Banking Cybercrime as One of the Main Problems of Modern Society[1]

Karina A. Kovtun
Student of the Faculty of Law of St. Petersburg Polytechnic Peter the Great University, Saint Petersburg, Russian Federation; wermoment@mail.ru

ABSTRACT
This article examines the specifics of banking cybercrimes, their victims, as well as criminals who commit these crimes. The research method is based on statistical data from the Bank of Russia. The author concludes that improving the economic and legal literacy of the population is the most effective way to reduce the trend of banking cybercrime.
Keywords: human factor, economic illiteracy, psychological influence, theft, prevention methods, fraud prevention, implementation methods

Cybercrime is one of the main forms of crime, which gains momentum. The predominant increase of cybercrime in the twenty-first century is observed together with the widespread introduction of computer technologies into society. This type of crime differs from the other in that the attacker's goal is not some small amounts of money, which constitute «theft» in most crimes, but the theft of funds, which turnover usually begins with several hundreds of thousands and can reach billions of rubles, i.e. cybercrime. Such amounts are primarily due to the fact that the person committing the crime usually carefully chooses the victim, based on his or her earnings.[2] Hardly anyone is immune to the theft of funds from accounts. There are cases in the criminal history, when the well-known banks employees transmitted information about card holder, including his passport data and other information necessary for transferring money to the fraudster's account. Fraudsters who specialize in the theft of money from victims' cards use a certain fraud scheme. Bank employee that is involved in this scheme is looking for a customer who has not used their bank card for a long time but has a certain amount of money in his bank account. This employee receives an agreed amount for transferring passport data and bank card information to the fraudster. !!!A fraudster commits fraud with passport data and a card, as well as certifies a power of attorney by an involved in the scheme notary, gets the opportunity to withdraw funds from the victim's card by a third party. Then money are stolen from the account. It is almost impossible to prove, and even more so to return money stolen under this scheme.

Banking cybercrime is a rapidly developing industry. To have something to do with this bank is not even necessary in order to steal from the victim's account[3]. A fraudulent scheme that resulted in the theft of more than 5 billion rubles from the Russians bank accounts in 2020 is especially developed at the moment according to the Center for Monitoring and Responding to Computer Attacks in the credit and financial sphere. Financial and legal illiteracy of the population is the main reason for such overwhelming figures. These two facts are confirmed by the clarification of this fraudulent scheme: subscriber gets a call from allegedly well-known bank's employee that simply asks the question: «Have you made transfers in the amount of several thousand rubles in the past hour?» The victim replies that no transactions were committed. Further, the alleged bank employee exerts moral pressure on the subscriber by hurrying and assuring the client that he has to tell the card number and the secret number on its back otherwise the remaining amount in the subscriber's account will be withdrawn directly by the fraudsters. The victim, being under a strong influence, tells everything that is required. The outcome of this fraud is obvious known[4].

What is the reason for the five-billion-dollar amount of money stolen by fraudsters? First, as we said before, this is financial illiteracy. For example, Sberbank users know that an official bank representative does not call subscribers from a regular number, since this bank uses an official phone number to prevent cybercrimes[5].Secondly, people who are more susceptible to psychological influence than others are more likely to fall for the fraudster's tricks. In turn the latter think out the

---

1 Academic adviser: Nikolay Aleksevich Lipsky, Associate Professor of the Department of Criminal Law Disciplines, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russian Federation.
2 See: T. Krivenko. Investigation of crimes in the credit and finance sphere /Vol. Kryvenko, E. Kuranova //Legality. 1996. № 1. Pp. 19-25.
3 Economic crime in the finance and credit system of Russia [Online source]. URL: https://pravo.studio/dengi/prestupnost-finansovo-kreditnoy-sisteme-rossii.html (date of access: 05.03.2021).
4 See: Abalkin L. Qualitative changes in the structure of the financial market and capital flight from Russia [Online source]. URL: https://cyberleninka.ru/article/n/kachestvennye-izmeneniya-struktury-finansovogo-rynkai-begstvo-kapitala-iz-rossii/viewer (date of access: 05.03.2021).
5 Satuev R. S., Shraer D. Ya., Yaskova N. Yu. Economic crime in the financial and credit system. Moscow: Center for Economics and Marketing, 2000.

course of events, paying special attention to details (even background noise during the conversation between scammers and the victim completely copies the work of the bank – you can hear the voices of call center employees).

A question of concern to all those affected by this financial fraud: who are the once cyber-criminals who can so skillfully withdraw billions of rubles from the victims' accounts? The answer to this question is very non-trivial. Prisoners are the ones who make the phone calls most frequently. This information is presented in the article of the Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere (FinCERT) of the Bank of Russia[6]. Phones, routers, chargers, headphones, as well as notebooks with the names of the victims were found during a search of cells in one of the Moscow prisons. Based on the above information, it should be concluded that the prison authorities at least relate indirectly to the fraudulent calls. The Prosecutor's Office of the Russian Federation proposed to allocate money in the amount of 10 million rubles for the installation of devices capable to jam the telephone signals in prison territories. Of course, this is one of the most effective ways to solve the problem in this case.

The most difficult and almost impossible aspect of this situation is the compensation to the bank's customers. Legally, the subscribers voluntarily transferred personal information of their cards to cybercriminals, that is why to recover money is even more difficult. Banks reimbursed customers only 15%, or 932 million rubles of stolen funds' total amount. The scale of the problem is colossal, there are practically no ways to solve it – all this is disappointing statistics from economic experts[7].

