European Journal of Economics, Finance and Business Development
ISSN (E): 2938-3633
Volume 2, Issue 10, October - 2024

CURRENT ISSUES OF ENSURING FINANCIAL SECURITY IN MODERN CONDITIONS

Рузиева Диёра Сулаймановна
Доктор философии по экономическим наукам (PhD)
Преподаватель Академии Министерства внутренних дел Республики Узбекистан

Abstract
This article discusses the topical problems of improving the database for obtaining electronic evidence in the internal affairs bodies in order to solve crimes of financial fraud in the field of modern payment systems.
This article discusses current problems of improving the basis for obtaining electronic evidence in internal affairs bodies in order to solve crimes of financial fraud in the field of modern payment systems.

Keywords: economic crime, financial fraud, payment systems, payment organizations, digital expertise.

Introduction

The emergence of financial infrastructure (banks, insurance companies, stock exchanges, electronic payment systems, etc.) in the world, as well as the rapid development of digital technologies, have led to an unprecedented increase in the types of financial and economic transactions of enterprises and the volume of their income. financial statement falsification, debit and credit card fraud have been recognized as the typical and most frequently committed financial crimes of 2023, according to analytical data from Comply Advantage, a leading source of financial crime risk data in the financial industry and AI-powered detection technologies. The saddest thing is that such crimes are committed not by ordinary professional criminals, but also by economic entities that previously acted legally1.

That is why, despite the fact that today several institutions of internal and external control have been created, inherent in the principles of a market economy, the issue of economic security and financial security, which is its constituent element, has become the most urgent problem of our time. This has led to the need to strengthen law enforcement measures to combat crime in this regard.

A long time has passed since the gong of financial crimes known to us so far, such as theft of material and financial assets, forgery of documents or reports, financial crimes, etc., began to be struck. As a result, we have gained experience in applying special economic knowledge in detecting crimes in the banking sector, detection of financial fraud in documents and methods of their commission, verification of documents used in the commission of economic crimes, and the appointment of a certain type of forensic economic examination on their basis,

[1] Four trends shaping the state of financial crime in 2023/ https://complyadvantage.com/insights/four-trends-shaping-the-state-of-financial-crime-in-2023/

identification and disclosure of types of crimes typical for the banking system using traditional methods. Especially from a theoretical point of view, our ability to use forensic expert opinions (!) and the analysis of judicial and investigative practice in determining the signs and methods of their commission characteristic of these offenses are very high.

However, financial fraud committed today in electronic systems, crimes related to illegal transactions, and the fact that banks remain intermediaries or direct participants in these illegal actions, have also begun to strengthen the need to further improve the mechanism for effectively combating this type of offense, creating and strengthening the evidence base for these types of economic crimes.

Definitions of electronic evidence are given in the scientific developments of Russian scientists. In particular, V. A. Laptev, A. V. Grebelsky, P. V. Samolysov, E. A. Nakhovas determine: "Electronic evidence is information about facts in electronic form, determining the presence or absence of circumstances substantiating the claims and objections of persons participating in the court case, as well as the presence or absence of other circumstances that are important for the proper consideration of the case2."

Many researchers of our republic have considered the concepts of electronic or digital evidence from a scientific and theoretical point of view. In particular, according to researcher B. Karimov, digital evidence is important, valuable information that is stored on a digital device and network or transmitted through them as a result of the human factor or cyberprocess3.

According to I. Astanov and B. Gamidov: "Logically, the concept of "evidence" confirms the fact that a certain action or inaction that is important for the case took place in the previous reality. For example, when fingerprints are found at a crime scene, the investigator finds, records and records the fingerprints left by the previous criminal, but does not create or create prints himself. This also applies when working with digital evidence. The investigator searches, collects, and documents evidence left by the previous offender. Consequently, the processes associated with the "creation" and "processing" of digital information do not participate in the formation of the concept of digital evidence. Accordingly, digital evidence is information stored or transmitted digitally on a digital device or network that has value for business purposes. This definition covers issues related to the content, form, characteristics and admissibility of digital evidence4.

Today, in addition to instant settlements in international and national payment systems, convenient online lending through them, benefits created for use in the delivery of goods have also contributed to a sharp increase in the number of frauds.

