Piotr Milik*
Grzegorz Pilarski**

Cyberattacks and the bank's liability for unauthorized payment transactions in the online banking system – theory and practice

Abstract

The article discusses the matter of contemporary cyberattack techniques aimed at the financial security of banks and their clients and presents the relationship of banks with their clients in the light of the applicable provisions of the European Union (Directive of the European Parliament and the EU Council 2015/2366 of November 25, 2015 on payment services in internal market) and the Polish Act of 19 August 2011 on payment services. The authors also analyze the practical side of the relationship between banks and their customers who have fallen victim to computer fraud, pointing out that the common practice of banks refusing to return funds stolen from their customers in the electronic banking system is inconsistent with the applicable standards of Polish and European law.

Key words: cyberattack, financial security, electronic banking system, computer fraud, European Union

* Assoc. Prof. Piotr Milik, PhD, War Studies University in Warsaw, e-mail: p.milik@akademia.mil.pl, ORCID: 0000-0002-1204-4882.
** Assoc. Prof. Grzegorz Pilarski, PhD, War Studies University in Warsaw, e-mail: g.pilarski@akademia.mil.pl, ORCID: 0000-0001-9728-2611.

Introduction

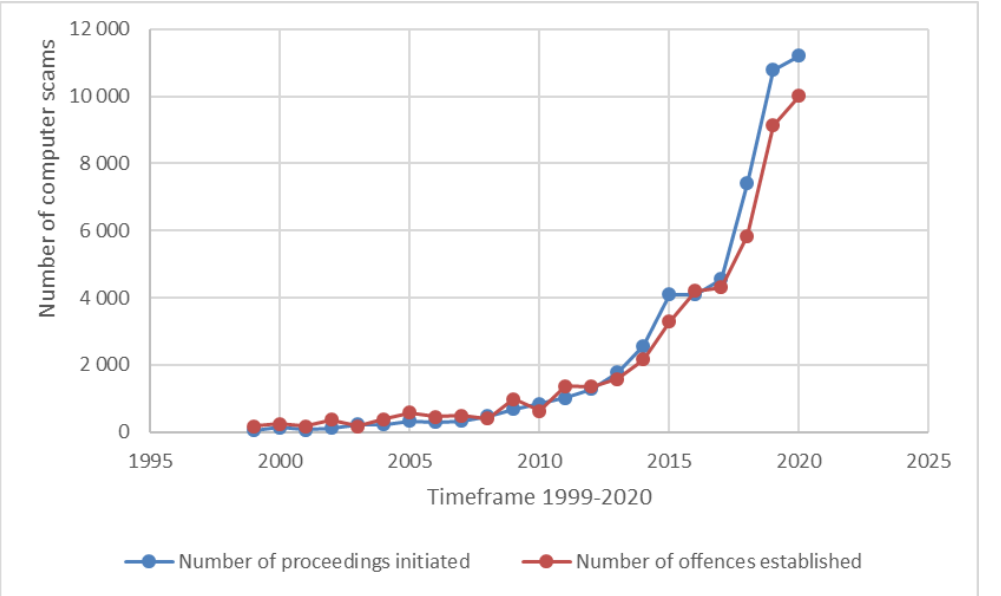
Internet banking dates back to the beginning of the 1990s. It was started in the United States of America, where the first transactions in cyberspace were carried out via the still fledgling Internet. Nowadays, all financial institutions, including banks, provide their clients with special systems, thanks to which they can perform financial operations without leaving home, only with the use of a home computer or personal smartphone.

Today's cyberspace is a global network consisting of interconnected ICT systems built of devices that enable the creation, processing and exchange the information automatically between devices or consciously and intentionally between their users. Cyberspace defined in this way (constituting a zone of everyday activity of states and their citizens, in which the interests of these entities are pursued) is constantly threatened in the first place by illegal activities of persons and criminal groups, including terrorist groups, and then also as a result of errors or failure of individual ICT systems.

The COVID-19 pandemic that the world collided with in 2020 has accelerated the computerization of public and private services. The information (digital) revolution that we have witnessed in recent decades has accelerated. The life and professional activity of developed societies has largely moved to cyberspace. Common education, academic lectures, banking operations, purchases of all kinds of goods and services, communication with public institutions almost overnight moved to the Internet. Developed societies have undergone an accelerated course in the use of new information technologies. Unfortunately, the rapid pace of these changes resulted in an intensified wave of abuse. Cybercrime has flourished as digital online operations intensify. The issue of cybersecurity has become more important and topical than ever before.

The Scale of Unauthorized Payment Transactions

The years of the COVID-19 pandemic, in addition to technological development and the growing role of the Internet in modern society, contributed to the increase in committing computer frauds enshrined in Art. 287 of the Polish Criminal Code. Figure 1 below presents statistical data relating to this type of crime.



Source: own study based on data from the website https://statystyka.policja.pl [access: 15.10.2022].

