CZU 343.711

DOI 10.5281/zenodo.7624981

PROCEDEE DE SUSTRAGERE ILEGALĂ A MIJLOACELOR BĂNEȘTI PRIN INTERMEDIUL CARDURILOR BANCARE SAU A BANCOMATELOR. METODE DE PREVENIRE

Marian GHERMAN,
doctor în drept, conferențiar universitar

Subiectul cercetat se referă la un fenomen infracțional foarte răspândit în ultimii ani. Sustragerile ilegale a mijloacelor bănești de pe cardurile bancare sau prin intermediul bancomatelor au luat o mare amploare, fapt care este confirmat de către statisticile structurilor polițienești autohtone, dar și internaționale. În studiul dat mă voi axa pe cercetarea celor mai răspândite forme de sustragere a mijloacelor financiare de pe cardurile de plată, precum și la procedeele de compromitere a ATM-urilor(Automated Teller Machine – automat bancar), săvârșite în aceleași scopuri. Concomitent mă voi referi și la metodele de prevenire a acestui flagel, expuse deseori în recomandările Băncii Naționale a Moldovei (BNM), care au menirea de a recomanda deținătorilor de carduri de plată respectarea unor reguli elementare în procesul de mânuire a acestora pentru a evita riscurile de compromitere a bancomatelor sau cardurilor bancare.

Cuvinte-cheie: Card bancar, ATM, skimming, phishing, malware, cash trapping, black box.

PROCEEDINGS OF ILLEGAL EMBEZZLEMENT OF FUNDS THROUGH BANK CARDS OR ATMS. PREVENTION METHODS

Marian GHERMAN,
PhD, associate professor

The researched subject refers to a criminal phenomenon that became very widespread during the recent years. Illegal withdrawals of money from bank cards or through ATMs have taken a large scale, a fact that is confirmed by the statistics of domestic and international police structures. In the given study, I will focus on researching the most widespread forms of embezzlement of financial means from payment cards, as well as the procedures for compromising ATMs (Automated Teller Machines), carried out for the same purposes. At the same time, I will also refer to the methods of preventing this scourge, often exposed in the recommendations of the National Bank of Moldova (NBM), which are intended to justify payment cardholders to observe some elementary rules in the process of handling them in order to avoid risks of ATMs or bank cards compromising.

Keywords: bank card, ATM, skimming, phishing, malware, cash trapping, black box.

Introducere. Dezvoltarea social-economică și atingerea unor noi performanțe în toate sferele vieții sociale ale Republicii Moldova și ale altor țări este imposibil de efectuat fără o luptă activă cu criminalitatea, inclusiv cu persoanele ce fabrică sau pun în circulație cardurile bancare false, dar și sustrag sursele financiare existente pe aceste carduri.

Pe acest „câmp de luptă" continuă, unde nu există timp de pace, nu de acum, ci de câțiva ani buni, se confruntă două tabere: pe de o parte a baricadei sunt autoritățile statului – și aici putem menționa emitenții cardurilor bancare, autoritățile de aplicare a legii, de cealaltă parte se află „adversarii" acestora, falsificatorii

Introduction. The socio-economic development and the achievement of new performances in all spheres of the social life of the Republic of Moldova and other countries is impossible without an active fight against crime, including the people who manufacture or put into circulation fake bank cards, but also embezzle financial sources existing on these cards.

Two camps are facing each other on this continuous "battlefield" where there is no time for peace, the fight lasting for several years: on the one side of the barricade are the state authorities - and here we can mention bank card issuers, law enforcement authorities, on the other side are their "adversaries", bank card

de carduri bancare sau persoanele care sustrag banii de pe carduri.

Fiecare dintre cei aflați de partea „dreaptă" a baricadei își au sarcini și scopuri determinate, unii de dezvoltare a mijloacelor și metodelor de protecție a cardurilor bancare, precum și a măsurilor de contracarare a sustragerilor de pe aceste carduri, alții de a fi în pas cu progresul tehnologic și respectiv concentrându-se pe acumularea de cunoștințe și aptitudini (dexterități) pentru a „sparge" sistemul electronic de protecție și deservire a cardurilor bancare.

Actualitatea temei investigate. Cu toate că nivelul cultural de dezvoltare al omenirii în prezent este destul de înalt, fabricarea și punerea în circulație a cardurilor false sau sustragerea ilegală de surse bănești de pe cardurile bancare este o problemă actuală. Deseori, pentru satisfacerea cerințelor materiale, îmbogățirea ilicită, procurarea de averi etc., unele persoane recurg la fabricarea sau punerea în circulație a cardurilor bancare false, dar mai des la sustragerea prin înșelăciune a mijloacelor bănești de pe cardurile bancare perfectate legal ale victimelor. Falsul de carduri bancare devine din ce în ce mai perfect, iar modalitățile de sustragere ilegală a banilor din ce în ce mai inventive. Este de menționat că activitatea de falsificare și sustragere ilegală tot mai des are un caracter internațional, infractorii cu ușurință deplasându-se în orice colț al lumii pentru a efectua sustrageri ilegale de bani.

Progresul tehnologic a generat apariția noilor tehnologii, precum și a aparatajului nou și performant de copiat și multiplicat, care de fapt a contribuit la creșterea masivă a numărului cardurilor bancare falsificate și, evident, la creșterea posibilităților de ocolire a măsurilor de protecție bancară.

Mărimea pagubei aduse sistemului bancar al statului, dar și fiecărui cetățean în parte (deținător de card bancar) este în creștere. În contextul celor expuse mai sus, am hotărât să contribuim, prin intermediul acestei cercetări, la înmulțirea cunoștințelor despre criminalitatea economică, cu ajutorul cardurilor bancare sau prin intermediul lor (sustrageri ilegale de pe cardurile bancare), dar și să propunem anumite măsuri de protecție în vederea contracarării acestui flagel.

Scopul cercetării constă în fundamentarea cunoștințelor în domeniul investigării

forgers or people who steal money from cards.

Each of those on the "right" side of the barricade have their own specific tasks and goals, some to develop the means and methods of protecting bank cards, as well as measures to counter embezzlement from these cards; others to keep pace with technological progress and respectively focusing on the accumulation of knowledge and skills (dexterity) to "break" the electronic system of protection and servicing of bank cards.

