norway [15]. In many modern countries, the volume of non-cash payments

exceeded 70% of the total volume of transactions as a result of the application of legislative measures to limit settlements using cash, which led to the need for additional legal protection of this sphere of public relations [16].

Since 2015, there has been a tendency in the European Union to reduce losses from illegal activities with electronic means of payment, however, in 2019, independent analytical agencies recorded an increase in losses from this type of crime in 19 European countries [17]. A distinctive feature of the mechanism of this act is the application of social engineering methods in order to obtain information about the owner of a bank card or its details, and the number of registered attempts to commit an illegal money transaction has also increased [18]. It should be noted that the criminal legislation of foreign countries is characterized by an expansive approach to understanding fraud using electronic means of payment, whereas in the Criminal Code of the Russian Federation [19], theft associated with the use of electronic means of payment, is allocated based on the method of the act.

The largest number of registered fraud cases using electronic means of payment among the EU countries is observed in the United Kingdom of Great Britain, the French Republic and the Russian Federation, which makes up 77% of the total number of detected cases of fraud, despite the fact that the French Republic and the United Kingdom of Great Britain have reduced the specific crime rates of this type are 6% and 8%, respectively. The most active growth of this type of illegal act was recorded in the following countries: the Republic of Austria (+ 20%), the Hungarian People's Republic (+ 14%), the Kingdom of Denmark (+ 7%), the Kingdom of Norway (+ 5%), the Polish People's Republic (+ 5%) [20].

This type of crime in the EU was detected only in a small number of countries, namely: the Kingdom of the Netherlands (-35%), the Hellenic Republic (-10%), the United Kingdom of Great Britain and Northern Ireland (-8%), the French Republic (-6%), the Portuguese Republic (-3%) and the Federal Republic of Germany (-2%), respectively, the study of the experience of these countries is of particular importance [21].

Compared to 1992, the United States of America (hereinafter referred to as the USA) managed to reduce losses from bank card fraud by 70%; in the EU countries, the implementation of preventive measures allowed to reduce losses from fraud by more than 75% compared to the level of the end of 1990 years, largely due to the effective international cooperation, technological improvement of electronic means of payment, updating security systems, etc [22].

5. THE BASICS OF INTERNATIONAL PAYMENTS FRAUD PREVENTION

The United Nations is actively involved in the prevention of electronic payment fraud. The UN assists the member states of the organization in developing strategies for the prevention of fraud using electronic means of payment, provides training for law enforcement officers to improve their skills, assists in the discovery and investigation of particularly complex criminal cases, and implements measures to identify transnational criminal communities. The International Criminal Police Organization (hereinafter - Interpol) and the European Union Police Service (hereinafter - Europol) play a key role in this area.

Prevention of this type of crime today is one of the priorities of Interpol, in the framework of which it interacts with financial institutions around the world, credit organizations, representatives of the sphere of goods and services.

Interpol created coordination banks to exchange information on fraud and other crimes using electronic means of payment using issuers of bank cards and electronic stores, that is, an online data bank. Information resource management comes from the Interpol Global Innovation Complex (IGCI), located in Singapore, founded in 2014 [23].

6. PRIORITY MEASURES FOR PAYMENT FRAUD PREVENTION

The basis of the package of measures to prevent fraud using electronic means of payment in foreign countries is the response of the bank. The development of the Real-Time Gross Settlement (RTGS) system, as well as the use of the latest transaction algorithms with additional information ISO20022, are more likely to identify an illegal transaction in the overall payment stream [24].

The introduction of information chips into bank cards capable of processing the properties and features of the operation, notifying the issuing bank of the conditions for the transfer has also made it possible to increase the security of cashless payments, that is, improving the technical support of payments is a necessary measure in preventing this type of crime.

In addition to banking programs to optimize financial activities, from the beginning of the 1990s, legal entities that offer services to analyze models of financial activities have been formed in the countries of the European Union, as well as to develop on the basis of the data obtained a program to combat illegal transactions. For example, Falcon Intelligence Network [25]. Program developers indicate that the complex of proposed solutions is regularly updated and supplemented, the staff of credit institutions periodically undergo additional training, which allows to maintain a satisfactory level of payment security. Today this software package monitors more than 9,000 transactions per second, 2/3 of all transactions in the world, respectively, the study of the features of this complex seems to be the most relevant.

It should be noted that a specific approach to the prevention of fraud using electronic means of payment implemented in the countries of Northern Europe is to organize preventive work with the public to bring the main ways of committing illegal activities, as well as measures

to ensure their own security in order to prevent victim behavior.