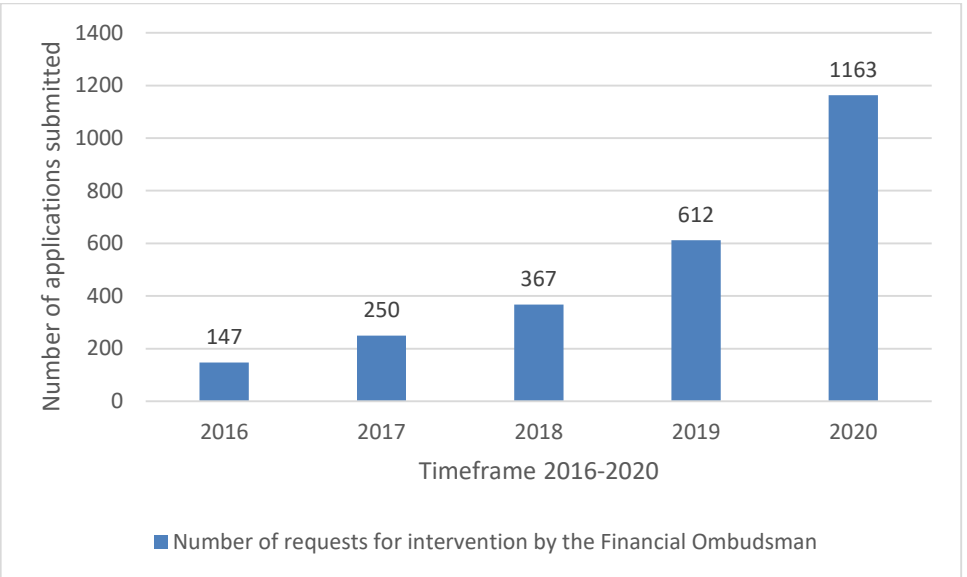
Figure 1. The number of computer frauds under art. 287 CC in the years 1999–2020

Based on the above data, it can be clearly stated that the number of computer frauds has almost doubled since 2019. These crimes relate to various spheres of the functioning of society. One of them is finance, which can be seen from the increase in unauthorized payment transactions over the past few years. This type of transaction is not defined by law, however, pursuant to the PSD2 directive[1], Art. 64 (sec. 1), an authorized transaction is considered a payment transaction only if the payer grants consent to execute this payment transaction (the transaction authorization may be performed before or after the execution of the payment transaction), and in the event of disagreement, the payment transaction is considered as unauthorized (sec. 2). Moreover, in Art. 74 (sec. 3) there is a provision stating that „the payer shall not bear any financial consequences resulting from the use of a lost, stolen or misappropriated payment instrument, unless he acted with dishonest intentions". The condition for such a state to occur is notification by the payer

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC, Official Journal of the European Union 2015, L 337/35.

in accordance with Art. 69 (sec. 1b) of the loss, theft, misappropriation or unauthorized use of a payment instrument. The guidelines of the European Banking Authority (EBA) indicate that an unauthorized transaction is one that was performed without the consent of the payer. In this case, the payment instrument can be either a credit card or a banking application enabling access to a bank account. These provisions show that an unauthorized transaction may also be an authenticated transaction, but made without the consent of the payer.

Based on the data posted on the Polish Financial Ombudsman's website, an upward trend of this phenomenon can be observed in the form of the number of submitted applications for the intervention of the Financial Ombudsman, which is illustrated in Figure 2.



Source: own study based on data from the website https://rf.gov.pl [access: 15.10.2022].

Figure 2. Number of submitted applications for the intervention of the financial ombudsman in disputes regarding unauthorized transactions in 2016–2020

Quantitative data clearly indicate an upward trend in the problem of unauthorized transactions on the financial market. This is related to two main points. The first relates to committing computer crimes related to the making of unauthorized financial transactions, and the second to the actions of banks in this regard, i.e. not reimbursing clients for losses incurred despite the existence of such a statutory obligation. Banks indicate the provisions

of the Payment Services Act as the basis for the refusal, where in Art. 46 indicates the fault of the payer of an unauthorized payment transaction as a result of intentional or grossly negligent breach of his obligations. According to experts, as a result of the development of e-services such as e-commerce[2], m-banking[3], e-banking[4], and open banking[5], one should expect an increase in computer fraud in the form of unauthorized payment transactions.

Threats of an Unauthorized Payment Transaction

In this part of the article, the authors present examples of threats for the payer that may result in an unauthorized transaction. Payment fraud can occur in the transaction system as a result of threats such as[6]: 1) social engineering and phishing activities; 2) malicious programs (malware); 3) APT (Advance Persistent Treats); 4) denial of access DDoS (Denial Distribution of Service); 5) botnets; 6) other threats.

In terms of payment crimes, the above threats may affect specific transaction processes[7], which is presented in the table below (Table 1).