Actuality of the investigated topic. Although the cultural level of development of humankind today is quite high, the manufacture and circulation of fake cards or the illegal embezzlement of money sources from bank cards is a current problem. Often, in order to satisfy material requirements, illicit enrichment, acquisition of wealth, etc., some people resort to the creation or circulation of fake bank cards, but more often to fraudulently withdrawing funds from the victims' legally completed bank cards. Forgery of bank cards is becoming much more perfect and the ways of illegally money siphoning progressively inventive. It should be mentioned that the activity of forgery and illegal embezzlement increasingly has an international character, with criminals easily moving to any corner of the world to carry out illegal embezzlement.

Technological progress has generated the emergence of new technologies, as well as new and high-performance equipment to copy and multiply, which in fact has contributed to the massive increase in the number of counterfeit bank cards and, obviously, to the increase in the possibilities of circumventing bank protection measures.

The amount of damage caused to the state banking system, but also to each individual citizen (bank card holder) is increasing. Within the context of the above, we decided to contribute, through this research, to the increase of knowledge about economic crime, with the help of bank cards or through them (illegal embezzlement from bank cards), but also to propose certain protection measures in order to counteract this scourge.

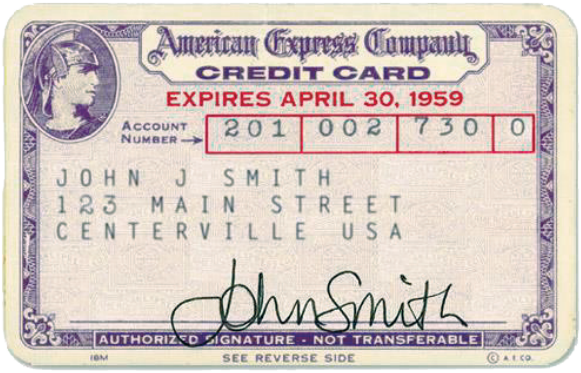
The purpose of the research consists in substantiating knowledge in the field of inves-

infracţiunilor legate de sustragerile ilegale a mijloacelor băneşti de pe cardurile bancare, precum şi în elaborarea metodelor de prevenire a acestora.

Conţinutul de bază. Cardurile bancare s-au transformat dintr-un mijloc de lux de plată în unul din cele mai populare şi utile obiecte care uşurează viaţa fiecărui dintre noi. Deşi această bucată de plastic nu pare la prima vedere sigură, cardurile reprezintă unul din cele mai sigure eficiente mijloace prin care puteţi efectua plăţi şi tranzacţii bancare.

La moment cea mai mare rată de utilizare a cardurilor bancare este în SUA, unde au fost emise peste 900 mln de carduri bancare. Pe plan mondial au fost emise circa 8 000 000 000 de bucăţi. Dacă unim toate cardurile bancare, acestea vor acoperi o suprafaţă de 37 km pătraţi sau de 84 de ori suprafaţa totală a Vaticanului! În medie, cardurile bancare sunt responsabile pentru circa 5,5 trilioane de tranzacţii în cele 24 de milioane de locaţii în peste 200 de ţări ale lumii.

Prima idee generală de card a apărut la începutul secolului XX, când corporaţiile petroliere şi magazinele comerciale au emis propriile carduri pentru dezvoltarea serviciu-



lui clienţi şi drept un mijloc de a contribui la consolidarea spiritului de loialitate a clienţilor. Cardurile puteau fi folosite doar la întreprinderile emitente ale cardului, de aceea popularitatea acestora nu era recunoscută pe scară globală.

În anul 1949, Diners Club şi American Express au lansat primul card bancar modern creat din plastic. Acesta a fost creat exclusiv pentru plăţile în 27 de restaurante renumite din oraşul New York. Până în anul 1951 circa 20 000 de norocoşi erau deţinători ai acelor carduri bancare[1].

tigating crimes related to the illegal embezzlement of funds from bank cards, as well as in developing methods to prevent them.

Basic content. Bank cards have turned from a luxury means of payment into one of the most popular and useful objects that make life easier for each of us. Although this piece of plastic does not seem secure at first glance, cards are one of the most secure and efficient means by which you can make payments and bank transactions.

Nowadays, the highest rate of use of bank cards is in the USA, where more than 900 million bank cards have been issued. About 8,000,000,000 pieces were issued worldwide. If we put all the bank cards together, they will cover an area of 37 square kilometers or 84 times the total area of the Vatican! Overall, bank cards are responsible for about 5.5 trillion transactions in the 24 million locations within over 200 countries of the world.

The first general card idea appeared at the beginning of the 20th century, when oil corporations and retail stores issued their own cards for the development of customer service

and as a means of helping to strengthen the spirit of customer loyalty. The cards could only be used at card-issuing businesses, so their popularity was not recognized on a global scale.

Diners Club and American Express launched the first modern bank card made of plastic in 1949. It was created exclusively for payments in 27 famous restaurants from New York City. About 20,000 lucky people were holders of those bank cards until 1951 [1].

Although in 1952 the Diner's Club card was accepted in 400 restaurants, 30 hotels, 200

Deşi în anul 1952 cardul Diner's Club era acceptat în 400 de restaurante, 30 de hotele, 200 de companii de închiriere a maşinilor şi la 4 florării, creatorul cardului McNamara considera că aceste carduri bancare au devenit inutile şi a vândut partea sa din companie. Acesta a primit 200 000 de dolari, ceea ce este echivalentul a 1,6 milioane de dolari în ziua de azi.

Prima utilizare a cardurilor cu bandă magnetică se datează la începutul anilor '60 ai secolului trecut, atunci când Autoritatea de Tranzit de la Londra a instalat banda magnetică pentru a putea introduce informaţiile cu privire la contul deţinătorului. Odată cu introducerea benzii magnetice, cardurile bancare au început să devină din ce în ce mai populare datorită asigurării unei securităţi sporite pentru economiile clienţilor, comodităţii şi mai târziu datorită posibilităţii de a folosi cardul bancar la terminalele şi bancomatele băncilor comerciale.

