ARTICLES

CENTRAL EUROPEAN REVIEW OF ECONOMICS & FINANCE
Vol. 39. No 4 (2022) pp. 39-55
DOI https://doi.org/10.24136/ceref.2022.016

Wiesław Łukasz Macierzyński[*], Wojciech Boczoń[**]

The impact of COVID-19 pandemic on cybersecurity in electronic banking in Poland.

Abstract
Purpose: The purpose of the article is to present both theoretical and practical basis for cybersecurity in electronic banking in Poland during the COVID-19 pandemic. During this period a major reorganisation of IT solutions occurred, which allowed to extend the range of online products and services offered both to bank customers and employees. As our life is more and more dependent on digital technologies, cyber attacks have become more costly and more dangerous. Driven by dynamic technological development regulations have changed, which resulted in cybersecurity becoming a key priority in financial institutions.

[*] DSc Wiesław Łukasz Macierzyński is a Professor at the University of Technology and Humanities in Radom, a graduate from the University of Warsaw, the Head of the Chair in Economic Politics and Banking at the Faculty of Economics and Finance at the University of Technology and Humanities in Radom. He is the author of 80 publications (including 11 monographs) covering the areas of banking, investor relations, public relations, advertising, marketing and management. He is a co-founder and a long-time member of the Review Committee of Polish Business Ethics Association – EBEN Poland.

[**] MA Wojciech Boczoń a graduate from Melchior Wańkowicz Higher School of Journalism in Warsaw, and Maria-Sklodowska Curie University in Lublin. He is an author of hundreds of publications covering the areas of personal finance, banking, and cybersecurity. He is the leading editor of PRNews.pl portal, an analyst at Bankier.pl, a journalist for Puls Biznesu newspaper (pb.pl), the winner of the Journalist of the Year 2013 Award, granted by the jury of the competition held during the 9th Congress of Electronic Economy organised by the Polish Bank Association (ZBP). Nominated twice, he is the winner of the Marian Krzak Journalist Award for the year 2014. He is also a finalist of Economic Journalism Award in 2019, organised by Press Club Polska.

All the more so because the rapid technological development has been followed by more and more advanced techniques used by criminals searching for easy financial profits.
Methodology: The paper uses the method of literature review - mostly electronic sources, descriptive and comparative analyses
Findings: From customers' perspective, the impact of COVID-19 pandemic on cybersecurity in electronic banking in Poland may be recognized as negative. The years 2020-2021 brought a dynamic growth in the number of digital banking customers, especially mobile banking. In those years financial institutions recorded an enormous increase in online payments, which was the result of strong, forced by the pandemic, surge in sales in E-commerce. At the same time, there was a sharp rise in the crime rate targeted at banks, but most of all, at bank customers. While the security of the very financial institutions remained unthreatened, there was an explosion in the number of cybercrimes targeted at E-banking users, with the losses giving dozens of millions PLN in total. That is reflected by the data provided by the National Bank of Poland, numerous complaints to the Financial Ombudsman, the Office of Competition and Consumer Protection, as well as the police investigations.
Practical implications: The analysis of relations between theoretical and practical bases of cybersecurity in E-banking in Poland during the COVID-19 pandemic is a key factor for financial institutions. Cybercrime undermines customers' trust in E-channels and therefore negatively influences how banks are perceived, the level of the users' activity in digital channels, and consequently, activity and sales in E-channels. Besides the image and financial risks, banks need to take into consideration the increase in reputation, operation and legal risks. On these grounds, it is possible for state organisations and financial institutions to develop professional education concerning cybersecurity, not only for E-banking customers, but for the whole society.

Kewords: Cybersecurity, cyber threat, ransomware, phishing, smishing, vishing, spoofing, malware

Paper type: Research paper

Introduction

E-banking allows to manage completely both personal and business finances. With a use of a computer or a smartphone, it takes bank customers just a few minutes to open a bank account, apply for complex deposit and credit products. All these operations can be carried out either by the customers themselves, or with remote support of bank staff via a video conference or a text chat. Using chatbots for simple operations is becoming more and more common. A chatbot is a software application designed to conduct an online conversation with a human in a natural language. Chatbots, in a programmed and self-learning way, automate customer support and handle frequently asked customers' questions. In most cases, not only can E-channels replace conventional departments, but also offer a range of additional e-services which are not available in traditional distribution. More and more banks are announcing plans for digitalizing processes of purchasing and servicing more complex products, e.g. the process of granting mortgages. Customers are quickly getting used to purchasing other financial products like insurance, leasing, factoring, but also products which are more loosely related to finances, such as bus tickets, parking fees, motorway tolls, or gitf-cards. All these operations are more and more frequently performed with a smartphone, which in many cases, has become the main distribution channel, as can be contributed to sales of more than a half basic financial products. Smartphones, and even intelligent watches are more and more replacing traditional, plastic paycards.

