УДК 336.7
JEL E42, O14
https://doi.org/10.31520/ei.2021.23.2(79).172-184

ХАЯЛАДДІН Р.ТАГІЄВ
Кандидат економічних наук, старший науковий співробітник Інституту Наукових Досліджень Економічних Реформ
Міністерства економіки Республіки Азербайджан
AZ 1011, проспект Х. Зардабі, 88а, Баку, Азербайджан
Email: khayaladdin_tagiyev@cbar.az, xstagiyev@gmail.com
ORCID: 0000-0002-3058-7143

ТАМЕРЛАН Г.РУСТАМОВ
Докторант, Інституту Наукових Досліджень Економічних Реформ
Міністерства економіки Республіки Азербайджан
AZ 1011, проспект Х. Зардабі, 88а, Баку, Азербайджан
Заступник директора департаменту платіжних систем ВАТ "Банк Баку",
Керівник експертної групи з питань платіжних систем та цифрового банкінгу Азербайджанська Банківська Асоціація.
AZ 1052, Agha Nemetulla, 219 (63 \ 65) Баку, Азербайджан
Email: thrustamov@bankofbaku.com, tamerlanrustamov@gmail.com
ORCID: 0000-0002-9510-1917

АРАЗ А.ГАСАНЗАДЕ
Департамент платіжних систем та розрахунків
Центральний Банк Азербайджанської Республіки
AZ1014, вул.Р.Бехбудова, 32, Баку, Азербайджан
Email: araz_hasanzade@cbar.az, arazhasanzadeh@gmail.com
ORCID: 0000-0002-4316-6866

АНАЛІЗ ТРАНЗАКЦІЙ ШАХРАЙСТВА З ПЛАТІЖНИМИ КАРТКАМИ ТА ЗАХОДИ ЩОДО ЇХ ЗАПОБІГАННЯ

Актуальність. *У цій статті проаналізовано тенденції шахрайства та історію шахрайства загалом із появою нових прогалин внаслідок стрімкого розвитку інформаційних технологій. Зроблено систематизацію типів та форм шахрайського втручання, їх наслідків та шляхів протидії з урахування інтересів користувачів.*

Мета та завдання. *Причини шахрайства з платіжними картками, основні форми та типи можливих шахрайських операцій та сфери шахрайства з платіжними картками були детально класифіковані та досліджені.*

Результати. *У ході дослідження було виявлено найпоширеніші випадки, включаючи загублення та викрадення платіжних карток, підроблення карток та шахрайські операції без платіжної картки, також були визначені заходи боротьби з ними. Одночасно були проаналізовані шляхи використання різних методів для здійснення шахрайських операцій. В контексті швидкого зростання електронної комерції під час глобальної пандемії було виявлено широкомасштабне шахрайство та заходи, які слід вжити проти нього. Ще однією цікавою частиною дослідження є продовження досліджень мовою чисел на основі статистичних даних, а також зборі та точності статистичної звітності.*

Висновки. *Таким чином, спочатку було розкрито випадки шахрайства з операціями з платіжними картками в Європейському Союзі, а потім розраховано коефіцієнт кореляції між платіжними операціями на ринку платіжних карток в Азербайджанській Республіці та шахрайськими операціями. Також було проведено розслідування щодо запобіжних заходів проти шахрайських операцій, важливих для фінансових установ та користувачів платіжних послуг, а також про те, як послідовно вживати заходів, що пояснюється у статті. Життєвий цикл платіжних карток поділяється на три основні етапи - прийняття клієнтом, ідентифікація та прийняття рішень, у статті зазначено особливості кожного етапу та способи запобігання ризикам на цих етапах. Зрештою, результати дослідження відображені у розділі висновків статті.*

Ключові слова: *карткові платежі, управління шахрайством, операції з шахрайством, пом'якшення шахрайства, коефіцієнт кореляції.*

KHAYALADDIN R.TAGHIYEV
P.h.D on economy, senior researcher in Institute of Scientific Research on Economic Reforms

of Ministry of Economy of the Republic of Azerbaiijan
AZ 1011, H.Zardabi prospect, 88a, Baku Azerbaijan
E-mail: khayaladdin_tagiyev@cbar.az, xstagiyev@gmail.com
ORCID: 0000-0002-3058-7143

TAMERLAN H.RUSTAMOV
Doctoral student, Institute of Scientific Research on Economic Reforms
of Ministry of Economy of the Republic of Azerbaiijan
AZ 1011, H.Zardabi prospect, 88a, Baku Azerbaijan
Deputy director at the Payment Systems Department, Bank of Baku OJSC,
Head of Payment systems and digital banking expert group Azerbaijan Banking Association.
AZ 1052, Agha Nemetulla, 219 (63\65) Baku, Azerbaijan
E-mail: thrustamov@bankofbaku.com, tamerlanrustamov@gmail.com
ORCID: 0000-0002-9510-1917

ARAZ A.HASANZADE
Payment Systems and Settlements Department
The Central Bank of the Republic of Azerbaijan
AZ1014, 32, R.Behbudov str., Baku, Azerbaijan
E-mail: araz_hasanzade@cbar.az, arazhasanzadeh@gmail.com
ORCID: 0000-0002-4316-6866

ANALYSIS OF PAYMENT CARDS FRAUD TRANSACTIONS AND MEASURES TO PREVENT THEM

Topicality. *The trends of fraud and the history of fraud in general with the emergence of new gaps due to the rapid development of information technology is analysed in the article.*

The systematization of types and forms of fraudulent intervention, their consequences and ways of counteraction taking into account the interests of users is made.