In conclusion, it should be noted that citizens who have been influenced by cybercriminals specializing in banking operations are partly to blame. Carelessness and illiteracy contribute to an increase in the total number of stolen money in our country[8]. To reduce the number of crimes in this area, it is necessary to improve the financial literacy of the population, as well as to inform the older generation which is more than others susceptible to psychological influence from cybercriminals[9] about the presence of this problem. Our country will be able to cope with such a global problem as cybercrime in the banking sector only with the joint assistance of experts and the population.

Based on Chapter 28 of the CC RF «Crimes in the field of computer information», which does not have rules for regulating cybercrime in the banking sector, we can say that The Criminal Code of the Russian Federation does not contain rules of law aimed at preventing fraud with bank accounts. Crimes committed in this area are most often referred to Article 159.6 «Fraud in the field of computer information», the maximum penalty in which is one and a half years of imprisonment. At the moment, there is no article in the CC RF that would be aimed at resolving specific offenses in the field of embezzlement of funds from bank cards by submitting information by a bank employee and disposing of false information. The only way to reduce the trend of crime in this area is to introduce legal norms that cover this problem.

Based on the articles «Illegal access to computer information» (Article 272), «Creation, use and distribution of malicious computer programs» (Article 273), «Violation of the rules for the operation of means of storing, processing or transmitting computer information and information and telecommunications networks» (Article 274), considered during the analysis of existing legal acts regulating banking cybercrime, it was found that the Criminal Code of the Russian Federation does not contain articles that fully implement legal regulation of relations in the field of banking cyber attacks. The only sure way to solve the problem of widespread and rapid spread of banking cyber crime in the Russian Federation is the adoption of a new article of the Criminal Code, which will contain a hypothesis and a disposition covering this topic, as well as the corresponding punishment provided for in the article. The introduction of new legal norms that contribute to the regulation of legal relations in this area is the only and necessary measure that can lead to the elimination of banking cybercrime.

References

1. Abalkin, L. Qualitative Changes in the Structure of the Financial Market and Capital Flight from russia [Kachestvennye izmeneniya struktury finansovogo rynka i begstva kapitala iz Rossii] [Online source]. URL: https://cyberleninka. ru/article/n/kachestvennye-izmeneniya-struktury-finansovogo-rynka-i-begstvo-kapitala-iz -rossii / viewer (date of access: 05.03.2021). (in Russian)
2. Bykov, S. A. Analysis of the Specifics of Economic Crime in Russia [Analiz osobennostei ehkonomicheskoi prestupnosti v Rossii] [Online source]. URL: https://www.elibrary.ru/item.asp?id= 12849326 (date of access: 05.03.2021). (in Russian)
3. Viktorov, I., Mironov, V. Legality in the Credit and Banking Sector [Zakonnost' v kreditno-bankovskoi sfere] [Online source]. URL: https://wiselawyer.ru/poleznoe/13872-zakonnost-kreditno-bankovskoj-sfere (date of access: 05.03.2021). (in Russian)
4. Krivenko, T. Investigation of Crimes in the Credit and Financial Sphere [Rassledovanie prestuplenii v kreditno-finansovoi sfere] / T. Krivenko, E. Kuranova // Legality [Zakonnost']. 1996. No. 1. Pp. 19-25. (in Russian)

[6] See: Bykov S. A. Analysis of the characteristics of economic crime in Russia [Online source]. URL: https://www.elibrary.ru/item.asp?id=12849326 (date of access: 03/05/2021).

[7] Olshany A. I. Bank lending: Russian and foreign experience / ed. E. G. Ishchenko, V.I. Alekseeva. M.: Russian business literature, 1997.

[8] See: Viktorov I., Mironov V., Legality in the credit and banking sector [Online source]. URL:https://wiselawyer.ru/poleznoe/13872-zakonnost-kreditno-bankovskoj-sfere (date of access: 05.03.2021).

[9] See: Krivenko I. Criminal economy in modern society [Online source]. URL: https://elar.urfu.ru/bitstream/10995/38772/1/dn_2015_01_29.pdf (date date of access: 03/05/2021).

5. Krivenko, I. Criminal Economy in Modern Society [Kriminal'naya ehkonomika v sovremennom obshchestve] [Online source]. URL: https://elar.urfu.ru/bitstream/10995/38772/Vdn_2015_01_29.pdf (date of access: 05.03.2021). (in Russian)
6. Olshany, A. I. Bank Lending: Russian and Foreign Experience [Bankovskoe kreditovanie: rossiiskii i zarubezhnyi opyt] / ed. E. G. Ishchenko, V. I. Alekseeva. M.: Russian Business Literature [Russkaya delovaya literatura], 1997. (in Russian)
7. Satuev, R. S, Shrayer, D. Ya., Yaskova, N. Yu. Economic Crime in the Financial and Credit System [Ehkonomicheskaya prestupnost' v finansovo-kreditnoi sisteme]. M.: Center for Economics and Marketing [Tsentr ehkonomiki i marketinga], 2000. (in Russian)
8. Economic Crime in the Financial and Credit System of Russia [Ehkonomicheskaya prestupnost' v finansovo-kreditnoi sisteme Rossii] [Online source]. URL: https://pravo.studio/dengi/prestupnost-finansovo-kreditnoy-sisteme-rossii.html (date of access: 05.03.2021). (in Russian)