You should be aware that this is only a demonstrative assignment of threats that may arise with high probability in the implementation of specific transaction operations. The first group of threats concerns the attack vector directed not at the technologies used, but at the human who uses them. Social engineering are specific activities that use human error to achieve the intended benefits. In the field of social engineering, attackers use various techniques to try to influence the opinion of the attacked person and make them disclose, for example, confidential information.

2 E-commerce – electronic commerce, a type of commerce that enables the conclusion of commercial transactions using the Internet.

3 M-banking – a financial service enabling access to a payment instrument via mobile devices with Internet access.

4 E-banking – a financial service enabling access to a payment instrument through: computer, ATM, POS terminal, mobile phone, telecommunications line and the Internet. This service enables the implementation of transactional banking.

5 Open banking – a new standard of payment services, in which financial service providers are required to provide third parties with the so-called TPP (Third Party Providers) access to payers' accounts through the so-called API (Application Programming Interface) in accordance with the EU directive PSD2.

6 *2021 Payment Threats and Fraud Trends Report*, Brussels 2021, p. 3.

7 Ibidem, p. 19.

Table 1. Impact of financial payment threats on transaction-related processes

Selected transaction processes	Social engineering	Malware	APT	DDoS
On-boarding/ Provisioning	X	X		
Invoicing/payment request	X	X		
Initialization/ Authentication	X	X		
Payment processing	X	X	X	X

Source: *2021 Payment Threats and Fraud Trends Report*..., p. 19.

In terms of techniques used for the needs of a social engineering attack, the following activities can be distinguished: 1) online baiting – a form of a social engineering attack consisting in „luring" a potential victim through a properly prepared online advertisement that contains a link to initiate the installation of malware in the operating system; an example may be encouraging to take advantage of the opportunity to open a favorable term deposit with a high interest rate well above what the banks actually guarantee on the market; 2) phishing – a social engineering technique consisting in sending messages using e-mail containing content encouraging to click on a link included in the message; an example may be a message from a bank describing that the user's account has been compromised by breaking the password and in order to confirm this situation, it is recommended to log into the account via a link included in the message, which directs to a crafted bank's website that is confusingly similar to the real page, in order to obtain authentication data i.e. login and password; attacks of this type can be divided into spear phishing, whaling and CEO fraud – these are personalized attacks that also impersonate employees of the organization in which the victim works, including e.g. the CEO (General Manager); 3) vishing and smishing – these are social engineering techniques that are used respectively by an initiated telephone conversation or a properly prepared SMS; an example message and conversation may concern a situation in which the bank or a person from the bank provides information that the payer's account will be deactivated and to avoid this, log in to your account via a link (referral to a fake bank's website) or provide login details; 4) online enticement – a technique that uses advertisements on the Internet, which are characterized by the fact that they offer too favorable conditions than it could be in reality, e.g. a reduction in the

purchase of computer equipment at the level of 80% of the market price or a false offer of „click credit", etc.; 5) romance scam – in this technique we deal with a criminal assuming a false internet identity in order to gain the trust and sympathy of a potential victim of fraud, manipulation or robbery of the victim. This is possible by creating the illusion of a close relationship; in 2021, social engineering attacks using this technique were among the most financially harmful cyberattacks[8]; 6) spoofing – a social engineering attack technique in which the attacker impersonates an organization or financial entity, creates a counterfeit domain of a real company to provide WWW and e-mail services that are used to obtain the payer's confidential data; 7) pretexting – this is a technique that enables the preparation of an appropriate social engineering attack and consists in creating a context in the form of a hypothetical story, which is used by an employee of e.g. a bank to obtain confidential information, forging is carried out usually by phone call.

The second group of threats concerns the use of malicious programs (malware). It is assumed that any type of malware is designed to harm an IT system or steal data[9]. The use of malware is one of the biggest threats to cybersecurity today. This type of threat is currently used for a wide range of activities, in which we can distinguish among others: gaining remote access to information systems; damage or deactivation of computers or information systems; spying, modifying, damaging or intercepting data without the user's consent[10]. These and other malicious actions are possible to implement thanks to various types of malicious programs, which include: viruses, worms, trojans, exploits, etc. In terms of the occurrence of unauthorized payment transactions, one of the most dangerous and effective actions can be carried out using trojans. A software called a trojan horse, a trojan is a type of software disguising itself as useful or interesting applications that, when launched by the user, may allow criminals to perform undesirable activities such as: spying

8 *FBI: 6,9 miliarda dolarów – tyle w 2021 roku utracono z powodu przestępstw internetowych*, CyberDefence24, Warszawa 2022, https://cyberdefence24.pl/cyberbezpieczenstwo/fbi-69-miliarda-dolarow-tyle-w-2021-roku-utracono-z-powodu-przestepstw-internetowych [access: 5.09.2022].