The rapid development of E-banking is a result of trying to increase the effectiveness measured by, standard for a bank sector, financial indicators – ROA (return on equity) and ROE (return on assets). It is also one of the main factors which influences the universal for all sectors measure of costs level (C/I – Cost to Income). It shows the relation between income and the cost of acquiring that income. Both natural and supported adoptions of E-channels allow to reduce costs quickly, which in the service sector is connected mainly with staff costs. Therefore, the more customers use e-banking, mobile banking and paycards, the more bank branches are closed. This phenomenon is mostly observed in Western Europe, but pandemic increased the pace of this process, which has been in progress since the beginning of 21st century [DW, 08.06.2021].

The worldwide phenomenon of adopting e-banking by retail customers and MSP appears both in Poland and European Union, which is reflected by statistic data. While at the end of 2006 in Poland there were 4.3 million of e-banking users [Związek Banków Polskich, 2010, p. 5], in the second quarter of 2022 the number of users was five times bigger – over 21.6 million ! [Związek Banków Polskich, 2022, p. 6]. Over those 16 years another technological revolution emerged. During this time an absolutely new

channel of bank distribution appeared – mobile banking using mobile applications. In 2006, customers generally did not use mobile phones for bank services. The first mobile application was introduced in Poland in 2009 by now-defunct Raiffeisen Bank Polska [Macierzyński, 06.03.2009]. The application worked only for certain telephones, those operating on system Symbian OS or MS Windows Mobile. Along with the rapid growth in the number of smartphones, other banks subsequently introduced mobile applications into their offer, which resulted in a significant increase in the number of mobile banking customers – 18 million at the end of the second quarter of 2022. While the number of e-banking customers remains stable, the number of users of mobile banking is increasing rapidly. Another important phenomenon is the appearance of the so called 'mobile only' group of customers. Their contacts with the bank rely exclusively on a mobile phone, and only in exceptional situations either use e-banking or visit a bank branch. According to market data, in 2022 there were nearly 13 million of such customers[Boczoń, 09.11.2022].

Along with the growing number of e-banking customers, the importance of these channels increased – not only in the ongoing customer service, but also in the sales of banking services and products. It can be observed with one of the most profitable, high-interest products – cash loans for individual customers. In 2019 sales of these loans in e-channels constituted a significant share - 20-40% of all cash loans sales in Polish banks [Frączyk, 12.10.2019]. Market leaders sold more than a half of loans via e-channels [Bank Millenium, 20.10.2019]. In 2022 the number of loans sold via e-channels constituted on average more than 50%, and in case of the most digital banks, nearly 90% [ING Bank Śląski S.A., 4.08.2022].

The growing importance of e-channels significantly influences changes in using payment services by bank customers. More and more often, the customers are replacing cash with cashless instruments – not only paycards, but also mobile and Internet payments [Maison, 2021]. The number of issued paycards in Poland is growing dynamically. According to the data provided by Narodowy Bank Polski, by the end of the second quarter of 2022 banks had issued nearly 44 million of paycards, including 39 million of paycards for individual customers. The largest group are debit cards – 36.7 million, followed by credit cards – 5 million. In the same quarter, individual customers (96% of all transactions) made with paycards over 2.2 billion cashless transactions, worth over 150 billion PLN [NBP, 2022a]. The statistics provided by Narodowy Bank Polski take into account also technological changes. Currently, over 96% of all issued paycards allow contactless payments. At the same time, however, card payments are more and more frequently made in a digital way, i.e. with a mobile phone, or other devices with a tokenized paycard number,