Până în anul 1966, clienţii se puteau folosi doar de propriile economii de pe contul curent al acestuia, iar din conceptul de a face profit băncile comerciale au creat primele carduri de credit. Ideea genială de a percepe dobânda pentru banii folosiţi de către clienţi a fost bazată pe afacerea de percepere a taxelor.

Odată ce cardurile bancare puteau aduce profit, în anul 1966 Bank of America a înfiinţat corporaţia BankAmerica Service, pe care mai târziu a creat drept franciză brandul BankAmericard. Acel brand în ziua de azi este recunoscut drept Visa. În acelaşi an, un grup de bănci emitente au fondat asociaţia InterBank Card pentru crearea unui nou sistem naţional de carduri bancare, care avea drept scop concurenţa directă cu programul Visa. Acel sistem se numea MasterCharge, în zilele noastre fiind recunoscut sub numele MasterCard Worldwide.

Deşi American Express a fost una dintre primele companii care au creat carduri bancare, abia în anul 1987 aceasta a lansat primul card de credit ce oferea posibilitatea de a rambursa creditul, indiferent de perioadă şi nu doar la sfârşitul fiecărei luni.

În timp ce cardurile bancare din plastic au fost standardizate pentru o jumătate de secol, noile evoluţii recente demonstrează crearea unor forme alternative în metodele de plată. Una dintre inovaţiile recente sunt plăţile prin intermediul portmoneelor electronice şi chiar implantarea cipurilor în telefoanele mo-

car rental companies and 4 florists, the creator of the McNamara card believed that these bank cards had become useless and sold his share of the company. He received $200,000, which is the equivalent of $1.6 million today.

The first use of magnetic strip cards dates back to the early 60s' of the last century, when the London Transit Authority installed the magnetic strip to be able to enter the holder's account information. With the introduction of the magnetic strip, bank cards began to become more and more popular due to the provision of increased security for customers' savings, convenience and later due to the possibility of using the bank card at the terminals and ATMs of commercial banks.

Until 1966, customers could only use their own savings from their current account, and commercial banks created the first credit cards from the concept of making a profit. The brilliant idea of charging interest on the money used by customers was based on the toll collection business.

Once bank cards could bring profit, in 1966 Bank of America established the BankAmerica Service Corporation, which it later franchised under the BankAmericard brand. That brand is recognized today as Visa. During the same year, a group of issuing banks founded the InterBank Card Association for the creation of a new national bank card system, which aimed to compete directly with the Visa program. That system was called MasterCharge, nowadays known as MasterCard Worldwide.

Although American Express was one of the first companies to create bank cards, only in 1987 it launched the first credit card that offered the possibility to repay the loan regardless of the period and not just at the end of each month.

While plastic bank cards have been standardized for half a century, recent new developments demonstrate the creation of alternative forms of payment methods. One of the recent innovations is payments through electronic wallets and even implanting chips in mobile phones or other devices. The majority of their users consider bank cards the preferred payment method and that is why commercial banks are always implementing new

bile sau alte dispozitive. Cardurile bancare sunt considerate preferata modalitate de plată de majoritatea utilizatorilor acestora şi de aceea băncile comerciale implementează mereu noi tehnologii pentru sporirea securităţii, precum şi pentru reducerea semnificativă a timpului pentru fiecare tranzacţie. Una dintre cele mai populare inovaţii create pentru cardurile bancare este tehnologia contactless, ce se răspândeşte rapid printre toate ţările lumii.

Cardurile bancare pot fi considerate adevăraţi veterani ai sistemului bancar datorită ratei de utilizare a acestora. Miliarde de tranzacţii bancare sunt create zilnic prin aceste bucăţi de plastic; astfel, putem spune ferm că cardurile bancare sunt nişte pioneri în piaţa tranzacţiilor bancare şi acestea nu vor dispărea prea curând de pe scenă plăţilor.

Primul card bancar din Republica Moldova, VISA Classic, a fost emis la 5 iunie 1997 de către Victoria Bank. În România numărul cardurilor aflate în circulaţie ajunge la aproximativ 22 de milioane de unităţi, în Ucraina – circa 25,4 de milioane (la moment activitatea bancară este perturbată din pricina conflictului militar între Rusia şi Ucraina), iar în Rusia numărul cardurilor bancare aflate în circulaţie ajunge la 50,2 milioane de unităţi.

În Republica Moldova, la ora actuală, sunt puse în circulaţie peste 2,3 mln de carduri bancare, cu peste 20 % mai mult decât în anul 2021. În primele 6 luni ale acestui an, deţinătorii de carduri din Republica Moldova au efectuat tranzacţii, fără numerar, în valoare de circa 30 mlrd lei. Datele băncii Naţionale a Moldovei arată că cetăţenii au retras mai puţin bani în numerar de pe card, preferând să facă mai multe achitări online. Reducerea numerarului în circulaţie este o prioritate pentru a scădea cota economiei tenebre, deoarece tranzacţiile devin transparente şi respectiv din ele se percep impozite, iar în consecinţă creşte bugetul ţării. Însă plata fără numerar, care a devenit în ultimii ani (în special pe perioada pandemiei) tot mai utilizată, este însoţită şi de un şir de riscuri, pe care autorităţile, dar şi băncile, depun efort să le combată. Cardul bancar, fiind un portmoneu electronic de acumulare a surselor băneşti, dintotdeauna a fost ţinta doritorilor de a acapara aceste mijloace, deseori obţinând accesul la acest portmoneu cu ajutorul victimei însăşi. Astfel, potrivit datelor BNM, doar în trimestrul

technologies to increase security, as well as to significantly reduce the time for each transaction. One of the most popular innovations created for bank cards is contactless technology, which is rapidly spreading among all countries of the world.

Bank cards can be considered real veterans of the banking system due to their usage rate. Billions of banking transactions are created daily through these pieces of plastic; thus, we can firmly say that bank cards are pioneers in the banking transaction market and they will not disappear from the payment scene anytime soon.

Victoria Bank issued VISA Classic, the first bank card in the Republic of Moldova on June 5, 1997. In Romania, the number of cards in circulation reaches approximately 22 million units, in Ukraine - approximately 25.4 million (at the moment banking activity is disrupted due to the military conflict between Russia and Ukraine), and in Russia the number of bank cards in circulation reaches 50.2 million units.