9 J. Janczak, G. Pilarski, B. Biernacik, *Technologia informacyjna w zarządzaniu*, Warszawa 2009, p. 171.

10 J. Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015, p. 93.

and stealing confidential user data (spyware[11]); installing backdoor software[12] that allows access to the system bypassing security measures, for example, to send spam or carry out DDoS attacks; deletion, modification and encryption of data, e.g. ransomware[13].

Another group of threats concerns APT (Advanced Persistent Threat) attacks, which means:

– Advanced – attackers use various techniques and methods to effectively breach security, use known vulnerabilities and also look for new vulnerabilities to carry out a given attack;

– Persistent (prolonged, persistent, stubborn) – the attack is to be effective, performed in such a way that it does not attract anyone's attention, and after gaining access to one victim's system, the purpose of the attack is to extend the control to other systems in a way that allows long-term and constant presence and supervision;

– Threat – because the attacker is an organized group with the appropriate technical background and budget. The threat remains constant as long as the attacker has the (political, economic) incentive to steal the victim's information[14].

These types of attacks can target a specific person, company, organization, institution or state. Attackers use highly personalized tools (exploits, viruses, worms, rootkits, zero-day vulnerabilities) and hacking techniques often developed for a specific attack. Attacks of this type may be directed at financial institutions in order to hack into payment networks or systems with the intention, for example, to execute unauthorized payment transactions and steal means of payment.

The next group of threats concerns DDoS access denial attacks and the use of botnets. DDoS is a tool used to damage or prevent the correct operation of the victim's ICT infrastructure. These activities may contribute to the loss of reputation of financial institutions or hinder customer service. DDoS attacks are performed by many, sometimes hundreds of thousands

11 Spyware – designed to collect information about the user, as well as send it to third parties without the user's knowledge.

12 Backdoor – A security or software vulnerability created intentionally by the software developer that could allow access to the user's operating system bypassing security systems.

13 Ransomware – a type of malware that can steal and encrypt user data in order to obtain a ransom for unlocking data or not disclosing it.

14 See G. Pilarski, *Cyberprzestrzeń – relacje w wojnie hybrydowej*, Warszawa 2020, p. 69–73.

of devices connected to each other in the so-called botnet network. Botnets are a collection of devices connected to the Internet that were previously attacked by criminals in order to take control over them without the victim's knowledge. The purpose of these attacks is to enable DDoS, spam or ransomware campaigns. In recent years, this type of activity has become more and more popular among cybercriminals, an example of which is the Emotet botnet, which in 2021 contributed to malware infection of 19% of companies around the world[15].

Other threats that may constitute transaction frauds include all kinds of activities aimed at obtaining data enabling the use of e-banking services, in particular the use of payment instruments in the form of credit and debit cards. In order to obtain data enabling the execution of electronic transactions, criminals use various methods, including: 1) installation of additional illegal devices in ATMs: card reader (skimming – enables reading data from the magnetic stripe of the card); keyboard overlays (fake keyboard – allows you to register PIN codes entered for cards); hidden cameras (hidden cameras – allow you to record the payment process, which allows you to obtain a PIN, card number and CVV/CVC codes); card trapping mechanism – allows the card to be retained when it is introduced to an ATM in order to obtain it after the payer leaves, false fronts (placed on ATMs in order to obtain credentials); 2) the use of public wi-fi networks and fake applications – using these tools, cybercriminals can collect confidential user data, including data enabling authentication in transaction systems; 3) use of false documents – fraudsters using stolen personal data, obtained from forms, applications, etc., that have been lost, stolen or thrown away, produce new cards or other payment instruments that enable payment transactions to be made without the payer's knowledge.

The authors are aware that the above catalog of threats is not a complete catalog and presents selected examples, moreover, it should be taken into account that new methods and techniques are emerging that are used by criminals in the field of payment fraud, which may lead to unauthorized payment transactions.

15 M. Duszczyk, *Powraca najbardziej niszczycielski cyberwirus. Firmy mają powody do obaw*, „Rzeczpospolita", 23.11.2021, https://firma.rp.pl/biznes/art19126551-powraca-najbardziej-niszczycielski-cyberwirus-firmy-maja-powody-do-obaw-emotet-cyberwirus_IT [access: 10.09.2022].

One of the most important measures to be applied in the field of payment fraud prevention is increasing security awareness among various stakeholders in the payment system.

Examples of initiatives in this area were presented by the Polish Financial Ombudsman (FO) in his report on unauthorized payment transactions[16], where he described the procedure to be followed after identifying irregularities by the payer. According to FO, the following actions should be taken:

1. After discovering a transaction fraud, you should immediately notify: your bank, the CERT.PL team (incydent.cert.pl), the nearest police unit (reporting and obtaining a certificate of committing a crime).

2. Filing a financial claim with your bank for the reimbursement of lost funds.

3. If the bank does not respond within D + 1, a complaint should be submitted, which should be processed within 15 working days.