Aim and tasks. *The causes of payment card fraud, the main forms and types of possible fraudulent transactions and areas of payment card fraud were further classified and investigated.*

Research results. *The investigation revealed the most common cases, including lost and stolen payment cards, counterfeit cards and fraudulent transactions without a payment card, and identified measures to combat them. At the same time, the ways of using different methods for the implementation of fraudulent transactions were analyzed. In the context of the rapid growth of e-commerce during the global pandemic, widespread fraud and steps to be taken against them have been revealed. Another noteworthy part of the research is the continuation of research in the language of numbers based on statistical data, as well as the collection and accuracy of statistical reporting.*

Conclusion. *Thus, first, the cases of fraud on payment card transactions in the European Union were disclosed, and then the correlation coefficient between payment transactions in the payment card market in the Republic of Azerbaijan and fraudulent transactions was calculated. An investigation was also conducted into the implementation of preventive measures against fraudulent transactions, which are important for financial institutions and payment service users, as well as and the steps to be taken in a consistent manner are explained in the article. The life cycle of payment cards is divided into three main stages, customer acceptance, identification and decision-making, the specific features of each stage and ways to prevent risks in these stages are noted in the article. In the end, the results of the research are reflected in the conclusion section of the article.*

Keywords: *card payments, fraud management, fraud transactions, fraud mitigations, coefficient of correlation.*

Problem statement and its connection with important scientific and practical tasks. In the digital age we live in, as in various sectors of the economy, we can observe the expansion of the usage of innovative technologies, payment solutions based on cryptographic numbers and passwords in mutual settlements among economic entities as well. As the digital transformation deepens, the structure and principle of payment transactions between economic entities are rapidly evolving and changing.

The rapid development in the field of digital payments, the increase in the volume of transactions, the natural squeezing of cash settlements in some countries, which has become the daily norm, attracts the attention of fraudsters who want to make money in a more convenient way. The changing trends observed in innovative solutions, the fact that the population of a certain age group is not fully open to innovations or assimilation of characteristics, the lack of public awareness, and so on, create favourable conditions for fraudsters.

Analysis of recent publications on the problem. The first financial fraud was reported in Greece in 300 BC. Greek merchant Hegestratos got a large insurance policy called bottom try. From a commercial point of view, the merchant had to repay the loan with interest when he reached the seaport. If the merchant refused to repay the loan and the interest accrued on it, the creditor could demand the corn and the ship used to transport it. In this financial transaction, Hegestratos fraudulently intended to sink a hollow ship at sea and misappropriate the funds and corn cargo allocated as a loan [4].

However, the fraudulent operation he wanted to carry out did not take place, and Hegestratos was caught red-handed by the ship's crew when he tried to carry out his plan. Although this is the first recorded fraud in the financial sector, it is not ruled out that other transactions may have taken place before.

At different stages of the historical development of the society, different tools and values were used as a means of payment in settlements. Against the background of improvements in this area, there have been changes in the characteristics of fraud operations. In the process of the historical evolution of digital payments, the introduction of payment cards since the 1950s has created a new sphere of activity for fraudsters. Over the past 70 years, the characteristics and principles of fraudulent transactions in the payment card market have also improved.

The methods of fraudsters are becoming more sophisticated, and their approaches can change quickly to adapt. Banks need to respond quickly to new threats and master them new approaches and technologies to predict and prevent fraud. Fraud prevention issues have been the subject of research by many scientists and specialists in this field [1–3; 5–7]. Consumer protection issues were on the agenda of leading international organizations, banks, consulting agencies [4; 9; 10], which investigated these issues and proposed a mechanism to protect bank users. These works investigated the risks of fraud in the banking sector, trends in typologies of fraud, the challenges faced by banks in minimizing internal and external threats [14; 15; 17]. According to these studies, the losses from fraud increase faster than the cost of risk management. Urgent new trend analyses are proposed.

The paper [18] found that the risk of cyber-fraud is the biggest challenge for financial institutions in the regions they study. In fact, the five biggest risks of fraud in all regions are associated with the digital transformations taking place in the world. To minimize these risks in the future, financial institutions need to comprehensively change their approach to them. By and large, financial institutions need to understand the digital transformation that is rapidly happening around us, assess the new fraud risks posed by these rapid changes, and develop fraud risk management principles that can effectively and efficiently minimize those risks while delivering sustainable results. Because neither existing "safes" nor other cost-effective solutions currently used by financial institutions, given their significant fragmentation and imperfection, can effectively protect against the risks of ever-transforming fraud. Next-generation fraud risk management systems must be able to operate in a constantly digital transformation, identify new, hitherto unknown risks of fraud, take advantage of technology and reduce compliance costs

Allocation of previously unsolved parts of the general problem. A study of banks from all regions has shown that they consider cyber attacks to be the biggest challenge when fraudsters obtain customer data through the use of hacking technology, social engineering tools, the Dark Web and criminal networks after data breaches outside the control of banks. This threat is multifaceted and the question arises whether banks are ready to adequately meet the challenge. According to the results of the study, it is established that the tendency to spread illegal schemes around the world is growing. For example, the United Kingdom has adopted a Code for a Potential Compensation Model in the form of an authorized push to ensure that customers are reimbursed in certain cases and to ensure that regulators and governments develop a reliable solution for victims of illegal schemes. Requires research on the degree of reliability of controls, in addition, the use of open banking provides an additional opportunity to obtain customer data as an additional measure to detect fraud and compensate for the damage caused by fraudulent attacks.