such as watches, wristbands, etc. According to market data, more than 20% of paycards on the Polish market have their digital counterpart in the form of the most popular systems, i.e. Apple Pay, Google Pay or HCE [Sikorski, 26.08.2022].]. Also, there is a growing number of alternative forms of payments on the Internet or in physical shops, with BLIK, a solution offered by Polski Standard Płatności (Polish Payment Standard – PPS) being the best example. In 2022 over 11 million customers used this solution [Sikorski, 24.08.2022]. Just only in the second quarter of 2002 there were made 292 million transactions worth nearly 40 billion PLN. Customers use BLIK mainly on the Internet (57% of all transactions), payment terminals (14%) and for cash deposit and withdrawal (4%) [NBP, 2022b]. The popularity of this method of payment is strictly connected with the growing number of Internet payments, which is closely related to the increase in sales in E-Commerce during the pandemic [PWC, 11.07.2022]. At the end of 2021 the most popular with Polish customers payment methods were BLIK, online transfers (PayBy-Link) and paycards. In the Tpay survey conducted by SW Research Agencja Badań Rynku i Opinii (Market and Opinion Research Agency) 70% of the surveyed chose BLIK as their favourite method of payment. As for the online transfer and paycards the numbers were 38% and 34% respectively. The particular choice of a payment method actually depends on the availability of payment methods in a given Internet shop. However, even then, Polish customers usually will choose payment by BLIK [Tpay, 2022].

1. The increase in cybercrime during the COVID-19 pandemic

The global COVID-19 pandemic has dramatically increased the speed of digital transformation of companies, and had considerable influence on customers' shopping preferences. Years 2020-2021 brought a rise in the number of customers using mobile banking, and mobile payments such as BLIK. While at the end of 2019 there were 12 million mobile banking users [Związek Banków Polskich, 2020], two years later there were already 16.5 million of them, which meant an almost 40% increase. At the end of the second quarter of 2022 mobile applications had already 18 million users. At the same time, there had been a rise in the number of transactions made by BLIK – from 72 million in the fourth quarter of 2019, to 240 million two years in the same quarter, which meant a 330% increase! A little less spectacular growth occurred in a similar time in case of other Internet payment instruments. The Pay-by-link-like payments had risen by 21% - from 79 million to 96 million transactions, and paycards – 44% - from 33.7 million to 48.8 million transactions. The above given data prove that Polish citizens willingly use modern forms of payments,

which places Poland among the most developed in this matter countries in European Union [Marciniak, 2020].

The development of modern E-banking services and a fast inflow of less experienced customers have contributed to the occurrence of negative phenomena, among which the rapid growth of cybercrime is of the biggest importance. A larger number of users and remote transactions in connection with fast methods of transferring stolen funds led to a rapid increase in the crime rate and attacks on users of digital banking. Those activities increased especially during the COVID-19 pandemic, which is since the beginning of 2020. The fact that transferring stolen funds, cryptocurrencies included, from Poland abroad was very easy also contributed to the situation. According to the data provided by the Police Headquarters, in 2021 there were recorded 14,500 crimes related to e-banking and phishing (art.287 of the Criminal Code). For comparison, in 2020 – the number of them was 6700, in 2019 – 6300, in 2018 – 3600, and in 2017 – 1800. The data from the first three quarters of 2022 indicated a growing tendency (over 15,000), similarly the number of unique cybersecurity incidents recorded by CERT Polska. In 2021 there were recorded 29,500 incidents, in total, which meant 182% growth in comparison to the previous year, whereas by December 2022 the number had reached more than 37,000 [Wittenberg, Rutkowska, 19.12.2022]. The data provided by the Police include exclusively information about ascertained cases, not taking into account those that are still being investigated. Also, not all cases are obligatorily recorded within the e-banking or phishing categories.

The Financial Ombudsman also connected the growing number of crimes related to bank thefts with the COVID-19 pandemic, emphasising it is the most common reason for complaints of financial market customers concerning breaching the Act on Payment Services of 19th August 2011 [Rzecznik Finansowy, 29.07.2021]. It is confirmed by the data regarding the number of complaints to the Financial Ombudsman Service [PAP, 09.09.2021]. The issue of unauthorised transactions frequently appeared in the interventions conducted by the Financial Ombudsman in years 2020 -2022. He also pointed out new types of cyber attack, including the problem of customers robbed by means of the ‘Click Loans’ [Rzecznik Finansowy, 20.04.2022]. While a few years ago criminals focused on attacking customers who possessed considerable funds on their accounts, nowadays, due to a rapid technological development, also those customers who have borrowing power fall victims more and more frequently. The Internet or a mobile application makes it possible for a customer or a thief who has stolen their identity, to take out, almost automatically, an even several-thousand loan in just a couple of minutes. Then, the money is quickly transferred out of the bank.