4. If the bank proves that: a) the transaction was made by an authenticated person trying to defraud the bank, b) the payer breached its obligations intentionally or as a result of gross negligence[17], c) the payer will be required to return previously declared financial claims.

5. In the event of a dispute with a bank, an application for intervention may be submitted to the Financial Ombudsman or the Consumer Ombudsman.

In terms of recommendations addressed to both the payment service provider and the payer, an important element of security are guidelines and recommendations developed by the Polish Financial Supervision Authority[18].

16 *Nieautoryzowane transakcje – zasady i główne problemy*, Warszawa, 18 czerwca 2019, p. 13, https://rf.gov.pl/wp-content/uploads/2020/05/Nieautoryzowane_trasnsakcje_analiza-RF_2019.pdf [access: 5.09.2022].

17 Pursuant to Art. 42 of the Act on Payment Services, the obligations of the payer include: using the payment instrument in accordance with the principles set out in the contract; promptly reporting the loss, theft, misappropriation or unauthorized use of a payment instrument or unauthorized access to it; taking the necessary measures to prevent the violation of individual security features of this instrument, in particular, is obliged to store the payment instrument with due diligence and not to disclose it to unauthorized persons.

18 Interesting documents in this regard include: *Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe*, Warszawa 2015, https://www.knf.gov.pl/knf/pl/komponenty/img/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_43526.pdf [access: 12.08.2022]; *Rekomendacje dotyczące bezpieczeństwa płatności internetowych*, Frankfurt n. Menem 2013; *Ostrzeżenie przed dopuszczaniem pośredników do rachunku bankowego w płatnościach internetowych*, Warszawa 2016, https://www.knf.gov.pl/knf/pl/komponenty/img/ostrzezenie_posrednicy_platnosci_60551.pdf [access: 10.09.2022]; K. Leżoń, *Otwarta bankowość w świetle wymogów*

The role of the payer in increasing the level of security of payment transactions is, first of all, to properly ensure the security of the payment instrument and to use the latest solutions and technologies recommended by the payment service provider of the transaction system. One of the user's actions is taking care not to provide access to data that enables authentication (login and password); use of strong passwords with a minimum length of more than 15 characters; use of two-factor authentication mechanisms; reporting irregularities in payment services to relevant authorities; use of payment solutions without the need to use payment cards (non-cash payments, withdrawals and deposits at ATMs).

Banks' Reactions to Unauthorized Payment Transactions

Under Polish law, the basic document defining the rules for the provision of payment services, as well as the scope of the providers' liability for the performance of payment services, is the Act of August 19, 2011 on payment services (consolidated text, Journal of Laws 2019, item 659) – Payment Services Act.

The solutions included in the Payment Services Act were aimed at standardizing the method of providing payment services and regulating the activity of providing payment services in such a way as to ensure the harmonization of the provision of these services throughout the European Union. The Act implemented Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market and amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (PSD directive), which is the so-called directive full harmonization.

The new Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC.

In the above-mentioned, current EU directive we can read (rule 71) that in the case of an unauthorized payment transaction, the payment service provider should immediately return the amount of this transaction to the payer,

dyrektywy PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech, Warszawa 2019.

unless there is a high probability of an unauthorized transaction resulting from fraudulent actions of the payment service user and this suspicion based on the objective grounds notified to the relevant national authority. In this case, the payment service provider should carry out an investigation within a reasonable period of time before making a refund to the payer. In order to encourage the payment service user to report to his payment service provider without undue delay on any theft or loss of the payment instrument, and thus to reduce the risk of unauthorized payment transactions, the user should only be liable up to a very limited amount, unless that user has acted fraudulently intentions or has been guilty of gross negligence in doing so. In this context, an amount of EUR 50 appears to be adequate to ensure a harmonized and high level of user protection in the European Union. The payer should not be held liable if he or she could not have been aware of the loss, theft or misappropriation of the payment instrument. Moreover, from the moment the user reports to the payment service provider that there may have been an unauthorized use of his payment instrument, the payment service user should not be required to bear any further losses resulting from the unauthorized use of that instrument. The aforementioned provision of the EU Directive establishes a general principle of the liability of a bank (payment service provider) for unauthorized payment transactions. In such a situation, the bank should immediately return the amount of this transaction to the payer (bank customer). In other words, the European legislator formulates a postulate that the money credited to the client's bank account belongs to the bank and not to the client, and therefore the potential theft of funds from the client's account is actually detrimental to the bank. An exception has been formulated from this rule, concerning a situation where a bank's client acts knowingly to the detriment of the bank or commits gross negligence in using a payment card or access codes to an internet account.

The above-mentioned principles are implemented into Polish law by the above-mentioned Act of 19 August 2011 on payment services (Payment Services Act).