Formulation of research objectives (problem statement). Taking into account the above justifications of the complexity of the problem, our purpose is to analyze the transactions of fraud with payment cards and measures to prevent them. Particular attention is paid to the forms and types of fraudulent transactions, classified areas of fraud with payment instruments and the causes of their occurrence.

An outline of the main results and their justification. A careful analysis of the problems of storage with payment cards proved the need to systematize them to determine the characteristics of each of them:

I. Classification of payment card fraud

There are a number of reasons that make it easy to carry out fraudulent transactions in the field of payment cards, the ultimate goal of which is the misappropriation of other people's funds [1; 6; 11]:

➢ ***Gaps in the application of the technology*** – Gaps related to the technology (s) applied before the issuance of the payment instrument allow subsequent fraudulent transactions. For example, non-compliance with security requirements during the personalization of payment cards allows for the subsequent production of fraudulent payment cards based on real payment card information and their use for fraudulent purposes;

➢ ***The application of the skills of the new generation in different directions*** – a more adequate approach to the application of modern technologies, knowledge and skills of the representatives of the Millennium and Generation create favourable conditions for the emergence of new cases of fraud. The introduction of the concept of cyber security in the economic literature in recent years and the rapid growth of such fraudulent transactions, the seizure of information about the cardholder and his payment card, social network accounts on the basis of social engineering is a clear example of this;

➢ ***Gaps in the information technology infrastructure*** – while the development of information technology infrastructure, it is important to organize a secure exchange of information between the parties, to keep the necessary network protectors active, to ensure resistance to possible external interference. Fraud operations resulting from possible gaps in this area can include the seizure of necessary information as a result of external interference during the exchange of information, unauthorized interference with information resources where payment card information is stored;

➢ ***Sensitivity of the network of payment terminals*** – the network of payment terminals used in the conduct of payment transactions creates a suitable environment for fraudulent transactions. An example of the simplest fraud in this area is the installation of counterfeit ATMs. Counterfeit ATMs operating under standard requirements allow for the subsequent production of counterfeit payment cards based on the information of the payment cards in which the transaction is made;

➢ ***Low level of financial literacy*** – low level of financial literacy of those who use financial services in one form or another, lack of knowledge of the features of the payment instrument or payment terminal infrastructure used creates right conditions for fraudsters. Fraud operations in this area include the deception of the elderly by fraudsters during the distribution of social payments financed from the state budget, the application of the classic "phishing" method, and others.

Fraud transactions in the field of payment cards can be grouped at least in the following forms [1; 7; 12]:

➢ ***on payment card (s)*** – fraudulent operation is carried out in the form of non-delivery of the payment card, theft of the payment card or its data in the simplest way and other forms, focusing on the card holder (s);

➢ ***on the network of payment terminals*** – this type of fraud is carried out through a network of ATMs, POS-terminals and other payment terminals that accept payment cards, as well as mobile phones. This fraudulent operation is carried out through a payment terminal or common infrastructure;

➢ ***on the software or network where the payment card information is stored or transmitted*** – such fraudulent transactions are mainly of a mass nature, the capture of information on the basis of internal or external interference with the software on which the payment card information is stored, captures relevant information between the issuing bank or service centre and other parties during the information exchange and manifests itself in other forms.

Payment card fraud occurs in two different areas - payment card issuance and payment card acquiring services:

Fraud transactions on the issuance of a payment card take the form of theft of a payment card, seizure of information by unauthorized persons during the issuance and the production of counterfeit payment cards.

Fraud transactions on the acquiring of payment cards are carried out through a network of payment terminals, including business entities. Examples of such fraudulent transactions include double payment transactions in business entities, man-in-middle attack during the exchange of information between the payment terminal and the issuing bank or service centre, as well as the use of counterfeit payment terminals.

There are several common types of fraudulent transactions with payment cards [1; 5; 12]:

➢ **Transactions with lost / stolen payment cards**

It is one of the oldest and simplest types of fraud. The cardholder unknowingly loses the payment card or other persons seize the payment card. Fraudsters carry out transactions with a payment card until it is discovered that the payment card is lost or stolen.

To avoid such situations, the cardholder must keep the payment card in a safe place. Also, information on payment transactions should be provided. Thus, SMS notification about the execution of payment transaction allows preventing the next unauthorized payment transactions in a timely manner in case of loss

or theft of the payment card. The simplest form of this type of fraud is the unauthorized seizure of a payment card by a family member, relatives, and in some cases, trustees of the cardholder.

Refund fraud is one of the few fraudulent transactions in this category. In this type of operation, the fraudster obtains the product over the internet with a payment card and then tries physically return the product to the business entity. Fraudster requires a refund to another payment card or in cash.

In order to prevent transactions with a PIN-code in case of loss or theft of a payment card, the PIN-code shouldn't be kept together with the payment card.

However, it should be noted that recently it has become widespread to make contactless payments with payment cards without requiring a certain amount of PIN-code. While this feature provides convenience in retail payments, it also carries a high risk of fraud. It is more convenient to carry out fraudulent transactions with lost or stolen payment cards, as contactless payments do not require entering PIN-code until certain amount. The application of limits (number, amount) on contactless payment operations defined by issuer banks aimed to prevent losses in such type operations and these limits adapted to consumer habits.