Nowadays, in the Republic of Moldova over 2.3 million bank cards are in circulation, meaning over 20% more comparatively to the year 2021. During the first 6 months of this year, cardholders from the Republic of Moldova made no cash transactions worth about 30 billion lei. Data from the National Bank of Moldova show that citizens withdrew less cash from the card, preferring to make more payments online. Reducing cash circulation is a priority to diminish the share of the dark economy, because transactions become transparent and taxes are collected from them, and consequently the country's budget increases. But cashless payment, which has become increasingly used during the recent years (especially during the pandemic), is also accompanied by a series of risks, which the authorities, as well as the banks, are trying to combat. The bank card, being an electronic wallet for the accumulation of monetary sources, has always been the target of those wishing to seize these means, often obtaining access to this wallet even with the help of the victim. Thus, according to NBM data, only in the 2nd quarter of 2022, fraudulent operations carried out using payment cards constituted (estimated damage in MDL lei):

2 al anului 2022, operaţiunile frauduloase efectuate cu utilizarea cardurilor de plată au constituit (paguba estimată în lei MLD):

– **Cu utilizarea cardurilor de plată emise în Republica Moldova**

1. Fraude cu carduri contrafăcute – 7 768
2. Fraude cu carduri furate – 1 453
3. Fraude cu utilizarea numărului cardului – 464 246
4. Fraude de tip social engineering – 912 391

În total – 1 385 858 lei.

– Cu utilizarea cardurilor de plată emise în străinătate

1. Fraude cu carduri contrafăcute – 86 831
2. Fraude cu carduri furate – 113 293
3. Fraude cu utilizarea numărului cardului –2 583 278
4. Fraude de tip social engineering – 63 504
5. Alte tipuri de fraude – 34 218

În total – 2 881 124 lei.

Potrivit datelor Direcţiei investigaţii infracţiuni informatice a Inspectoratului Naţional de Investigaţii, în perioada primului semestru al anului 2022 au fost pornite 92 de cauze penale legate de operaţiunile frauduloase efectuate cu utilizarea cardurilor de plată/ datelor cardurilor bancare[2].

În această ordine de idei, în continuare mă voi referi la unele dintre cele mai frecvente modalităţi de clonare a cardurilor bancare, cu sustragerea ulterioară a mijloacelor financiare de pe ele şi de compromitere a bancomatelor în aceleaşi scopuri. De asemenea, voi încerca să nominalizez gama de măsuri de precauţie care ar trebui să fie întreprinse de către deţinătorii cardurilor bancare pentru a evita sustragerile ilegale a mijloacelor băneşti disponibile.

Skimming. Datele cardului sunt informaţiile despre contul clientului, stocate pe un card bancar folosit pentru a iniţia o tranzacţie prin intermediul unui bancomat sau al unui alt aparat de citire a cardului. Datele pot fi stocate sau pe o bandă magnetică, sau pe cipul unui card, sau combinat. Compromiterea datelor cardului se realizează prin orice metodă care permite copierea, interceptarea sau modificarea informaţiilor despre contul clientului. Skimmingul este o categorie specifică a compromiterii datelor cardului, care constă în copierea electronică, ilegală, a datelor cardului bancar în

– **With the use of payment cards issued in the Republic of Moldova**

1. Counterfeit card fraud – 7 768
2. Stolen card fraud – 1 453
3. Fraud using the card number – 464 246
4. Social engineering fraud – 912 391

Totally – 1 385 858 lei.

– With the use of payment cards issued abroad

1. Counterfeit card fraud – 86 831
2. Stolen card fraud – 113 293
3. Fraud using the card number – 2 583 278
4. Social engineering fraud – 63 504
5. Other types of fraud – 34 218

Totally – 2 881 124 lei.

According to the data of the Department of Computer Crime Investigation of the National Inspectorate of Investigations, during the first semester of 2022, 92 criminal cases related to fraudulent operations carried out with the use of payment cards/bank card data were initiated [2].

In the same manner, in the following I will refer to some of the most common ways of cloning bank cards, with the subsequent theft of financial means from them and of ATMs compromising for the same purposes. I will also try to nominate the range of precautions that should be taken by bank card holders to avoid illegal embezzlement of their available funds.

Skimming. Card data means customer account information stored on a bank card used to initiate a transaction via an ATM or other card reader. Data can be stored either on a magnetic stripe, or on a card chip, or a combination. Compromising of card data is achieved by any method that allows copying, interception or modification of customer account information. Skimming is a specific category of card data compromise, which consists of the electronic, illegal copying of bank card data in the process of carrying out an operation with it, such as purchasing goods, paying for services or withdrawing money from an ATM. Bank card skimming is done directly in two places:

a) at ATMs; b) at the payment terminals (or in their close proximity).

ATM skimming. To copy or clone bank

procesul efectuării unei operaţiuni cu acesta, ca de exemplu procurarea mărfurilor, achitarea serviciilor sau extragerea în numerar a banilor din bancomat. Skimmingul cardului bancar se realizează nemijlocit în două locuri:

a) la bancomate; b) la terminalele de plată (sau în imediata lor apropiere).

Skimmingul bancomatelor. Pentru copierea sau clonarea datelor cardurilor bancare infractorii folosesc nişte dispozitive electronice minuscule, numite skimmer, care au capacitatea de a copia datele cardului de pe purtătorii electronici de informaţii. La instalarea skimmerului infractorii folosesc diferite procedee tactice care complică depistarea acestuia. Dispozitivele de skimming ATM sunt instalate atât în exteriorul bancomatului, cât şi în interiorul acestuia (de obicei în interiorul dispozitivului reader card al bancomatului). În unele cazuri interfaţa autentică a bancomatului este eliminată şi înlocuită cu dispozitiv de skimming, dar este posibilă şi montarea dispozitivului de skimming deasupra interfeţei autentice a bancomatului.