Unfortunately, despite the clear and precise provisions of the EU Directive and the Polish Payment Services Act, banks, as providers of electronic services, do not comply with their provisions. Banks, after receiving a complaint from their client indicating the occurrence of an unauthorized payment operation (theft of funds over the Internet from the client's bank account), each time refuse to return the stolen money to the client's account. A negative response to the complaint is a standard among financial institutions in Poland. In

response to the complaints, the banks refer to Art. 46 sec. 3 of the Act of 19 August 2011 on Payment Services, which states that „The Payer is responsible for the full amount of unauthorized payment transactions if he caused them intentionally or as a result of intentional or grossly negligent breach of at least one of the obligations referred to in Art. 42". At the same time, they indicate that the customer's behavior, such as clicking on a link pointing to a fake bank website and providing authorization data there, is a grossly negligent act.

In the situation described above, there are several scenarios of the bank's customer behavior and several possible reactions from the bank itself.

Firstly, customers let go of the further battle with the bank after receiving a negative response to the complaint. Then the illegal behavior of the bank has no consequences for it. Despite the lack of detailed data, it can be assumed that this is the case of the vast majority of reactions from bank customers who do not believe in effective pursuit of their claims against the bank, and do not know the applicable law in this regard.

Secondly, some bank customers attempt to act independently and submit a complaint to the Polish Financial Ombudsman, acting pursuant to the Act of 5 August 2015 on Complaints Handling by Financial Market Entities and on the Financial Ombudsman. This extends the entire client's recovery process and does not have the direct effect of returning stolen funds to the client. The ombudsman may, at best, issue an opinion favorable to the client on the matter, which may be brought before the court, if the client decides to sue the financial institution.

Thirdly, as it seems, the least numerous group of defrauded bank customers report to a professional representative – an attorney or legal advisor, requesting legal assistance immediately after the theft. This is undoubtedly the most effective method of pursuing claims against banks, because professional representatives are perfectly familiar with the applicable regulations and procedures and can effectively enter into relationships with banks on behalf of defrauded clients.

Professional representatives send requests for payment to the banks, in which they ask banks to fulfill their statutory obligations and return the money stolen from their online accounts to customers, informing at the same time that in the absence of a positive reaction, the case will be referred to a common court. In such a situation, banks proceed three ways to behave. First, immediately upon receipt of a payment order signed by a professional representative, they return the stolen money to the customers in full. Such

a situation takes place when the stolen sums are not too large, it can be assumed that they reach several thousand złotych.

In the case of higher amounts, the banks address the client directly, bypassing the professional representative, with a proposal to conclude a settlement in which the bank undertakes to return the entire sum of money stolen from the client, and the client undertakes not to disclose the content of the settlement to third parties, including his professional representatives. In the indicated situation, the customer will receive a cash refund, but will not be able to publicly inform about it, e.g. via social media, under the penalty of canceling the settlement and taking the money back. The bank returns the stolen money and gains a guarantee that the rest of its current and potential customers, including deceived customers, will not find out that such a procedure exists, thus the bank will be able to continue to refuse to return money to customers robbed via the Internet with impunity.

Finally, there is also a way for banks to delay and wait for the client to successfully file a lawsuit, which involves the client's costs of legal representation and other costs of the trial, including a court fee in the amount of 5% of the value of the dispute (stolen money). For some clients, court costs may constitute a significant barrier in deciding to engage in a court battle, the outcome of which no one can guarantee to the client. However, even when the lawsuit is successfully filed, the bank may conclude a settlement with the client and agree to return the stolen money without waiting for a court judgment unfavorable to the bank.

Statement of the Financial Ombudsman

Pursuant to the interpretation of the provisions of the Act of 19 August 2011 on Payment Services, consistently presented by the Polish Financial Ombudsman, banks should, pursuant to Art. 46 sec. 1 of the cited act, first return their clients money they lost as a result of unauthorized transactions, and only then, if they claim that there has been gross negligence on the part of their clients, to demand the return of the funds paid out in court. Then the burden of proof and the costs of initiating court proceedings rest with the banks initiating the proceedings, and the court decides about the actual gross negligence of their clients.

In the opinion of the Polish Financial Ombudsman, as a result of the implementation of the PSD2 directive, Art. 46 of the Payment Services Act,