---

[2] Laptev V. A. Electronic Evidence in the Arbitration Process // Russian Justice. 2017. № 2. Pp. 56-59. Grebelsky A. V. Electronic Evidence in International Commercial Arbitration. 2015. № 10. Pp. 59 — 70. 2022. Samolysov P. V. Electronic Evidence in Cases of Violation of Antimonopoly Legislation // Law and Economics. 2016. № 5. Pp. 58-65. 2022. Nakhova E. A. Problems of Electronic Evidence in the Civil Process // Leningrad Law Journal. 2015. № 4. Pp. 301—312. Oct. 2022

[3] Karimov Beaubourgeon (2020). Scientific and theoretical issues of the category of digital evidence. Review of law sciences, 5 (Special Issue), 149-153. doi: 10.24412/2181-919X-2020-149-153.

[4] И.Астанов, Б.Ҳамидов Жиноят процесси. Криминалистика, тезкор-қидирув ҳуқуқи ва суд экспертизаси. Электрон ёҳуд рақамли далилларга оид умумназарий масалалар: муаммо ва ечим. Жамият ва инновацияла–Общество и инновации – Society and innovations Special Issue – 7 (2021) / ISSN 2181-1415

As a result, today, in the process of online lending, fraudsters have the opportunity to freely issue loans in the names of citizens in various ways without their knowledge. For example, in the examination appointed by the internal affairs units in a similar case, the main attention was paid to the identification of a citizen in the process of online lending of his low-quality photo, uploaded to the application and not meeting the technical requirements, with a photo of this citizen in the passport. As a result of the examination, 85% similarity was revealed, and the penalty was directed at the citizen who became a victim of fraud. Such an incorrect approach provoked a suicidal situation in a citizen who became a victim of fraud. Therefore, in these cases, it was advisable to appoint a forensic medical examination not to identify the citizen in the photo, but to the application of the online lending payment system and its technical criteria, as well as to consider the issue of the responsibility of the bank or payment organization for a loan issued for a low-quality photo.

Drawing our attention to another financial fraud related to bank cards, in 2022 the damage from this type of fraud worldwide reached $33.45 billion, and by 2024, according to forecasts, it will reach $38.79 billion. Citizens of the Russian Federation suffered losses of 15.8 billion rubles from such thefts5, and more than 4 thousand Kazakhstanis 6suffered in the Central Asian region, in Uzbekistan, only Tashkent residents suffered losses of at least 45.2 billion soums. Of this money, only about 9.2 billion soums were recovered by employees of the internal affairs bodies7.

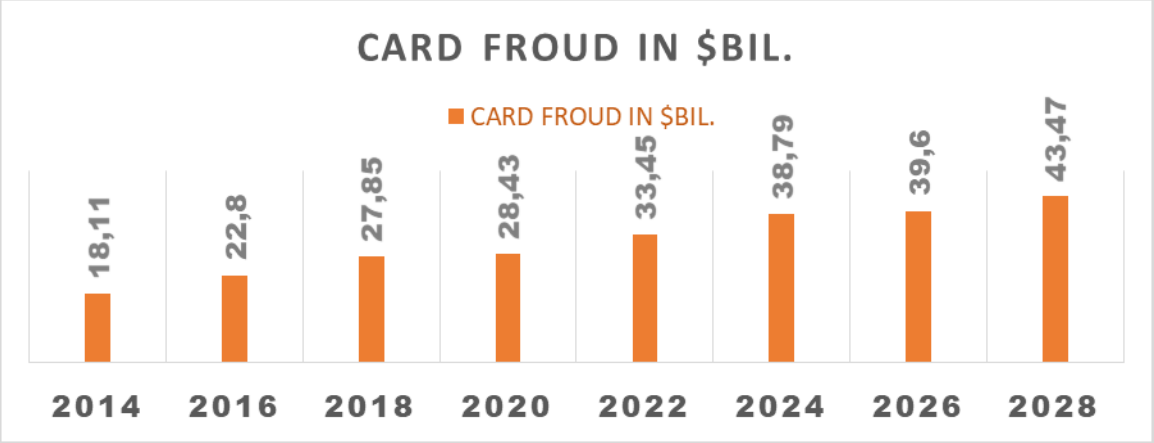

Figure 1. Global dynamics of bank card fraud8.