The main reason for the losses from fraud with electronic means of payment, the researchers consider to the imperfection of personal data protection mechanisms, which led to numerous leaks of information about customers of credit organizations and their subsequent use for criminal purposes.

Based on this, an important element in the system of measures to prevent fraud using electronic means of payment has become a set of solutions in the field of protecting user data from discredit.

An analysis of the legislation of foreign countries allows us to highlight the legal features of the normative regulation of criminal liability for committing fraud with electronic means of payment.

The first approach is the legislative consolidation of a set of rules that separately criminalize various types of acts involving electronic means of payment, for example, fraud, theft of electronic means of payment, and their falsification. This approach is typical for most countries in Europe, including the Russian Federation, that is, countries representing the continental legal family.

A fundamentally different approach is associated with the allocation in the criminal legislation of the country of a special design, in the structure of which acts related to the misuse of electronic means of payment are distinguished. See for example art. 342 of the Criminal Code of Canada [26], the structural elements of which are devoted to the regulation of criminal liability for committing unlawful acts with electronic means of payment.

In our opinion, the above approach to the normative regulation of criminal liability involves the allocation of electronic means of payment as a special object of criminal law protection, which is most relevant at present and correspondence to the demands of a systematic and balanced criminal law.

An analysis of foreign criminal law made it possible to classify countries according to the availability of specialized act criminalizing fraud using electronic means of payment. Thus, the group of countries that distinguish a special composition of fraud using electronic means of payment include, for example, the Republic of Austria, the Republic of Finland, the French Republic, the Federal Republic of Germany, the Republic of Latvia, the Kingdom of the Netherlands, the Kingdom of Norway, the Portuguese Republic, the Swiss Confederation, the United States America, Canada, People's Republic of China, State of Japan, Republic of Singapore, Republic of Estonia, Republic of Northern Macedonia, etc.

The group of countries whose criminal legislation does not contain a special article criminalizing fraud using electronic means of payment includes, among others: the Republic of Albania, the Republic of Armenia, the Republic of Azerbaijan, the Republic of Bulgaria, the Republic of Georgia, the Republic of Kazakhstan, the Principality of Liechtenstein, Ukraine etc.

7. CONCLUSIONS

We have approved at the following conclusions. It is necessary to put in practice a systematic approach in the implementation of banking response measures, technological improvement of the settlement procedure, optimization of the regulatory framework, and work with the public. In the criminal legislation of a significant number of foreign countries, the consolidation of an article criminalizing the theft of payment cards is widespread due to the fact that payment cards are subject to special criminal legal protection. The justification for the use of this article is that stolen payment cards open to attackers access to the cardholder's personal information, money on his account, besides stolen cards can be further used in illegal activities.

It is noteworthy that the criminal law of foreign countries has widespread application of an article that criminalizes the unlawful acquisition, storage, transportation, transfer for sale of special technical equipment and computer programs designed to obtain unauthorized access and counterfeiting payment cards, which can also be used in the criminal legislation of the Russian Federation in order to protect personal data of customers of credit organizations, as well as the procedure for the implementation of cashless cash payments.

In this regard, we consider it necessary to supplement Chapter 19 of the Criminal Code of the Russian Federation with Article 138.2 «Illegal Traffic of Special Technical Means and Computer Programs Designed for Counterfeiting Payment Cards» with the following content:

«1. Illegal manufacture, acquisition, storage, transportation, transfer for marketing purposes, as well as the sale of special hardware and computer programs designed to obtain unauthorized access, modification, or falsification of payment cards,-

shall be punishable by a fine in the amount of up to three hundred thousand rubles or in the amount of the convict's salary or other income for a period of up to eighteen months, or by restriction of liberty for a term of up to four years, or forced labor for a term of up to four years with deprivation of the right to occupy certain positions or engage in certain activities for a term of up to three years or without it, or deprivation of liberty for a term of up to four years with deprivation of the right to occupy certain positions or engage in certain activities for a term of up to three years or without that.

2. The same acts committed by an organized group -

shall be punishable by forced labor for a term of up to five years or imprisonment for a term of up to seven years with a fine in the amount of up to one million rubles or in the amount of the wage or other income of the convicted person for a period of up to five years or not».

The results of the study allow us to conclude that it is necessary to provide timely and complete information support for the activities of the authorized law enforcement agencies in the field of fraud prevention using electronic means of payment. The Central Bank of Russia has formed a database of the recipients of funds without

the consent of the clients. However, this information is not transmitted to the internal affairs bodies until a corresponding request is sent, which negatively affects the efficiency of law enforcement.