In order to prevent online transactions from fraudsters, the issuing bank or service centre must use the 3D Secure Service to authorize payments. The dynamic password provided by this service (one-time password – One Time Password) is constantly changing for each payment transaction and is received by SMS notification, e-mail, e-token and other methods. Otherwise, the password is set in static form by the cardholder and remains unchanged.

➢ ***Transactions with fake cards***

During these fraudulent transactions, fraudsters create a fake payment card based on real payment card information. Payment card information captured in various ways. For example, during the embossing of a payment card, the personalization of a new payment card can be shown by unauthorized interception of payment card information.

Fig. 1. Equipment for scimming, installed in the payment terminal

The most common technology calls skimming. Skimming is the creation of a new payment card based on the information captured on the magnetic tape of the payment card through special equipment installed in the payment terminal (Pic 1).

In some cases, the cashier, waiter and other persons of the business entity seize payment card information by the usage of the same method and these information provided to fraudsters.

The cardholder should pay attention to the above-mentioned cases in order to prevent unauthorized seizure of payment card information. For example, the cardholder must make sure that no additional equipment installed before making transactions at the payment terminal or must not present the payment card to other persons. When the payment card is presented to other persons, it must be controlled. It is also important to avoid the use of unsupervised and, in general, suspicious ATMs located in unlit areas.

➢ ***card not present (CNP) operations***

CNP operations usually carried out without the physical presence of the payment card and the card user. While the execution these types of payment transactions, the cardholder communicates the necessary information of the payment card by various means. Payment transactions made without a payment card divided into the following parts:

✓ ***E-commerce –*** the cardholder obtains products and services and enters payment card information via the internet;

✓ ***Periodic payment operations (Recurring)*** – the cardholder agrees once on the period and amount of the payment transaction. In the next stages, payment transactions are made through the card account on the basis of this agreement;

✓ ***MO / TO payment operations*** – in the absence or widespread use of the internet, remote payment card transactions carried out by mail, telegraph, telephone, and mobile phone. For this reason, such payment transactions are called Mail order\Telephone order. Necessary information of the payment card is disclosed, stating the product and service to be obtained by the cardholder for the payment transaction. After entering the data manually in the POS-terminal, the payment operation is performed;

✓ ***Instalment payments*** – the execution of payments for the cost of products and services, loan payments in instalments. The total amount to be paid by agreement between the card user and the business entity is divided into parts and removed from the card account.

There are various types of fraud for payment transactions made without the above-mentioned payment card. This includes fraudulently presenting himself as an authorized representative of a bank or business entity, obtaining payment card information, conducting transactions on fake e-commerce pages, conducting MO / TO transactions with stolen or counterfeit payment cards, etc.

Different security requirements must be observed in order to avoid fraud in card not present transactions. For example, SMS notifications should be considered for regular payment transactions. Reliable business entities should be selected in MO\TO operations, and various applications should be properly evaluated under the guise of providing payment card information. In case of doubt, the issuing bank should be contacted directly.

When making payments through e-commerce, payments must be made in the same way in reliable businesses, 3D Secure Service must be used, the payment window must have the logo of the relevant international card organization and other requirements. It should be noted that these requirements must be provided by each issuing bank to its customers beforehand.

Currently, the most common cases of fraud in the world occur in places where the payment card is not physically used. According to research conducted by international think tanks, at least 130 billion dollars will be lost worldwide between 2018 and 2023 as a result of fraudulent transactions without a payment card. It is forecasted that the funds will be lost in the amount of USD.

✓ ***transactions with undelivered payment cards***

This type of fraud is carried out by a bank or postal service employee. Before the payment card is delivered to the cardholder, payment operations are carried out by taking the payment card information. At the same time, a fake payment card can be made based on the information of this payment card. In this case, the fraudster tries to deliver the payment card to the cardholder in an untouched state. In practice, bank specialists prepare new payment card information, and even prepare a new one by obtaining a PIN-code.

To avoid such situations, the cardholder should be careful if the payment card is delivered to the address, for example, make sure that the envelope with the PIN-code is opened by himself. It should be noted that an important tool in preventing this type of fraud is the PIN-set service which currently used by banks. The PIN-set service allows the customer to present only the payment card and at the next stage the PIN-code is generated independently by the card user via ATM or POS-terminal infrastructure.

Just as fraudulent transactions are divided into different types, different methods are used to carry out these operations:

Phishing – fraudsters send a fake e-mail to the cardholder on behalf of the bank and demand to enter the payment card information under various pretexts, to verify personal information. The information provided by the cardholder is used in the next stage of fraud. The most famous example of this is the practice of fraud, nicknamed the Prince of Nigeria. A person who introduces himself as a relative of Nigerian king or official demands personal information from people, promising millions. By constantly imitating (copying) received (trusted) e-mails, viruses can be sent to it, and as a result, any activity can be performed by accessing the computer.

Vishing and smishing – fraudster obtains payment card information from a cardholder appropriately by making a phone call or through SMS notification. Based on this information he/she could execute online payments or prepare fake payment cards.