From the latest information, it is known that these funds were "recovered" from the criminals, but "frozen and not returned from the current account to the current account." It is this information in itself that indicates that the creation of a modern base for solving and proving

[5] Sheikin A.G. Top 3 popular fraudulent schemes in 2024 //http://council.gov.ru/services/discussions/blogs/155339/ April 11, 2024.

[6] Factcheck.kz.https://factcheck.kz/analitika/my-ne-pokupaem-tovar-na-svoi-dengi-kak-moshenniki-ispolzuyut-chuzhie-bankovskie-karty

[7] In 2022, residents of Tashkent suffered damage from cybercrimes in the amount of 45.2 billion soums. https://www-gazeta-uz.translate.goog/uz/2023/02/21/cyber/

[8] Factcheck.kz.https://factcheck.kz/analitika/my-ne-pokupaem-tovar-na-svoi-dengi-kak-moshenniki-ispolzuyut-chuzhie-bankovskie-karty;

crimes of financial fraud, tracking the movement of financial transactions on accounts among traditional types of forensic economic expertise, the use of the capabilities of digital expertise of illegal transactions still remains a weak point.

Specialists of the Main Forensic Center of the Ministry of Internal Affairs of the Republic of Uzbekistan attribute this circumstance to the complexity of the process of solving crimes committed with the help of digital devices. Experts believe that such complexity is due, firstly, to the fact that the device on which the crime was committed is not presented to the examination as the object of the crime, and secondly,, with the inability to identify the device due to the fact that the crime was committed remotely (from other countries). They also emphasize that legal requirements regarding "bank secrecy" impede the conduct of this type of examination, the tracking of the movement of suspicious transactions and the receipt of electronic evidence on them. Therefore, the practice of expert examination of suspicious transactions or any illegal financial transactions made through bank accounts, unfortunately, is practically not developed, and the number of such examinations also does not correspond to crime statistics in this area, that is, we want to say that the indicators of crimes related to illegal transactions are very high, not a single digital examination has been carried out on them or is a very low indicator.

But at present, law enforcement agencies of many countries have established good relations in the world, exchange of information with banks, financial control institutions in general, when freezing an illegal transaction on the spot and returning the money stolen from bank cards to the owner. In addition, law enforcement agencies use the platforms of international payment systems, such as IBAN, SWIFT/BIC, as a very convenient tool for the recipient bank to independently determine the transaction of the country in which it is located. At the request of the victim, the police officer enters his card number into the system and determines the address of the transaction, that is, the number of the card to which he received the transfer, and his bank, the country in which the bank is located, immediately issues a request to the bank not to determine the address of the transaction, but to freeze the illegal transaction. Detection of such transactions in a short time is of fundamental importance, since the longer the interrogation is delayed, the less likely it is to find a trace of a crime.

However, this system cannot always be evaluated as ideal, especially if the thefts are committed by professionals. In addition, IBAN is used only in 70 countries, including the countries of the European Union and some other regions, including the Middle East and the Caribbean, while in the practice of banking systems of other countries, this system practically does not work.

This indicates the need for us to develop alternative options for obtaining electronic data on the movement of illegal transactions, conducting digital examinations and strengthening the evidence base from electronic data by strengthening the activities of law enforcement agencies to use them. This need is also particularly important to address the challenges posed by large illegal transactions and their digital forensics, in which banks themselves remain directly involved.

However, in this regard, there are currently national FATF systems working against the laundering of proceeds from illegal activities in countries. Perhaps we will also not deny the idea that the existence of such national systems will not leave the need for the appointment of a digital examination of illegal transactions countering financial fraud. For example, the use of the "freezing practice" by the Chairman of the Central Bank of the Russian Federation in the

fight against cyber fraud related to loans is similar to the creation of a laboratory by the Central Bank of Uzbekistan since 2019 to combat cybercrime, and in this direction, the regulator can especially note cooperation with FinCERT, a structure of the Information Security Department of the Central Bank of Russia9.