In our opinion, there is a practical need to establish the obligation of credit organizations to report information on identified violations of a money transfer without the consent of a client of a credit organization to the internal affairs bodies, as well as other characterizing information.

We consider it necessary to optimize the work of informing the population in order to prevent victim behavior, which involves the use of a wide range of media, mainly social networks and television.

Of great importance are measures to improve the banking sector software package, information support, quality training for credit institution employees, and other measures. In our opinion, the proposed criminal legal and organizational measures will contribute to the improvement of the criminal legislation of the Russian Federation and will have a positive effect on the prevention of fraud using electronic means of payment.

REFERENCES

[1] World Payments Report (March 17, 2020), available at https://worldpaymentsreport.com

[2] Retailers expect to reduce costs through the introduction of cashless payments (March 17, 2020), available at http://www.finmarket.ru/news/5067788

[3] V.D. Malkov, Criminology: Textbook for universities. Moscow, 2006, 528 p.

[4] G. G. Shikhantsov, Criminology. Moscow, 2009, 295 p.

[5] L.M. Prozumentov, A.V. Shesler, Criminology. General part: Textbook. Tomsk, 2007, 230 p.

[6] S.V. Sheveleva, A.A. Grebenkov; V. E. Novichkov, Criminology. Kursk, 2011, 298 p.

[7] S.L. Alekseev, R.R. Salimzyanova, Criminology. Kazan, 2013, 212 p.

[8] Ya. I. Gilinsky, Yu. V. Morozova, P. V. Fedyshina, Actual problems of criminology. St. Petersburg, 2016. - 192 p.

[9] L. Fernandes, Fraud in electronic payment transactions: threats and countermeasures (March 17, 2020), available at https://pdfs.semanticscholar.org/acf1/cafd5f8b8fb82ac11bc476673ebc63aa5f9a.pdf

[10] M. G. Rachavelias, Online financial crimes and fraud committed with electronic means of payment—a general approach and case studies in Greece (March 17, 2020), available at https://link.springer.com/article/10.1007/s12027-018-0519-2

[11] M. Mazitova, Consumer liability in case of fraud with electronic payment instruments: an analysis of European and Russian rules (March 17, 2020), available at https://www.duo.uio.no/bitstream/handle/10852/49691/ICTLTHESIS-8028.pdf?sequence=1

[12] Akshada K. Dhakade, K.K.Chhajed, A.S.Kapse, Review on Fraud Detection in Electronic Payment Gateway (March 17, 2020), available at https://www.irjet.net/archives/V4/i1/IRJET-V4I1147.pdf

[13] C. Tancock Fraudulent emails requesting payment: a warning for authors (March 17, 2020), available at https://www.elsevier.com/connect/authors-update/fraudulent-emails-requesting-payment-a-warning-for-authors

[14] Swedish money: Farewell to paper (March 17, 2020), available at https://ru.sweden.se/ljudi/dengi-eto-bumaga-tolko-ne-v-shvecii/

[15] The evolution of payments: what makes people refuse cash (March 17, 2020), available at https://plus.rbc.ru/specials/page1905509.html

[16] FICO Fraud Map (March 17, 2020), available at https://www.fico.com/en/newsroom/fico-fraud-map-shows-uk-card-fraud-losses-hit-record-671-million-2018

[17] The Criminal Code Of The Russian Federation No. 63-FZ dated June 13 1996 (March 17, 2020), available at http://www.consultant.ru/document/cons_doc_LAW_10699/

[18] Research: losses from card fraud in European countries grew by 30 million Euros over the year (March 17, 2020), available at https://www.banki.ru/news/lenta/?id=10587162

[19] Fraud. The facts 2012 (March 17, 2020), available at http://www.theukcardsassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf

[20] INTERPOL: Global Complex for Innovation opens its doors (March 17, 2020), available at

https://www.interpol.int/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors

[21] Instant Payments Mean Real-Time Payments Fraud (March 17, 2020), available at https://www.fico.com/blogs/instant-payments-mean-real-time-payments-fraud

[22] Falcon Intelligence Network (March 17, 2020), available at https://www.fico.com/en/fico-falcon-intelligence-network (дата обращения: 20.01.2019).

[23] Criminal Code of Canada, 1985 (March 17, 2020), available at https://laws-lois.justice.gc.ca/eng/acts/c-46/?wbdisable=true