Dispozitivele interne de skimming ale cititorului de carduri (cunoscute şi ca dispozitive de deep insert skimming) sunt plasate în diferite poziţii în cadrul portabilului cititorului de carduri. Formele şi dimensiunile reale ale acestor dispozitive sunt foarte mici şi subţiri, concepute pentru a permite cardului să treacă prin sau peste dispozitiv pe măsura ce cardul este introdus şi scos din slotul de intrare a cardului în ATM. Skimmerii de obicei captează ilegal datele şi le păstrează în interiorul bancomatului, acolo unde a fost instalat skimmerul. Or, odată cu dezvoltarea progresului tehnologic, schimmerii tot mai des folosesc pentru transmiterea datelor captate ilegal tehnologia Bluetooth sau Wi-Fi.

Concomitent cu compromiterea informaţiei electronice de pe cardul bancar, infractorii urmăresc scopul capturării şi a codului PIN, deoarece acesta le va permite accesul la contul bancar al victimei. Există diverse dispozitive, metode tehnice şi non tehnice care sunt utilizate pentru a compromite codurile PIN. Cele mai răspândite metode sunt: utilizarea tastaturilor false, camerelor spion ataşate la bancomat sau în mediul lui, supravegherea vizuală personală, instalarea unor software rău intenţionate (Malware).

Tastaturi false – sunt cele care au fost proiectate şi confecţionate (prioritar de

card data, criminals use tiny electronic devices, called skimmers, which have the ability to copy card data from electronic data carriers. During skimmer installing, the criminals use different tactical procedures that complicate its detection. ATM skimming devices are installed both outside and inside the ATM (usually inside the card reader device of the ATM). In some cases, the authentic ATM interface is removed and replaced with a skimming device, but it is also possible to mount the skimming device on top of the authentic ATM interface.

The internal skimming devices of the card reader (also known as deep insert skimming devices) are placed in various positions within the portable card reader. The actual shapes and sizes of these devices are very small and thin, designed to allow the card to pass through or over the device as the card is inserted and removed from the ATM's card entry slot. Skimmers usually illegally capture data and store it inside the ATM where the skimmer has been installed. Alternatively, with the development of technological progress, skimmers increasingly use Bluetooth or Wi-Fi technology to transmit illegally captured data.

Along with compromising the electronic information on the bank card, criminals aim to capture the PIN as well, as it will allow them access to the victim's bank account. There are various devices, technical and non-technical methods that are used to compromise PINs. The most common methods are the following: using fake keyboards, spy cameras attached to the ATM or close to it, personal visual surveillance, installing malicious software (Malware).

Fake keyboards – they are those that have been designed and manufactured (primarily Chinese production) according to the analogy of the original. They are typically installed over the genuine ATM keyboard and record the keystrokes made by the cardholder while mechanically pressing the genuine ATM keys underneath the fake keyboard. After registering and memorizing the PIN code, the fake keypad can be easily peeled off from the original one and later used for repeated criminal purposes.

Spy cameras – they are micro video devices, often very well camouflaged; and are in-

producție chineză) după analogia originalului. Ele sunt în mod obișnuit instalate peste tastatura autentică a ATM-ului și înregistrează apăsările de taste, efectuate de posesorul cardului în timp ce apasă mecanic tastele ATM-ului autentic de sub tastatura falsă. După înregistrarea și memorarea PIN codului, tastatura falsă poate fi ușor dezlipită de pe cea originală și ulterior folosită în scopuri criminale repetate.

Camere spion – sunt aparate video micro, adesea foarte bine camuflate, ele fiind destinate pentru captarea ilegală de imagini, în momentul în care utilizatorul cardului culege codul PIN. Acestea pot fi poziționate oriunde pe ATM (deseori creează impresia că fac parte din fațada ATM-ului), doar să permită un unghi direct de vizibilitate către tastatura ATM-ului. Unele camere transmit imaginile la distanță către un receptor, în timp ce altele le stochează pe medii de stocare locală.

Supravegherea personală constă în monitorizarea vizuală a victimei de către infractor în procesul de culegere a PIN-ului sau atunci când pur și simplu și-l reamintește, citindu-l de pe telefonul mobil sau de pe foaia unde l-a memorat.

Malware sunt softuri rău intenționate (programe virusate), create cu scopul de a forța distribuitorul ATM să livreze numerar (jackpotting) sau să captureze datele de pe cardul bancar și, respectiv, ocazional PIN-ul. Cel mai frecvent, infractorii folosesc programe de tip malware, care pot intercepta și stoca datele cardului bancar cu denumiri convenționale: Skimer-A, Skrooge, Dump Memory Grabber, Macau Malware, Ulssm.exe etc. Metoda de instalare ilegală a programelor malware o mai întâlnim și cu denumirea convențională **Black box[3]**. În practica polițienească se regăsesc mai multe exemple de atacuri malware asupra ATM-urilor și respectiv obținerea controlului deplin asupra acestuia, printre cele mai frecvente fiind:

– Pornirea sau rularea automată folosind un dispozitiv USB sau o unitate CD/ DVD, care instalează malware pe hard disk-ul ATM-ului.

– Pornirea folosind un dispozitiv USB sau un disc CD/DVD, care deja conține un sistem de operare și o aplicație ce permite controlul direct al bancomatului.

– Accesarea desktop-ului Windows și instalarea programei malware pe discul dur ATM din linia de comandă.

tended for the illegal capture of images, when the card user dials the PIN code. They can be positioned anywhere on the ATM (often giving the impression of being part of the ATM facade), just to allow a direct line of sight to the ATM keypad. Some cameras transmit images remotely to a receiver, while others store them on local storage media.

Personal surveillance consists in the visual monitoring of the victim by the criminal in the process of the PIN dial or when he simply remembers it, reading it from the mobile phone or from the sheet where he memorized it.

Malware are malicious software (virus programs), created for the purpose of forcing the ATM dispenser to deliver cash (jackpotting) or capture bank card details and occasionally PIN respectively. Most commonly, criminals use malware programs that can intercept and store bank card data with conventional names: Skimer-A, Skrooge, Dump Memory Grabber, Macau Malware, Ulssm.exe, etc. The method of illegal installation of malware is also known under the conventional name of **Black box [3].** In police practice, there are several examples of malicious attacks on ATMs and obtaining full control over them, among the most frequent being:

– Automatically starting or running using a USB device or CD/DVD driver, which installs malware on the ATM's hard driver.