However, a source published on the Fisgroup website on the topic "Investigation and fight against fraud in banks" says: "... One of the main methods of fraud detection is to monitor financial transactions for suspicious activity. Banks should create a transaction monitoring system to identify anomalous or unusual transactions that may signal criminal activity..." Opinions expressed in the content", 10this indicates that the monitoring of illegal transactions in banks themselves has not yet been developed at the level of modern needs. In addition, statistics related to illegal transactions indicate the need to obtain electronic evidence for such crimes and strengthen a transparent system for solving crimes.

As can be seen, new forms of crime generate the need to develop a new methodology for combating them, improving the knowledge of law enforcement officers about it. To achieve this goal, the following are proposed:

Strengthening the interaction of cybersecurity units of internal affairs bodies with the control departments of the Ministry of Finance, the Central Bank and payment organizations. To do this, it is necessary to create a single platform between them to monitor illegal transactions, to ensure visibility in the database of cybersecurity units of law enforcement agencies of each suspicious case that arises in the process of controlling financial transactions in this system. Thanks to this, it is necessary to quickly work with danger signals that signal suspicious transactions in advance, to establish a prompt exchange of information and to appoint a digital examination based on the information received;

Simplification and acceleration of the system of obtaining information from banks and payment organizations or credit organizations by special departments of internal affairs;

The need to consider the issue of appointing an expert examination to identify such cases as non-compliant technical shortcomings of applications in cases of fraud with bank cards and online loans, a low degree of their high vulnerability, to establish liability in relation to payment institutions and credit institutions on the basis of the identified shortcomings.

From the above, it can be concluded that now that financial transactions are related to digital devices, the basis for solving such crimes should also be digital devices and their expertise. The creation of an evidence base for such crimes, the improvement of not only the possibilities of obtaining electronic evidence on them, but also the goals of obtaining evidence should be attributed to the most important tasks of modern forensic examination.

References

1. Laptev V. A. Electronic Evidence in the Arbitration Process // Russian Justice. 2017. № 2. Pp. 56-59.
2. Grebelsky A. V. Electronic Evidence in International Commercial Arbitration. 2015. № 10. Pp. 59 — 70. Oct. 2022

[9] A laboratory to combat cybercrime has been created at the Central Bank. https://www.gazeta.uz/ru/2019/05/04/cybercrime/
[10] Verification and counteraction to fraud in the bank // July https://fisgroup.ru/blog/antifraud-v-banke/4, 2023

3. Samolysov P. V. Electronic Evidence in Cases of Violation of Antimonopoly Legislation // Law and Economics. 2016. № 5. Pp. 58-65. Oct. 2022
4. Nakhova E. A. Problems of Electronic Evidence in the Civil Process. 2015. № 4. Pp. 301—312. Oct. 2022
5. Karimov Beaubourgeon (2020). Scientific and theoretical issues of the category of digital evidence. Review of law sciences, 5 (Special Issue), 149-153. doi: 10.24412/2181-919X-2020-149-153.
6. 1 И.Астанов, Б.Ҳамидов Жиноят процесси. Криминалистика, тезкор-қидирув ҳуқуқи ва суд экспертизаси. Электрон ёҳуд рақамли далилларга оид умумназарий масалалар: муаммо ва ечим. Жамият ва инновациялар – Общество и инновации – Society and innovations. Journal home page: Жамият ва инновациялар – Общество и инновации – Society and innovations. Special Issue – 7 (2021) / ISSN 2181-1415 https://complyadvantage.com/insights/four-trends-shaping-the-state-of-financial-crime-in-2023;
7. https://nilsonreport.com/newsletters/1254;
8. Sheikin A.G. Top 3 Popular Fraudulent Schemes in 2024 //;
9. http://council.gov.ru/services/discussions/blogs/155339/
10. Factcheck.kz.https://factcheck.kz/analitika/my-ne-pokupaem-tovar-na-svoi-dengi-kak-moshenniki-ispolzuyut-chuzhie-bankovskie-karty;
11. https://www-gazeta-uz.translate.goog/uz;
12. A laboratory to combat cybercrime has been created at the Central Bank. https://www.gazeta.uz/ru/2019/05/04/cybercrime/
13. Verification and counteraction to fraud in the bank // July https://fisgroup.ru/blog/antifraud-v-banke/4, 2023.