As it is known, the peculiarities of the pandemic period had a positive impact on the expansion of remote banking services and the growth of e-commerce. The increase in the volume of digital payments in these areas encourages fraudsters to apply new methods in this area. Currently, two different methods used by fraudsters are more common:

❖ The scammer communicates with the seller of the product or service sold on the internet by contacting the mobile application "whatsapp" via telephone numbers belonging to other countries. They then state that they are currently in another region or country and will pay for the product or service in full or in part through a payment card. On this basis, the seller's payment card information is obtained. The fraudster, who identifies the issuing bank by issuing the first 6 digits of the seller's payment card, registers with the bank's mobile banking service. If additional information is required during registration, such as the user's identity card information to identify him, the fraudster also obtains this information for identifying the seller. Thus, the scammer creates confidence in the seller against himself. Most banks send a one-time password to the cardholder to complete the registration. The scammer asks to provide one-time password to complete the transfer. In convinces that the funds are currently in the intermediate account and a one-time password must be provided to the cardholder in order for it to be credited to the seller's card account. After the seller provides the fraudster with a one-time password received via SMS notification, the fraudster unauthorized seizes the funds on payment cards through the mobile banking service.

❖ The second method is the same as the first. However, the main difference is that in this case no card information or a one-time password is required directly from the seller. The scammer states that "postal services" will be used to purchase the product and that the goods will be delivered by courier. It then sends the link to the fake website to the seller for payment. After entering this link, the seller will come across a window with the name, surname and patronymic of the sender, the number of the payment order, the name of the purchased product and its price. There is no doubt that the design of the website is identical to the website of the country's banks, national postal operator or other payment service provider. In order to receive the money, the seller is required to enter the payment card number, cardholder's name and surname, expiration date and security code CVV or CVC in the newly opened window after pressing the button "accept money on the card" or another name. After entering this information, a window will open with the message "Enter the exact balance on the card to confirm you as a cardholder" and the seller will enter the information on that page. In this case, the fraudster looks at the information provided by the seller, and if the funds in the card account are attractive to him, the payment operation is carried out through the websites of foreign banks. If the card user's payment card supports the 3D Security protocol, then the bank will provide him with a one-time password based on SMS notification. As the user is not fully aware of the operation, he enters the received one-time password as a continuation of the operation. In this case, the fraudster has successfully completed the transaction and misappropriates the money on the seller's payment card. If the payment card is not connected to the 3D Security service, then the transaction is completed successfully or unsuccessfully within the limits set by the bank.

Fake anti-virus alerts – Some websites offer cheap or free anti-virus software, which, after downloading, installs a hidden virus on your computer and gives you access to personal information (Pic. 2). In this way, even a person can be blackmailed and extorted money by threatening to delete his computer files or share personal information.

Application fraud – this is in some cases related to the theft of an identity document. Thus, fraudsters illegally order a credit card from a bank on the basis of an identity document of other persons. In this case, the scammer must be prepared in advance to address any questions that may arise regarding the mobile phone and the workplace.

II. Statistics in the field of fraud

Fraud transactions and their development trends are evolving in line with the development trends of the payment card market. In many cases, these two indicators are directly related to the development of fraudulent transactions and the payment card market. New projects in the payment card market always attract the attention of fraudsters and create a favorable field of activity for them.

The issuance of payment cards and the introduction of innovations in the framework of social projects financed from the state budget create a favorable environment for the rapid increase in fraud in this area. The initial years of the distribution of social payments in post-Soviet countries by payment cards, createdan additional source of income for fraudsters. Thus, the first acquaintance of the population with payment cards,

the lack of necessary knowledge allowed to carry out such fraudulent operations without the use of additional technical means. In the days when social payments were distributed, fraudsters stood in line near ATMs and seized payment cards and PINs by various means to achieve their goals.

Fig. 2 Fake anti-virus alert

For this reason, it is important for the country's legislation to require financial institutions to conduct risk assessments when applying new payment solutions.

According to the 6th report of the European Central Bank "Payment Card Fraud" published in 2020, the total volume of fraudulent transactions with payment cards issued within the Single European Payment Area (SEPA) in 2018 amounted to 1.8 billion euros. In 2018, the total volume of transactions with payment cards issued under SEPA amounted to 4.84 trillion euros. This means that in 2018, 0.037% of the volume of transactions with payment cards within SEPA was fraudulent. The total volume of fraudulent transactions increased by 13% compared to 2017, while the total volume of card transactions increased by 6.5%. During 2018, 79% of fraudulent transactions with payment cards were carried out without payment cards, 15% through POS-terminal network, and 6% through ATM infrastructure [15].

Due to the underdevelopment of the payment card market in the Republic of Azerbaijan compared to developed European countries, cases of fraud with payment cards are not widespread. The volume of payment card transactions in the Republic of Azerbaijan in 2020 amounted to 28.1 billion manat, of which 23% (6.38 billion manat) falls on non-cash payments. 2.2 billion manat in non-cash payments was implemented through POS-terminal, 0.28 billion manat through ATM, 3.9 billion manat through e-commerce [16; 17].

Looking at the statistics on fraudulent transactions in payment cards in Azerbaijan, it is clear that the correlation between the volume of transactions with payment cards and the volume of fraudulent transactions in this area is negative. Thus, the total volume of domestic card transactions in 2015 amounted to 11.7 billion manat, the total volume of fraud operations 1.2 mln. manat, and in 2020 – 28.2 billion manat, and 0.6 mln. manat, respectively. This means that there was a negative correlation coefficient. The mathematical correlation coefficient of these two indicators for 2014-2020 is calculated as follows:

To calculate the correlation coefficient, find the standard deviation of the sample for each variable, and then the covarians [2; 3]:

$$S_X = \sqrt{\frac{\sum(X_i - \bar{X})^2}{n-1}} \quad (1)$$

$$S_Y = \sqrt{\frac{\sum(Y_i - \bar{Y})^2}{n-1}} \quad (2)$$

$$S_{XY} = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{n-1} \quad (3)$$

$$r = \frac{S_{XY}}{S_X S_Y} \quad (4)$$

Sample standard deviations of both variables are found, and after calculating the covariance between these variables, it is possible to calculate the correlation coefficient of these two variables.