The number of such crimes increased steeply in the years 2021-2022. This is confirmed by the data provided by Narodowy Bank Polski. The explicit conclusion based on the data is that most of them is reported neither to the police, nor to the Financial Ombudsman. It is so despite considerable amounts being stolen. An average worth of a fraudulent transaction was 3670 PLN in the second quarter of 2022, and was 23% higher compared to the previous quarter. According to the statistics collected by NBP, based on the data provided by banks, in the fourth quarter of 2019 there were 3007 fraudulent orders. Two years later, the number of such operations increased four times – to 12,034, reaching the number of over 18,000 in the first quarter of 2022. Similarly to the number of fraudulent transactions, NBP reported a high rise in the worth of such operations - from 12 to 41 million PLN comparing the fourth quarter of 2019 to 2021. The given data does not include fraudulent transactions made by paycards, whose number is significantly higher – over 60,000 operations quarterly. However, in this case, the number remained on a similar level in the years researched, and during the very pandemic period even dropped [NBP, 10.2022]. Nevertheless, the quoted data lead to an explicit conclusion that in this period attacks on E-banking users increased. This data is confirmed by the report published by CSIRT (Computer Security Incident Response Team) operating by the Office of the Polish Financial Supervision Authority. The report states that in 2021 nearly 11,500 Internet domains were identified and marked as dangerous, so that the access to them should be blocked. That number comprised almost 4,000 fake advertisement sites, 3,000 – courier services, over 2,200 – fake investments, over 1,000 – banks, over 300 – fake payment gateways. Besides, there were reported over 900 websites that should be blocked, which were classified as ‘other’ [Boczoń, 13.01.2022].

3. New scenarios of attacks on customers of banks and financial institutions

The growth in the Internet activity of bank customers is used by criminals who constantly work on new methods of attacks. For many years, ‘phishing’ and its various mutations have been the major threat to the users. The notion ‘phishing’ is a combination of two English words – ‘password’ and ‘fishing’, and means tricking someone into giving sensitive data, e.g. passwords. This fraudulent technique is a form of fraud in which an attacker masquerades as a reputable entity. An unaware user is substituted a fake Internet site for the original one, which are deceptively similar. The only difference is the text in the address bar, which is usually imperceptible, especially for those less alert bank customers. Sometimes they differ only in one letter, or one word. A common strategy is making use of similar Internet domains. The fraudsters masquerade as banks

or other reputable entities sending out fake emails to randomly chosen customers. On the pretext of blocking the bank account or an alleged cyber attack on the bank, they request an urgent logging in E-banking. Next, they provide a fake site, where the user enters sensitive logging in data, which are taken over by the fraudsters. Fraud methods evolve, which is influenced mainly by applying new security measures in E-banking. In the first decade of 21st century attackers using phishing asked customers for the login and the password to the account, and a few codes from the card with one-time pass-codes. These data allowed to log in to the system, and transfer money to the provided account. When PSD2 (The Revised Payment Services Directive) came into effect, it practically eliminated this method of authorisation [Deloitte, 20.09.2019]. One-time passcodes from the card of passcodes were replaced by text messages with codes connected with the operation in progress. The next step taken to increase customers' security was introducing mobile authorisation using the bank mobile application. In both cases, it was a smartphone which became a necessary device to authorise bank operations. This is the reason why currently, more and more attacks on clients are aimed at taking control over a mobile device [Boczoń, 20.01.2019].

