Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

TYPES AND CRIMINAL LEGAL ASPECTS OF THE THEFT OF PROPERTY USING BANK PLASTIC CARDS

Kholikov Farhod Uktamovich
Lecturer at the Department of Criminal Law,
Criminology and Combating Corruption"
Tashkent State University of Law
fxolikov@internet.ru

Abstract
This article discusses the practice of stealing bank plastic cards and the problems of their qualification, as well as measures to prevent this type of crime. Also, proposals for improving the national legislation of the Republic of Uzbekistan were developed.

Keywords: Bank plastic cards, Skimming, Phishing, Vishing, IM-frod

Introduction

In the modern world, computer technologies are becoming increasingly important in the daily life of any person. Computer technologies are present in many areas, and the banking sector is no exception. The non-cash form of settlements prevails over the cash form. The popularity of cashless payment forms, as well as plastic cards, is growing with geometric progression, and in connection with this, the number of fraudulent operations using plastic cards is growing. Because not only the positive aspects of society and state life, but also the world of crime, are subject to development. Fraudsters are acquiring more and more knowledge and skills in the banking sector, inventing new ways to steal funds from bank clients' personal accounts.

The payment card market in the Republic of Uzbekistan is actively developing. However, based on the share of credit institutions carrying out emission or acquiring in the total number of credit institutions, it can be concluded that with

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

each passing year, more and more credit institutions begin to implement emission and acquiring services. Thus, a bank card is a payment instrument that allows the holder to receive cash, make payments for the purchase of various types of goods and services, manage funds in a bank account, and use various types of additional services. Due to their advantages, they are becoming increasingly popular among the population, moreover, the share of card issuing credit institutions among the total number of credit institutions is growing, card issuance is increasing throughout the country, and the number and volume of operations performed using cards are growing.

However, there are a number of problems that negatively affect the development of "card business." One of the main and pressing problems is the problem of fraud using bank cards.

The development of payment systems is a characteristic feature of the modern world. However, despite the fact that foreign banks have been using the card system for quite some time, this tool entered our economy relatively recently. Nevertheless, bank cards are not only an integral part of our lives but also a convenient tool in the field of fraud.

This is justified by the fact that in this sphere there is an opportunity to act not only without attracting attention, but often even without leaving one's own home. A fraudster does not have to have certain skills, it is enough to simply find information on the Internet, which contains a huge amount of information, or to purchase the necessary equipment and special programs.

In the world of advanced technologies, it is becoming increasingly difficult for humanity to abandon the emergence of new remote banking services. Numerous companies annually develop and implement new protection systems, and representatives of the criminal world try to find ways to circumvent this protection.

Of course, if you show persistence, you can find a means to fight against any defense system, but usually it requires a lot of money. It is much easier to mislead a person who does not follow the development of modern technologies and does not know all the intricacies of this complex system. To avoid being deceived and losing money, one should regularly improve their knowledge in this area.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

Of course, one of the most important factors in the development of the banking sector of the economy is the range and nature of the use of payment cards. A bank card is a multi-use payment and credit instrument with a long service life, allowing access to a personal account in the bank and having a very high degree of protection against counterfeiting, as well as storing information about the original cardholder. In recent decades, there has been a global trend of developing non-cash forms of settlements, as they have great economic significance. Payments made without the participation of cash contribute to the acceleration of turnover, the reduction of the amount of funds required for circulation, which, as a consequence, leads to a reduction in circulation costs, increased transparency of settlements.

Let's take a closer look at the most popular types of fraud. **Skimming** (from English skimming) - the theft of card data using a special reading device (skimmer). The perpetrators copy all information from the card's magnetic strip (holder's name, card number, expiration date, CVV- and CVC-code), the PIN code can be found using a mini-camera or keyboard pads installed on ATMs. You can become a victim of skimming not only by withdrawing cash, but also by paying for purchases at retail outlets.