– Starting using a USB device or CD/DVD disc, which already contains an operating system and an application that allows direct control of the ATM.

– Accessing the Windows desktop and installing the malware on the ATM hard driver from the command line.

– Using a remote maintenance network system to compromise the ATM.

In order to install a malware program in the ATM, physical access (with the exception of network compromise) to the electronic components is needed; respectively for this purpose, the criminals use different methods:

– Physical use of a genuine key (or its copy) to open the ATM case.

– Tampering with the lock of the ATM case.

– Drilling, cutting or melting a hole in the

– Utilizarea unui sistem de reţea de întreţinere la distanţă pentru a compromite ATM-ul.

Pentru a instala un program malware în ATM este nevoie de accesul fizic (cu excepția compromiterii reţelei) la componentele electronice, respectiv în acest scop infractorii folosesc diferite metode:

– Utilizează fizic o cheie autentică (sau copia acesteia) pentru a deschide dulapul ATM-ului.

– Sabotează lacătul dulapului ATM.

– Găurirea, tăierea sau topirea unei găuri în interfaţa dulapului ATM-ului.

– Introducerea dispozitivelor cu programe malware prin slotul cititorului de carduri.

– Simularea identităţii unui tehnician de serviciu pentru a obţine accesul la dulapul ATM-ului.

– Racolarea persoanei care va instala programul malware din rândurile funcţionarilor băncii sau specialiştilor care deservesc sistemul electronic de securitate.

– Pentru a pune în funcţiune programele malware, infractorii deseori utilizează un anumit card ATM, introduc anumite secvenţe de numere pe panoul PIN sau utilizează anumite conexiuni de telefon mobil instalate anterior în ATM.

– Investigarea acestui fel de skimming este deseori dificilă, deoarece unele versiuni ale programelor malware sunt concepute pentru a se şterge automat după o perioadă de timp sau imediat după execuţie.

Cash trapping este o metodă de compromitere a bancomatelor, care constă în plasarea unei plăcuţe metalice lipite deasupra fantei bancomatului, ce blochează eliberarea banilor din bancomat. Nereuşind să aibă acces la bani, victima pleacă în căutarea altui bancomat, în timp ce infractorul scoate placa metalică şi intră în posesia banilor blocaţi în bancomat[4].

Skimmingul la terminalele de plată. Skimmingul cardurilor bancare la terminalele de plată pot avea loc oriunde: la achitarea serviciilor comunale, achitarea mărfurilor procurate în magazine, achitarea prânzului în restaurant, procurarea combustibilului în staţiile Peco, achitarea călătoriei în autobus sau troleibuz. Victime ale acestui fel de skimming sunt clienţii care nu doresc să efectueze plăţi în numerar, folosind carduri bancare. Un amănunt semnificativ al acestui fel de skimming constă în faptul că infractorul poate avea

interface of the ATM case.

– Introduction of malware devices through card reader slot.

– Simulation of a service technician to gain access to the ATM case.

– Recruitment of the person who will install the malware from the ranks of bank officials or specialists servicing the electronic security system.

– To launch malware, criminals often use a specific ATM card, enter specific sequences of numbers on the PIN pad, or use specific mobile phone connections previously installed in the ATM.

– Investigating this kind of skimming is often difficult because some versions of malware are designed to delete themselves automatically after a period of time or immediately after execution.

Cash trapping is a compromising ATMs method, which consists of placing a metal plate, glued over the slot of the ATM, which blocks the release of money from the ATM. Unable to access the money, the victim goes in search of another ATM, while the criminal removes the metal plate and takes possession of the money locked in the ATM [4].

Skimming at payment terminals. Bank card skimming at payment terminals can take place anywhere: during communal services paying, paying for goods during shopping, paying for lunch in a restaurant, buying fuel at Peco stations, paying for bus or trolleybus travel. Victims of this kind of skimming are customers who do not want to make cash payments using bank cards. A significant detail of this kind of skimming consists in the fact that the criminal can have physical access to the customer's bank card, especially when the victim is a gullible person and passes the card to the seller, restaurant or gas station clerk, etc., for the latter to carry out the transaction. In the vast majority of cases, the criminals have, in another pocket, skimming devices (skimmers), with the help of which they copy/clone the electronic data from the victim's bank cards. Taking a photo of the card is also not excluded, obtaining the card number, as well as the CVV and CVV2, which offer the possibility of subsequent payments in the online environment of

acces fizic la cardul bancar al clientului, mai ales când victima este o persoană credulă și transmite cardul vânzătorului, funcționarului restaurantului sau benzinăriei etc., ca ultimul să efectueze tranzacția. În marea majoritate a cazurilor infractorii dețin, în alt buzunar, aparate de skimming (skimmere), cu ajutorul cărora copie/ clonează datele electronice de pe cardurile bancare ale victimei. Nu este exclusă și fotografierea cardului, cu obținerea numărului cardului, dar și a CVV și CVV2 care oferă posibilitatea achitărilor ulterioare în mediul online a serviciilor ți produselor.

Măsuri de prevenire a skimmingului (cum te poți proteja de capcana skimming).

În general se consideră că nu poți observa orice skimmer instalat fie pe panoul ATM-ului, fie în interiorul acestuia, dar cu siguranță înainte de a retrage banii ar trebui să arunci o privire rapidă asupra acestuia. Uneori o examinare în plus a ATM-ului îți poate păstra atât banii, cât și timpul. La retragerea banilor din bancomat sau efectuarea altor operațiuni este necesar de atras atenția:

– Dacă cititorul de cartele se mișcă atunci când încercați sa-l folosiți, probabil că ceva nu e în regulă. Un cititor de carduri ar trebui să fie atașat atât de bine, încât să nu se miște. Un skimmer suprapus se poate mișca în jurul punctului de fixare.

– Cercetați bine ATM-ul, poate ceva nu e în regulă: încercați să observați dacă sunt piese în plus sau instalații de culoare diferită decât interfața bancomatului, poate observați o microcameră foto sau video.

– Examinați minuțios tastatura, nu diferă oare după grosime de tastaturile altor ATM-uri, se mișcă sau nu tastatura bancomatului.

– De fiecare dată protejați codul PIN când îl culegeți pentru a retrage bani în numerar.