The focus on remote attacks on smartphones could be clearly observed during the pandemic, when criminals impersonated official state applications for detecting threats. Analysts of CSIRT (Computer Security Incident Response Team) operating by the Office of the Polish Financial Supervision Authority gave the attack on the mobile application ProteGo Safe as an example. The fake version supposedly was to diagnose the user with the COVID-19 by the means of cough recording. In fact, it was malicious software (malware) Black Rock, which once having been installed on the device, was able to overlay bank applications. Activities like that were targeted at taking over sensitive data entered on the telephone screen [KNF 09.02.2021]. Another example was a website which looked like the official Google Play shop, from which an unaware user could download a fake application 'Home Quarantine'. The malicious application made use of being given an easy access to the telephone, provided the users with a fake login panel for E-banking [Zagańczyk, 05.02.2021]. The attackers infected a telephone mostly by the means of 'smishing' – a mutation of phising. The criminals used text message campaigns to send out links directing to the infected websites. Analysts of CSIRT by the Office of the Polish Financial Supervision gave as an example fake text messages about sending to home quarantine. The sent link redirected the users to the Cerberus Trojan, which infected the telephone. According to cybersecurity experts, smishing attacks became so common due to the fact that users trust text messages received on their phones much more than e-mail messages.

[Trendmicro, 2022]. Also, it is relatively easier for criminals to obtain a mobile phone number than an e-mail address. The thieves send out text messages to random 9-digit numbers from the Office of Electronic Communications register [UKE, 2022]. The reason why such attacks are so effective is, among others, that 98% users reads text messages, and 45% replies to them. For comparison, in case of e-mails, the numbers are 20%, and 6% respectively [Cote, 4.10.2019]. An attack by a text message may occur in a different form, especially when combined with various sociotechniques. A common form of an attack, resulting in customers' financial losses, were impersonating courier companies, parcel lockers operators, energy or gas providers, etc. In such cases, criminals requested surcharges for shipment or an electricity bill. Along the links directing to fake websites or infected software, it is common to provide a telephone number to a fake bank representative requesting an urgent contact.

A dangerous variant of 'smishing' occurred during the pandemic – tricking victims into handing over money by the means of social media. During the pandemic BLIK frauds became very common. The criminals took over accounts on Facebook, then using the Messanger communicator linked to the account, requested the victim's friends for an urgent loan. The scammers asked for a BLIK code to withdraw money from an ATM, or having given their telephone number, had the money transferred to their telephone. Another type of massive attacks via social media were attacks on users of advertisement portals, e.g. OLX.pl, Vinted, Allegro Lokalnie. Scammers used a user's phone number to redirect the chat from official channels to outside communicators, such as, popular in Poland, WhatsApp. Pretending to be interested in goods on sale, they sent out fake links directing to pay for the courier who had been sent by them. In fact, those were fake payment gateways. The templates the victims were provided with had been thoroughly designed, and the cyber criminals came into possession of all the data which had been entered, in real time. [Policja.pl, 23.09.2021]. Having accessed these date, the criminals made Internet transfers, payments by the victims' paycards, and even installed on the victims' behalf mobile applications, which gave them full access to the customer's finances. In such cases, not only did the customer lose all their money, but also fell victim of a cash loan taken on their behalf. The criminals most commonly used the popular with customers payment system – BLIK. The targeted attack on users of this service may serve as an example. The criminals sent text messages to random numbers informing about an alleged transfer from an unknown receiver, with a link directing to a fake bank website. The receiver of the message, having entered the data, shared sensitive information with cybercriminals, and as a result, lost their money [Konieczny, 31.01.2022].

Another dangerous variant of phishing, which intensified during COVID-19 pandemic, became 'vishing' – voice phishing. It was especially dangerous when combined with the so called 'spoofing' (the proper name of this attack is CallerID Spoofing). The attacks are made by the means of telephone calls when criminals disguise their identity so that it appears that the incoming call is from a financial institution, and the caller is a bank representative. Spoofing is a situation in which a person successfully identifies as another telephone number, including a bank help centre, or even the police. The receiver of the call being convinced they are talking to a bank representative, share with them all sensitive data. This is how the scammers gain information which allows them to log in to the victim's bank account. Another variant of this attack is installing common software for screen sharing. Having installed this type of software, the criminals make their unaware victims perform operations. This kind of cyber attack is extremely dangerous, as spoofing does not require advanced hacker techniques. Assuming identity of another number is possible thanks to numerous Internet portals which, for little fees, give the ability to control the Caller ID on all calls and texts. Even though this type of services has to be paid for, they may be used anonymously, e.g. using crypto-currencies for payments. This way makes it harder for the police to detect the culprits. This problem has become so common, that state institutions in collaboration with the Office of Electronic Communications have taken measures to limit it, drafting a Bill concerning fighting malpractice in electronic communication [KPRM, 12.2022]. The suggested solutions aim to create appropriate laws to take action within preventing malpractices in electronic communication by telecommunication entities, and consequently, limit the scope of the malpractices and ensure security of the attacked users.