Fishing. The scammer's goal is simple - to learn the victim's logins, passwords, card numbers, and CVV2/CVC2 codes. Further, using the received data, fraudsters gain access to bank cards, online bank accounts, and transfer funds to fraudulent accounts or make purchases in online stores. For this, various techniques are used:

The fraudster calls the client and, introducing himself as a bank employee, reports that the client has encountered a problem (options are possible), for the solution of which the client must immediately name a number of card details.

The victim receives an SMS with a message stating that their card is blocked and the phone number of supposedly support services calling the specified number is being "processed" by the fraudsters, using the client's confusion and learning during the conversation the necessary data for the fraud.

The fraudster, knowing the client's login and password, sends a letter to the victim stating that funds were fraudulently debited from his card and that to cancel the transaction, it is necessary to indicate the code received via SMS from

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

the bank. In reality, the SMS code confirms the operation initiated by the fraudster, and using the code named by the victim, the fraudster sends funds from the victim's account to their account or pays for the services of providers.
The fraudster conducts a mass distribution of emails on behalf of banks, postal services, or within social networks. In a letter, there is usually a direct link to the website, which outwardly is indistinguishable from the real one. After a user enters a fake page, they are asked to enter their login and password, which they use to access a specific website, allowing fraudsters to access accounts and bank accounts.

Vishing (from English vishing - voice phishing) is a type of telephone fraud that allows for the theft of confidential information from bank clients. The client receives a call from an auto-informant who reports that, for example, fraudulent actions are being carried out with the card and gives instructions - to call back to a specific number. Next, following the auto-response operator's instructions, the client must inform or enter the card details on the phone keyboard. Sometimes the perpetrators themselves call the victims, convincing them that they are bank employees.

IM-frod (SMS-frod) is a relatively new type of fraud based on the ability to access the SIM card or SMS messages of the bank cardholder. Fraud scheme: 1. The bank cardholder (hereinafter referred to as the victim) attaches a mobile phone number to the bank card (or internet banking) to receive SMS messages. 2. The victim loses control of their room. 3. The scammer gains access to the victim's number. 4. The fraudster receives an SMS notification to the received number and understands that he can use it for selfish purposes. 5. The fraudster sends an SMS message to the victim's bank with instructions to make a payment to their account (or to the account of third parties). Throughout the world, the problem of fraud using payment cards receives significant attention from both banking structures and law enforcement agencies at various levels.

To combat fraud, it is necessary to take various measures by the payment system, banks, and law enforcement agencies, but in most cases, it is necessary to improve the plastic cards themselves, increase the degree of their protection, since in most cases, the largest number of fraudulent transactions occur due to the unreliability of user identification methods.

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

Articles 169 and 168 of the Criminal Code of the Republic of Uzbekistan provide for liability for theft and embezzlement of funds from bank plastic cards. If in these cases the offender used computer equipment, he is qualified under Article 168, Part 2, Subparagraph "c" or Article 169, Part 3, Subparagraph "b" of the Criminal Code. Article 168, Part 1, or Article 169, Part 1, is qualified if it is committed without the use of computer technology, using only mobile devices and payment systems. But now, when this type of crime is increasing, it is necessary to strengthen the responsibility.

In other words, the "v" paragraph of part 2 of Article 168 of the Criminal Code should be supplemented with the words "if computer equipment is used using information technologies or electronic payment instruments or a remote service system."

It is also necessary to supplement paragraph 169 of part 3 of point "b" of the Criminal Code of the Republic of Uzbekistan, where "unauthorized access to a computer system" is defined as "unauthorized access to computer equipment, as well as to another information system, or using an electronic payment instrument or remote service system."

Article 169 and Article 168 of the Criminal Code of the Republic of Uzbekistan provide for liability for cases of embezzlement and secret misappropriation of funds from bank plastic cards. If in these cases the perpetrator used computer equipment, they are qualified under Article 168, Part 2, Clause "c" or Article 169, Part 3, Clause "b" of the Criminal Code of the Republic of Uzbekistan. If it was committed without the use of computer equipment, and only with the use of mobile communication devices and payment systems, then it is qualified under Article 168, Part 1 or Article 169, Part 1. However, considering the increasing number of crimes of this type, it is necessary to strengthen the responsibility for them.