Since the number of data is small and the manual calculation does not take much time, the correlation coefficient is calculated in the following sequence:

$$S_X = \sqrt{\frac{(1.26 - 1.6)^2 + (1.2 - 1.6)^2 + (0.6 - 1.6)^2 + \cdots \ldots + (0.62 - 1.6)^2}{7 - 1}} = 1.6$$

$$S_Y = \sqrt{\frac{(11.1 - 16.6)^2 + (11.7 - 16.6)^2 + (11.8 - 16.6)^2 + \cdots \ldots + (28.1 - 16.6)^2}{7 - 1}} = 6.5$$

$$S_{XY} = \sqrt{\frac{(1.26 - 1.6)(11.1 - 16.6) + (1.2 - 1.6)(11.7 - 16.6) + \cdots \ldots + (0.62 - 1.6)(28.1 - 16.6)}{7 - 1}} = -2.35$$

$$r = \frac{-2.35}{1.6 * 6.5} = -0.23$$

It is clear from the calculations that the correlation coefficient between the volume of payment card transactions in the Republic of Azerbaijan for 2014-2020 and the volume of fraudulent transactions is -0.23. The economic essence of this is that as the volume of payment card transactions increases, the volume of fraudulent transactions decreases.

In this regard, it was proved that, in contrast to international practice, there is no positive correlation between the volume of payment cards and the volume of fraudulent transactions in Azerbaijan. The main reason for this is the low volume of fraudulent transactions in Azerbaijan and, in some cases, the incorrect submission of statistical information on fraudulent transactions by banks to the Central Bank. The low volume of fraudulent transactions or the unattractiveness of the payment card market for fraud can be explained by the level of development of digital payments and the low level of domestic transaction turnover.

Comprehensive statistical reporting is important in making the right decisions to prevent payment card fraud. It is at this stage that regulators should ensure that statistical reporting is provided on a regular basis to ensure proper analysis of the payment card market and adequate action.

Statistical reporting should be collected on a regular basis (mainly on a quarterly basis). This period should correspond to the nature of transactions with payment cards. Statistical reporting must be submitted by financial institutions that issue payment cards.

Depending on the nature of the fraud, statistical reporting should be differentiated according to domestic and foreign, network of payment terminals, method of storing information on the payment card, the statistical unit's own network or network of payment terminals of another bank and other indicators will allow for a more accurate assessment of fraudulent transactions abroad.

The most important factor here is the implementation of a policy of control over the collected statistical reporting. The accuracy of statistical reports provided by financial institutions should be monitored by on-site inspections of financial institutions, regular market research, surveys, identification of existing gaps by acting as an anonymous client, and other methods.

III. Preventive measures against fraud

In addition to causing financial losses, fraudulent transactions have a negative impact on the security of the banking system and undermine public confidence in digital payments. Timely detection of fraudulent operations and identification and implementation of preventive measures have always been in the focus of regulatory and supervisory authorities, banks and other financial institutions.

In order to prevent fraudulent transactions, the Central Bank often acts in a different direction. First of all, the steps to be taken to prevent fraud are reflected at the legislative level. Examples include the need for financial institutions to have internal rules and procedures for risk management, the requirement to enforce a contract in a bank-customer relationship, and the security of payment terminal infrastructure.

This includes fraudulent transactions in some countries where a single centralized registry (portal) is formed at the initiative of central banks. This approach plays an important role in timely notification of other financial institutions and in the formation of future policy. On this basis, the formation of a working group with the involvement of financial market participants is one of the applied practices.

One of the priority goals of central banks in this area is to create an information platform to inform the public, including banking professionals, and to share international experience on a regular basis. Understanding the mechanism by which these fraudulent transactions occur will ensure that the preventive measures taken as a result of a systematic approach are more effective (Pic. 3). [5; 14].