results in significant changes to the procedure to be followed in the case of unauthorized payment transactions. Until 20 June 2018, in the event of an unauthorized payment transaction, the payer's provider was obliged to immediately return the amount of the unauthorized payment transaction to the payer, and, if the payer uses the payment account, restore the debited payment account to the state that would exist if the unauthorized transaction had not taken place. According to the new wording of Art. 46 sec. 1 of the cited act, in the event of an unauthorized payment transaction, the payer's supplier shall promptly, but not later than by the end of the business day following the day when the unauthorized transaction has been debited from the payer's account has occurred, or after receiving the relevant notification, returns the amount of the unauthorized payment transaction to the payer – with except when the payer's supplier has reasonable and duly documented grounds to suspect fraud and informs the law enforcement authorities of this in writing. Where the payer is using the payment account, the payer's provider shall restore the debited payment account to the state that would have existed if the unauthorized payment transaction not taken place. In the opinion of the Financial Ombudsman, this change is of paramount importance for the procedure to be followed in the event of an unauthorized payment transaction. In the opinion of the Financial Ombudsman, according to the current legal status, in the event of an unauthorized transaction, there are several basic rules. Rule 1: obligation to return funds to the client unconditionally; rule 2: obligation to refund the amount of the unauthorized transaction by D + 1; rule 3: establishing the rules of the payer's possible liability for an unauthorized transaction only after the funds have been returned.

From the provision of Art. 46 sec. 1 of the Payment Services Act, after the amendment, it results primarily that the national legislator, following the EU legislator, introduced the obligation to unconditionally return the amount of an unauthorized transaction to the payer by supplier.

The supplier should refund the amount of the unauthorized transaction immediately, and at the latest on the next business day after the notification or detection of unauthorized transaction. As we can see, the EU legislator decided to introduce very short deadline for the supplier to return the amount of the unauthorized transaction payment, while imposing on him an obligation to adopt such internal procedures that will allow him to be carried out within a reasonable time investigating whether there has been any fraudulent activity in a given case the payment service user himself.

In the opinion of the Financial Ombudsman, there is a rule, unconditional obligation to return funds from an unauthorized payment transaction by the provider, as soon as it is detected or found, and only after this return has been made the principles of possible joint liability of the payer for an unauthorized payment transaction. Establishing this joint liability is related to the factual and legal assessment of certain events, hence, in the opinion of the Financial Ombudsman, it should take place in the course of court proceedings.

In the opinion of the Financial Ombudsman, there are only two exceptions to the unconditional rule to return the funds to the customer. First, the documented suspicion of fraud and notification of law enforcement agencies. Secondly, the client's failure to meet the deadline reporting of an unauthorized transaction.

At this point, it should be noted that the evaluation of evidence in the Polish legal system has been assigned to common courts, hence payment service providers who are interested in a positive outcome for them in accordance with the principle „Nemo iudex in causa sua" cannot be judges in their own case[19].

Bank Account Agreement as an Irregular Deposit

In addition, it should be noted that the customer and the bank are bound by a bank account agreement. Pursuant to Art. 725 of the Polish Civil Code, by a bank account agreement, the bank undertakes to keep the account holder for a fixed or indefinite period of time and, if the agreement so provides, to carry out cash settlements at his request. At this point, it should be clarified that the conclusion of a bank account agreement causes the holder's funds to become the property of the bank. Despite the lack of unambiguous wording in certain provisions of the act, there is a common and generally uncontroversial view in doctrine and jurisprudence that the bank obtains ownership of the deposited funds. As indicated, among others, by The Court of Appeal in Kraków in its judgment of February 5, 2014, file ref. (LEX no. 1 540 886), the bank account agreement is based on the structure of the irregular deposit (Art. 845 of the Polish Civil Code), which means that the bank acquires ownership of the funds contributed, and the bank account holder acquires a claim for the return of the amount resulting from provisions of the agreement linking the customer

19 See *Nieautoryzowane transakcje...*

with the bank. Thus, any operations performed on the bank account against the will of the account holder do not charge the account holder, but only the bank. Therefore, despite the fact that an unauthorized person extorts the property owned by the bank, there will be no damage to the account holder, as the bank will still be obliged to fully satisfy its claims from its own funds. The protection of claims is guaranteed to the holder by the provisions of civil and financial law and the agreement with the bank based on them (see the decision of the Supreme Court of April 28, 2016, file ref. (Legalis no. 1 442 847).

It should also be stated that the risk of making a withdrawal from a bank account to an unauthorized person and making a cash settlement on the basis of an instruction issued by an unauthorized person is borne by the bank, also when the bank account agreement is covered by internet banking (cf. judgment of the Court of Appeal in Warsaw of 19 July 2018 (LEX no. 1 822 123). The basis of the bank's liability in this respect are the legal norms contained in the Act of 19 August 2011 on payment services.

In view of the above, customers' demands for banks to fulfill their statutory obligations under Art. 46 sec. 1 of the Act of 19 August 2011 on Payment Services, i.e. the full refund of the unauthorized payment transaction amount, is fully justified.