– Monitorizați în permanență tranzacțiile contului Dvs., verificați tranzacțiile suspecte și imediat anunțați banca care deservește cardul Dvs.

– Dacă aveți instalată aplicația Web-Banking în telefon (sau alte aplicații de acest gen), monitorizați încontinuu tranzacțiile bancare care se fac de pe contul Dvs.

– Consultați frecvent site-ul băncii Dvs., pentru a cunoaște măsurile de securitate în utilizarea cardului, dar și datele de contact ale băncii.

– Activați serviciul de tip SMS – notifica-

services and products.

Measures to prevent skimming (the way you can protect yourself from the skimming trap).

It is commonly believed that you cannot spot any skimmer installed either on the ATM panel or inside it, but you should definitely take a quick look at it before withdrawing money. Sometimes an extra examination of the ATM can save you both money and time. When withdrawing money from the ATM or performing other operations, attention should be drawn in the following cases:

– If the card reader moves when you try to use it, something is probably wrong. A card reader should be attached in order to be firmly secured. An overlapping skimmer can move around the attachment point.

– Research the ATM well, maybe something is wrong: try to notice if there are extra parts or installations of a different color than the ATM interface, maybe you notice a photo or video micro camera.

– Examine the keyboard carefully, does it differ in thickness from the keyboards of other ATMs, does the ATM keyboard move or not.

– Protect your PIN every time you dial it to withdraw cash.

– Continuously monitor your account transactions, check for suspicious transactions and immediately notify the bank servicing your card.

– If you have the Web-Banking application installed on your phone (or other similar applications), continuously monitor the banking transactions that are made from your account.

– Frequently consult your bank's website, to know the security measures in using the card, as well as the bank's contact details.

– Activate the SMS-notification service, through which you are immediately informed about the transactions made with the bank card.

– If a card transaction fails, promptly check the balance of the account to which the bank card is attached.

– Do not allow the bank card to be photographed or photocopied by unauthorized persons for such actions; in this way you will avoid

re, prin care sunteţi informaţi imediat despre tranzacţiile efectuate cu cardul bancar.

– În cazul eşuării unei tranzacţii cu cardul, verificaţi prompt soldul contului la care este ataşat cardul bancar.

– Nu permiteţi fotografierea sau xerocopierea cardului bancar de către persoane neautorizate pentru astfel de acţiuni, astfel veţi evita furturile de date înscrise pe card, ce pot fi utilizate la efectuarea tranzacţiilor de tip online.

Phishing. În era revoluţiei tehnologice avem multe posibilităţi care ne lărgesc orizonturile de acţiune. Totuşi, pe lângă aspectul pozitiv al tehnologiilor, există şi partea sumbră a lucrurilor. Tot mai des multe persoane cad pradă escrocilor din mediul online. Infractorii de cele mai multe ori folosesc fie numele unor companii recunoscute, fie se dau drept funcţionari ai băncilor pentru a obţine date personale sau ale cardului, această activitate frauduloasă fiind numită în spaţiul public **phishing.** Termenul provine din limba engleză şi se traduce ca pescuit, fiindcă scopul de bază al infractorilor este să ne prindă la „momeala" pe care ei au oferit-o. Cele mai des întâlnite scheme de phishing sunt:

– Apariţia mesajelor pop-up în timpul navigării pe internet, care , de obicei, vă anunţă că sunteţi unul din fericiţii participanţi la o presupusă tombolă şi vă invită să răspundeţi la întrebările unui sondaj. Apoi vi se propune să completaţi nişte câmpuri sau anchete cu indicarea datelor cardului bancar. Drept rezultat, infractorii întră în posesia numărului complet al cardului codului de securitate CVV/CVC şi respectiv obţine acces la portmoneul electronic. Prin analogie li se comunică că au obţinut o donaţie de bani sau pot obţine un credit în condiţii avantajoase şi că este necesar să facă un transfer de bani sau să comunice datele cardului.

– Mesajele parvenite de la adrese electronice necunoscute, care vă îndeamnă să accesaţi un oarecare link. Acest link vă poate redirecţiona pe site-urile clonate/false ale unor companii, bănci, sisteme de plăţi etc., foarte asemănătoare cu platforma de online banking, a paginii sistemei de plăţi sau a unei companii. Totodată aceste linkuri pot conţine viruşi cu ajutorul cărora infractorii au posibilitatea de a obţine controlul asupra informaţiei din telefonul sau calculatorul victimei.

– Contactarea victimelor prin intermediul telefonului mobil, când infractorii se

the theft of data written on the card, which can be used to carry out online transactions.

Phishing. During the age of the technological revolution, we have many possibilities that broaden our horizons of action. However, in addition to the positive side of technologies, there is also the dark side of things. More and more people are falling prey to online scammers. Criminals often use the names of well-known companies or pretend to be bank officials to obtain personal or card data, this fraudulent activity being called **phishing** within public space. The term comes from the English language and translates as fishing, because the basic purpose of the criminals is to catch us at the "bait" that they have provided. The most common phishing schemes are:

– The appearance of pop-up messages while surfing the Internet, usually announcing that you are one of the lucky participants in a supposed raffle and inviting you to answer survey questions. Then you are proposed to fill in some fields or surveys with the indication of the bank card data. As a result, criminals get possession of the full CVV/CVC security code card number and gain access to the e-wallet respectively. By analogy, they are informed that they have obtained a donation of money or can obtain a loan on favorable terms and that it is necessary to make a money transfer or communicate their card details.

– Messages from unknown email addresses that prompt you to click on some link. This link may redirect you to cloned/fake websites of companies, banks, payment systems, etc., very similar to the online banking platform, payment system or company page. At the same time, these links may contain viruses with the help of which criminals have the opportunity to gain control over the information on the victim's phone or computer.