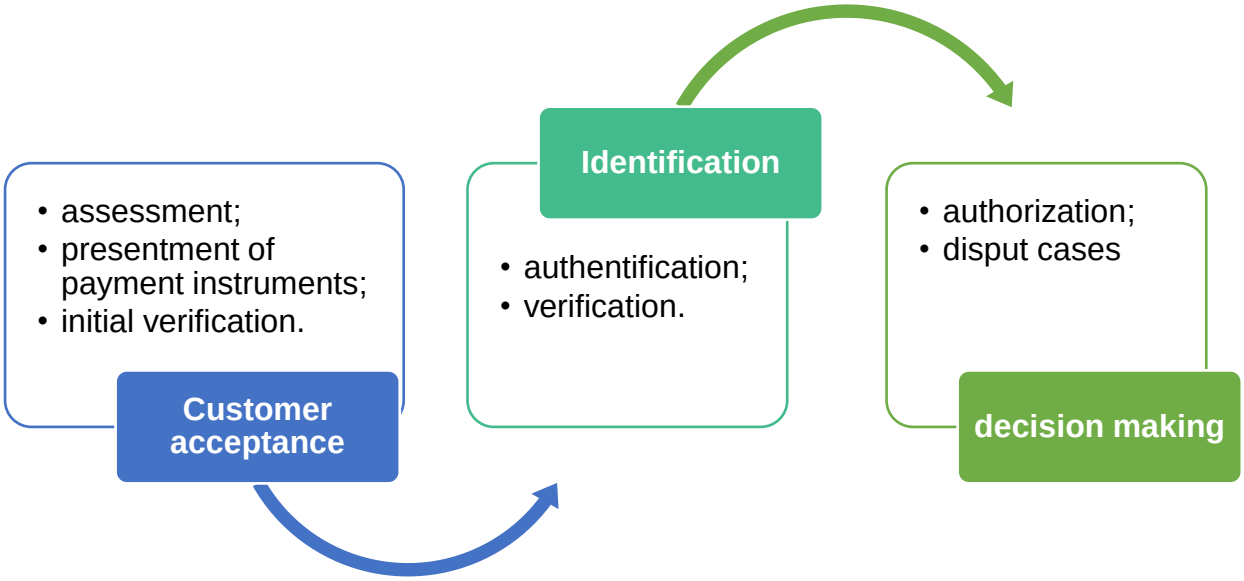

Fig.3. Payment cards and transaction stages

Customer acceptance. This stage plays a crucial role in the provision of both issuance and acquirer services, as well as in the operational regulation of fraud prevention in general. At this stage, when the bank first meets the customer, the customer is assessed, as well as risk analysis.

Information for customer evaluation is obtained from internal and external sources. This information is directly related to the products and services that the customer wants to obtain. For example, if information is requested from the centralized credit register when issuing credit cards related to a credit line, this is not necessary when issuing debit payment cards.

Internal sources can include the history of the customer formed as a result of previous service in the bank, the information about the customer by the bank employees. Information from external sources is obtained through centralized information resources, questionnaires, analysis of submitted documents, questions and answers with the client and other means.

Identification. Identification can be equated with the identification established by law in the field of combating money laundering and terrorist financing, ie the identification of an individual. In the case of identification in digital payments, the payment transaction is confirmed by the card user using a payment instrument that can be presented to him.

During authentication process, the financial institution identifies the payment transaction by the card user in possible ways, for example, with a one-time password. During verification, the financial institution verifies and verifies the information entered by the card user. Verification of the entered data is carried out at the expense of internal and external information resources.

Decision making. This is one of the most important steps in preventing fraudulent card transactions. During the authorization, the payment transaction carried out by the issuer on the basis of pre-entered risk scenarios is checked against fraud and approved. The risk scenarios applied are determined taking into account the cases of fraud that may occur.

Disputes arising from payment card transactions are resolved through platforms provided by international card organizations, unless they are resolved independently between banks. In this case, the dispute is resolved in compliance with the requirements of the internal rules of the international card organization.

In order to implement preventive measures against card fraud, the following steps should be taken by financial institutions:

1. **Assessment of current position**

First of all, the current situation should be assessed by banks. As part of this assessment, payment cards and transactions with them should be divided into stages to identify all possible areas where fraudulent transactions could be potentially affected.

Because fraud affects the stages described in this scheme in a specific way, each stage must be analyzed individually as part of a comprehensive approach. The analysis should distinguish between the effects of internal and external factors.

2. **Defining benchmark targets**

The assessment should identify a set of key targets to be considered a benchmark for fraud prevention. This set of targets may include interest rates on chargeback transactions, card user retention rate, number of failed transactions, approval rate for transactions without payment card, and other indicators.

3. **Separation of powers**

Once the evaluation results and benchmark set have been obtained, the division of powers between the structural units should be reconsidered. On this basis, the decision-making, executive and key influencing structures should be identified first. Also, the formulation of the strategy, preparation of the implementation plan, control over the implementation process and achievement of the identified targets, implementation stages and evaluation of the achieved results and other stages should be divided between the relevant structural units.

4. **Application of tools and means**

The tools and means to be applied in parallel with the division of powers are also identified. These tools and means include identifying risk scenarios, raising awareness, further improving the knowledge and skills of employees, building relationships with stakeholders, including regulators and regulators, international card organizations and banks, adopting and applying best international practices, and more. includes. The tools and means to be identified at this stage are aligned with the objectives.

5. **Usage of alternative opportunities**

The application of alternative instruments should also be analyzed when identifying internal resources and opportunities within the bank. As an alternative, the tools and tools used by international card organizations and processing service centers to prevent risks, as well as the risk management systems of various financial institutions can be considered.

Conclusions and perspectives of further research. Depending on the nature of payment card transactions and the risk scenarios used, the results obtained after a certain period (month, quarter, half a year, etc.) should be analyzed and evaluated. The results of the assessment, which will be prepared in the form of a specific act or report, should not only determine the level of achievement of the objectives set at the initial stage, but also determine the steps to be taken in the future. As a result of the assessment, deficiencies in existing procedures should be identified and improved.

As the digital payment market, including payment cards, develops, fraudsters who want to make easy money are becoming increasingly interested in the field. From the above, it is concluded that the main cases of fraud can be combated by financial institutions and card users by complying with these requirements. The negative correlation between the increase in the volume of transactions with payment cards and the volume of fraudulent transactions is explained by the inaccuracy of statistical reporting by financial institutions and the lack of interest for fraudsters due to the lack of market development. Payment card transactions should be analyzed step by step in order for financial institutions to apply preventive measures in a more systematic way.