Article 169 and Article 168 of the Criminal Code of the Republic of Uzbekistan provide for liability for cases of embezzlement and secret misappropriation of funds from bank plastic cards. If, in these cases, the perpetrator used computer equipment, they are qualified under Article 168, Part 2, Clause "c" or Article 169, Part 3, Clause "b" of the Criminal Code. If it was committed without the use of computer equipment, and only with the use of mobile communication

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

devices and payment systems, then it is qualified under Article 168, Part 1 or Article 169, Part 1. However, considering the increase in the number of crimes of this type, it is necessary to strengthen the responsibility for them. That is, the paragraph "if it was committed using computing equipment" specified in Article 168, part 2, clause "v" of the Criminal Code should be supplemented with the words "if it was committed using computer equipment, as well as information technologies, or an electronic payment instrument or a remote service system."

It is also necessary to fill in the clause "entry into a computer system without permission," specified in paragraph "b" of part 3 of Article 169 of the Criminal Code, as "entry into computer equipment and other information systems without permission or using an electronic payment instrument or a remote service system."

References

1. Mirziyoyev Sh.M. Address of the President of the Republic of Uzbekistan Shavkat Mirziyoyev to the Oliy Majlis // Address of the President of the Republic of Uzbekistan Shavkat Mirziyoyev to the Oliy Majlis of December 22, 2017.
2. Decree of the President of the Republic of Uzbekistan dated February 7, 2017 No. UP-4947 "On the Action Strategy for the Further Development of the Republic of Uzbekistan." Collection of Legislation of the Republic of Uzbekistan, 2017, No. 6, Art. 70.
3. Rustambayev M.H. Criminal Law. General Part: Textbook. - Tashkent: TDYUI, 2006. - P. 166.
4. Rustambayev M.H. Course of Criminal Law of the Republic of Uzbekistan. Vol.1. General Part. Crime Teaching: Textbook. - Tashkent: ILM ZIYO, 2010. - P. 164.
5. Zufarov R.A. Criminal Liability for Bribery. - Tashkent: TDYI, 2004. - P. 66.
6. Criminalistics course. Special Part. Vol. 1. Methodology for investigating violent and mercenary-violent crimes. / Edited by V.E. Kornoukhov. - M.,

Modern American Journal of Business, Economics, and Entrepreneurship
ISSN (E): 3067-7203
Volume 2, Issue 2, February, 2026
Website: usajournals.org

2001. - P. 70.; Raroğ A.I. Subjective side and qualification of crimes. - M., 2001. - P. 6.

7. Criminal Law. General Part: Textbook. / A.S. Yakubov, R. Kabulov, et al. - Tashkent: Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, 2009. - P. 160.
8. Criminal Law. General Part. Textbook for universities / Edited by I.Ya.Kozachenko, Z.A.Neznamov. - M., 1997. - P. 181.
9. Luneev V.V. Subjective assignment. - M.: Spark, 2000. - P. 6-7.
10. Criminal Law of Russia. General and Special Parts: Textbook. / M.P.Zhuravlev, A.V.Naumov, et al. - M.: Prospekt, 2004. - P. 87.
11. Criminal Law. Special Part: Textbook. Second revised and expanded edition / Sh.T. Ikramov, R. Kabulov, A. Otajonov et al.; Editor-in-Chief Sh.T. Ikramov. - Tashkent: Academy of the Ministry of Internal Affairs, 2016. - P.470.
12. Uktamovich K. F. TYPES AND CRIMINAL LEGAL ASPECTS OF THEFT OF PROPERTY USING BANK PLASTIC CARDS //European International Journal of Multidisciplinary Research and Management Studies. - 2022. - Vol. 2. - No. 08. - P. 7-10.
13. Kholikov F. U. ISSUES OF CRIMINAL LIABILITY FOR VIOLATION OF CUSTOMS LEGISLATION IN CERTAIN FOREIGN STATES //International journal of conference series on education and social sciences (Online). - 2022. - Vol. 2. - No. 6.