– Contacting victims via mobile phone, when criminals pose as bank employees and through various deception methods obtain the card number as well as the security code. Usually, potential victims are told that there was an attack on the bank's electronic system, and in order to avoid theft from the cards, the security system is changed, and for this, the bank card data of all the bank's customers is needed. In

prezintă drept funcţionari ai băncilor şi prin diferite metode de înşelăciune obţin numărul cardului, precum şi codul de securitate. De obicei potenţialelor victime li se comunică precum că a fost un atac asupra sistemei electronice a băncii şi în scopul evitării sustragerilor de pe carduri se modifică sistema de securitate, iar pentru aceasta este nevoie de datele cardurilor bancare ale tuturor clienţilor băncii. Pentru a oferi un grad de încredere înalt, pe telefonul apelantului se înregistrează Serviciul Clienţi ale anumitei bănci. Această modalitate de înşelăciune este foarte răspândită acum în R. Moldova, fiind specific că infractorii adeseori sunt persoane care în acel moment îşi execută pedeapsa penală în penitenciare pentru alte infracţiuni; aceştia din urmă au de obicei la dispoziţie gadgeturi performante şi destul timp pentru a „prelucra" victima[5].

– Infractorii expediază diferite mesaje prin e-mail, SMS-uri la telefon sau mesaje în privat pe reţelele de socializare, chipurile din partea unei rude sau unui prieten apropiat, care la o adică a nimerit într-o situaţie dificilă şi are nevoie urgent de bani. Iar pentru aceasta este nevoie să facă un transfer de bani pe un oarecare cont sau să comunice datele cardului bancar şi codul de securitate.

Metode de prevenire a atacurilor phishing:

– A nu accesa mesajele pop-up suspecte.

– A nu comunica nimănui rechizitele cardului bancar, codul PIN, codul de securitate sau parola de unică folosinţă recepţionată prin SMS sau e-mail.

– A nu comunica şi nu trimite nimănui datele bancare pentru realizarea transferurilor.

– A evita accesarea linkurilor suspecte aflate în e-mailuri, reţele de socializare, programe de transmitere a mesajelor, mai ales în cazurile când se solicită introducerea datelor personale sau datelor cardului bancar.

– A se asigura că adresa site-ului unde introduceţi datele despre card începe cu **https**: Aceasta înseamnă că conexiunea este protejată, iar datele cardului utilizate în timpul transferului nu pot fi furate.

– A instala un program antivirus licenţiat pe computerul personal, ce ar proteja de programe care colectează parole de la diferite resurse.

– A nu se deschide documentele ataşate la mesajele primite de la adrese necunoscute.

order to provide a high degree of confidence, the Customer Service of a particular bank is registered on the caller's phone. This way of cheating is actually rather widespread in the Republic of Moldova, being specific that the criminals are often people who at that time are serving their criminal sentence in prisons for other crimes; the latter usually have at their disposal powerful gadgets and enough time to "process" the victim [5].

– Criminals send various messages by e-mail, text messages on the phone or private messages on social networks, allegedly from a relative or a close friend, who got in a difficult situation and urgently needs money. In addition, for this they need to make a money transfer to some account or communicate their bank card data and security code.

Methods of preventing phishing attacks:

– Do not access suspicious pop-up messages.

– Do not share bank card details, PIN code, security code or one-time password received by SMS or email with anyone.

– Do not communicate or send bank details to anyone to make transfers.

– Avoid accessing suspicious links in e-mails, social networks, messaging programs, especially in cases where personal data or bank card data are requested.

– Make sure the website address where you enter your card details starts with **https**: This means that the connection is protected and the card data used during the transfer cannot be stolen.

– Install a licensed antivirus program on your personal computer that would protect against programs that collect passwords from various resources.

– Do not open documents attached to messages received from unknown addresses.

– Do not make payments on unknown or dubious sites.

– Do not use bank cards with high balances for online payments. If possible, use separate bank cards for internet payments only.

– Do not leave the bank card visible and do not allow it to be photographed or photocopied by persons who are not authorized for

– A nu se efectua plăți pe site-uri necunoscute sau care par a fi dubioase.

– A nu se folosi pentru plăți online carduri bancare cu solduri mari. Dacă este posibil, a se folosi în acest scop carduri bancare separate, destinate doar plăților prin internet.

– A nu se lăsa cardul bancar la vedere și a nu se permite fotografierea sau xerocopierea acestuia de către persoanele care nu sunt autorizate pentru astfel de acțiuni.

– A se păstra separat de card plicul ce conține datele de autentificare ale cardului (PIN, CVV2, CVC2 etc.).

– Memorarea numărului PIN fără a-l scrie pe card sau pe alt suport.

– Activarea serviciului SMS – notificare prin care vă va informa despre tranzacțiile efectuate cu cardul de plată.

– Dacă se pare ceva suspect, sunați imediat la serviciul clientelă al băncii care deservește cardul, inclusiv cu solicitarea blocării cardului bancar[6].

such actions.

– Keep the envelope containing the card's authentication data (PIN, CVV2, CVC2, etc.) separate from the card.

– Memorizing the PIN number without writing it on the card or other medium.

– Activation of the SMS-notification service that will inform you about the transactions made with the payment card.

– If something seems suspicious, immediately call the customer service of the bank that serves the card, including the request to block the bank card [6].

Referinţe bibliografice

Bibliographical references

1. http://bancamea.md/news/istoria-cardului-bancar-cnd-a-aparut-unde-ce-funcii-indeplinea.
2. Sinteza Direcţiei investigaţii infracţiuni informatice pentru sem.1, anul 2022.
3. htpps://www.mold-street.com. Black box sau cutia neagră, noua metodă de spart bancomate.
4. https://www.poliţia.md. Reţinuţi după ce au furat mai multe bancomate.
5. https://www.poliţia.md. Grup infracţional specializat în sustragerea mijloacelor băneşti de pe carduri bancare.
6. https://www.bnm.md. Recomandări pentru sporirea siguranţei în utilizarea cardului de plată.

Despre autor:
Marian GHERMAN,
doctor în drept, conferenţiar universitar,
şef al Catedrei „Activitate specială
de investigaţii şi anticorupţie"
a Academiei „Ştefan cel Mare" a MAI,
e-mail: liuboi1@rambler.ru
ORCID: 0000-0002-2033-1566

About author:
Marian GHERMAN,
PhD, associate professor,
head of the "Special Investigation
and Anti-Corruption Activity" Chair
of the Academy "Ştefan cel Mare" of the MIA,
e-mail: liuboi1@rambler.ru
ORCID: 0000-0002-2033-1566