ЛІТЕРАТУРА

1. Девід А. Монтегю. Методи запобігання шахрайству при шахрайстві з кредитними картками, видавництво Trafford, 6 липня 2006, 212 с.

2. Гуджаратська. Основна економетрика, 3-е вид. 1995, 838 с.

3. Гуджаратська. Основна економетрика, 4-е вид. 2004, 1003 с.

4. Індійський інститут банківської справи та фінансів. Запобігання кіберзлочинам та управління шахрайством, 2017

5. Мадан Лал Бхасін. Боротьба з банківськими шахрайствами шляхом інтеграції технологій: досвід країни, що розвивається. Школа бухгалтерії, Коледж бізнесу, Університет Утара, Малайзія, Сінток, Британський науковий журнал, 2016.

6. Реваті Субраманіан. Банківське шахрайство: використання технологій для боротьби із збитками – Уайлі, 2 квітня 2014, 192 с.

7. Capgemini – [Електронний ресурс]. – Режим доступу: https://www.capgemini.com/wp-content/uploads/2018/08/Capgemini-CPP-Fraud-Analytics-Solution-with-Google-Cloud.pdf

8. PwC Global – [Електронний ресурс]. – Режим доступу: https://www.pwc.com/cz/en/bankovnictvi/assets/pdf/pwc-forensic-capability-brochure.pdf

9. Fintexperts – [Електронний ресурс]. – Режим доступу: https://www.csiweb.com/how-we-help/enterprise-banking/core-bank-processing/fraud-risk-management/

10. SWIFT Company – [Електронний ресурс]. – Режим доступу: https://www.swift.com/your-needs/financial-crime-cyber-security/financial-fraud/payments-fraud

11. FIS fintech accelerator. – [Електронний ресурс]. – Режим доступу: https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/payment-fraud-vs-identity-theft-whats-the-difference

12. Chargebee. – [Електронний ресурс]. – Режим доступу: https://www.chargebee.com/blog/optimize-online-billing-stop-online-fraud/

13. Altexsoft software and engineering. - [Електронний ресурс]. - Режим доступу: https://www.altexsoft.com/whitepapers/fraud-detection-how-machine-learning-systems-help-reveal-scams-in-fintech-healthcare-and-ecommerce/

14. McKinsey and Company. – [Електронний ресурс]. – Режим доступу: https://www.mckinsey.com/industries/financial-services/our-insights/combating-payments-fraud-and-enhancing-customer-experience

15. European Central Bank. – [Електронний ресурс]. – Режим доступу: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202008~521edb602b.en.html

16. The State Statistical Committee of the Republic of Azerbaijan. – [Електронний ресурс]. – Режим доступу: www.stat.gov.az

17. Central Bank of the Republic of Azerbaijan. – [Електронний ресурс]. – Режим доступу: https://www.cbar.az

18. Глобальне дослідження з питань шахрайства у банківській сфері. KPMG-Україна. 2019. 24 с.

REFERENCES

1. David A. Montague. Fraud Prevention Techniques for Credit Card Fraud, Trafford Publishing, July 6, 2006, 212 pages.

2. Gujarati. Basic Econometrics, 3th edition. 1995, 838 p.

3. Gujarati. Basic Econometrics, 4th edition. 2004, 1003 p.

4. İndian İnstitute of banking and finance. Prevention of cyber crimes and fraud management, 2017

5. Madan Lal Bhasin. Combatting Bank Frauds by Integration of Technology: Experience of a Developing Country, School of Accountancy, College of Business, Universiti Utara Malaysia, Sintok, Malaysia, British Journal of Research, 2016.

6. Revathi Subramanian. Bank Fraud: Using Technology to Combat Losses – Wiley, 2 April 2014, 192 pages

7. Capgemini. (n.d.). Retrieved from https://www.capgemini.com/wp-content/uploads/2018/08/Capgemini-CPP-Fraud-Analytics-Solution-with-Google-Cloud.pdf

8. PwC Global. (n.d.). Retrieved from https://www.pwc.com/cz/en/bankovnictvi/assets/pdf/pwc-forensic-capability-brochure.pdf

9. Fintexperts. (n.d.). Retrieved from https://www.csiweb.com/how-we-help/enterprise-banking/core-bank-processing/fraud-risk-management/

10. SWIFT Company. (n.d.). Retrieved from https://www.swift.com/your-needs/financial-crime-cyber-security/financial-fraud/payments-fraud

11. FIS fintech accelerator. (n.d.). Retrieved from https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/payment-fraud-vs-identity-theft-whats-the-difference

12. Chargebee. (n.d.). Retrieved from https://www.chargebee.com/blog/optimize-online-billing-stop-online-fraud/
13. Altexsoft software and engineering. (n.d.). Retrieved from https://www.altexsoft.com/whitepapers/fraud-detection-how-machine-learning-systems-help-reveal-scams-in-fintech-healthcare-and-ecommerce/
14. McKinsey and Company. (n.d.). Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/combating-payments-fraud-and-enhancing-customer-experience
15. European Central Bank. (n.d.). Retrieved rom https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202008~521edb602b.en.html
16. The State Statistical Committee of the Republic of Azerbaijan. (n.d.). Retrieved from www.stat.gov.az
17. Central Bank of the Republic of Azerbaijan. (n.d.). Retrieved from https://www.cbar.az
18. Global Banking Fraud Survey. KPMG-Ukraine, 2019. 24 p.