Summary

Based on the research on payment frauds, it can be concluded that one of the biggest threats are social engineering and phishing attacks, often combined with the use of malicious software. User awareness campaigns are one of the most important remedial mechanisms against social engineering and phishing attacks that should be carried out by payment system institutions. Attacks using malicious software, and in particular ransomware, are becoming a more and more serious problem, which requires the use of new preventive actions and the use of measures to mitigate the effects of such attacks[20]. Preventing fraud in the payment system is not only a matter of indicating the payers' fault, but above all an institutional responsibility, where payment

20 Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating counterfeiting and fraud related to non-cash means of payment, replacing Council Framework Decision 2001/413/JHA, Official Journal of the European Union 2019, L 123/18, Art. 17, prevention.

service providers should notice threats and possible emerging effects of their occurrence, which forces investing in appropriate security and monitoring technologies, as well as raising awareness of potential victims users.

The phenomenon of frauds related to non-cash means of payment is nowadays a significant threat to the security of the state and the security of the international environment, because frauds committed in the payment system are a source of income for actors of organized crime in supporting their activities in the field of terrorism, illegal drug and weapons trafficking, human trafficking and also APT type activities.

The weakest actors in the circumstances described above are individual citizens, individual clients of financial institutions, who become victims of computer crimes and often lose their life savings. Unfortunately, the conducted analyzes show that despite the existence of clear legal regulations protecting individual clients against the negative consequences of fraud carried out via computer networks, banks try to protect their own interests in the first place by transferring the negative effects of computer crimes to individual clients.

Bibliography

Duszczyk M., *Powraca najbardziej niszczycielski cyberwirus. Firmy mają powody do obaw*, „Rzeczpospolita" 2021, https://firma.rp.pl/biznes/art19126551-powraca-najbardziej-niszczycielski-cyberwirus-firmy-maja-powody-do-obaw-emotet-cyberwirus_IT [access: 10.09.2022].

2021 Payment Threats and Fraud Trends Report, Brussels 2021.

FBI: 6,9 miliarda dolarów – tyle w 2021 roku utracono z powodu przestępstw internetowych, CyberDefence24, Warszawa 2022, https://cyberdefence24.pl/cyberbezpieczenstwo/fbi-69-miliarda-dolarow-tyle-w-2021-roku-utracono-z-powodu-przestepstw-internetowych [access: 5.09.2022].

Final report. Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2), 2018, https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2281937/5653b876-90c9-476f-9f44-507f5f3e0a1e/Final%20report%20on%20Guidelines%20on%20fraud%20reporting%20under%20Article%2096%286%29%20PSD2%20%28EBA-GL-2018-05%29.pdf?retry=1 [access: 5.09.2022].

Janczak J., Pilarski G., Biernacik B., *Technologia informacyjna w zarządzaniu*, Warszawa 2009.

Komunikat ws. stosowania wyłączenia z art. 6 pkt 11 ustawy o usługach płatniczych (aktualizacja), Warszawa, 1 czerwca 2022, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_ws_stosowania_wylaczenia_z_art_6_pkt_11_ustawy_o_uslugach_platniczych.pdf [access: 5.09.2022].

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Leżoń K., *Otwarta bankowość w świetle wymogów dyrektywy PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech*, Warszawa 2019.

Nieautoryzowane transakcje – zasady i główne problemy, Warszawa, 18 czerwca 2019, https://rf.gov.pl/wp-content/uploads/2020/05/Nieautoryzowane_trasnsakcje_analiza-RF_2019.pdf [access: 5.09.2022].

Ostrzeżenie przed dopuszczaniem pośredników do rachunku bankowego w płatnościach internetowych, Warszawa 2016, https://www.knf.gov.pl/knf/pl/komponenty/img/ostrzezenie_posrednicy_platnosci_60551.pdf [access: 10.09.2022].

Pilarski G., *Cyberprzestrzeń – relacje w wojnie hybrydowej*, Warszawa 2020.

Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe, Warszawa 2015, https://www.knf.gov.pl/knf/pl/komponenty/img/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_43526.pdf [access: 12.08.2022].

Rekomendacja dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, Warszawa 2013.

Rekomendacje dotyczące bezpieczeństwa płatności internetowych, Frankfurt n. Menem 2013.

Cyberataki i odpowiedzialność banku za nieautoryzowane transakcje płatnicze w systemie bankowości internetowej – teoria i praktyka

Streszczenie

Artykuł dotyczy współcześnie spotykanych technik cyberataków skierowanych przeciwko bezpieczeństwu finansowemu banków i ich klientów oraz relacji banków z ich klientami na podstawie obowiązujących przepisów Unii Europejskiej (Dyrektywa Parlamentu Europejskiego i Rady UE 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego) i polskiej ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych. Autorzy analizują też stronę praktyczną relacji banków z ich klientami, którzy padli ofiarami oszustw komputerowych. Zwracają uwagę, że powszechnie stosowana przez banki praktyka polegająca na odmowie zwrotu środków skradzionych ich klientom w systemie bankowości elektronicznej jest niezgodna z obowiązującymi normami prawa polskiego i europejskiego.

Słowa kluczowe: cyberatak, bezpieczeństwo finansowe, system bankowości elektronicznej, oszustwo komputerowe, Unia Europejska