The weakness in the infrastructure of telecommunication entities is not the only way used by criminals to rob bank customers. Another example is massive using of automatic advertising systems of the biggest technological companies such as Google and Facebook. According to British banks, as much as 75% of their customers' loss was linked to advertisements displayed on the websites connected with the biggest search engine in the world, advertisements on Facebook, or advertisements on dating or e-commerce portals [Finextra, 25.07.2022]. As a result of no effective action taken by such companies, graphic advertisements using the image of renowned companies, people or media appear on sites of the biggest information portals. In this way, criminals gain a wide range, which could not be accessed in a traditional way. They make use of the image of the medium on which the fake advertisement appears. Automating advertising systems leads to practically no control over the content of the advertisements. However,

both Google and Facebook require their users to report suspicious advertisements, shifting the cost on entities which fell victims to fake advertisements, fake sites, but still keeping the profits gained from publishing this type of advertisements for themselves. Users, misled by fake information spotted on websites of the biggest Internet services in Poland, being convinced they invest in shares or crypto-currencies, lose their money. This type of attacks, besides the sociotechniques used by criminals, may not have worked without the use of tools offered by Google or Facebook in order to reach millions of unaware victims.

4. The increase in the number of attack on state and financial institutions during the period of COVID-19 pandemic

Over the years 2019-2021 the increase in cyber attacks concerned also the government administration, but also corporate customers, banks included. The pandemic resulting in the necessity to organise work online has posed a challenge as for the security, as companies became more vulnerable to cyber attacks. It increased the necessity to implement improvements within crisis management, ensure the continuity of operating, but also increase the funds for cybersecurity. The results of research conducted by the European Union Agency for Cybersecurity (ENISA) show that a threat to cybersecurity in European Union has impact on sectors which are crucial for a society. Those who suffered from cyber attacks most were: public administration/ the Government, digital services providers, society in general, healthcare/medicine, and finances/banking [PE, 27.01.2022]. The fast digital transformation, which was enforced by the new situation, triggered new attack vectors. Cybercriminals, taking advantage of the COVID-19 pandemic, targeted particularly at institutions and companies whose employees worked online. According to KPMG – a global network of professional firms providing audit, tax and advisory services, 55% of the surveyed companies in Poland claimed that the outbreak of the pandemic contributed to the increase in the risk of cyber attack. In 2020, as many as 64% of companies had recorded minimum one incident of breaching security. That meant a 10% increase in comparison to the previous year. In the same year 19% companies recorded an increase in cyber attack attempts; whereas only 4% of the surveyed claimed the number had dropped. According to the surveyed, data leak with the use of malware posed the biggest threat, and phishing was placed on a similar level. On the other hand, the least risky cyber threats were: breaking into mobile devices, attacks making use of application errors, and attacks on wireless networks [KPMG, 12.2022]. However, according to the report prepared for Volkswagen Bank GmbH Branch in Poland, as many as 16% of domestic companies had been a target of a cyber attack. Phishing attacks were most frequent – 54%. Ransomware

attacks constituted 7% of total attacks. The consequences of the attacks were listed as: the necessity to suspend the company's operating putting some company processes at halt – 10% of the companies surveyed, data breach or loss – 3%. The remaining 13% chose other answers [PRNews, 18.11.2021]. In case of Polish banks, the most common cyber attack method, especially after the Russian invasion on Ukraine, were DDoS attacks. According to the statistics provided by the Polish Financial Supervision Authority (KNF), the number of such attacks especially increased in 2021 – there were 500% more of them than the year before [Marszycki, 23.02.2022]. In fact, it meant that during this time an average company from the banking-financial sector in Poland was a target of a cyber attack almost one thousand times a week [Duszczyk, 23.02.2022].

According to companies which provide advisory services, from the global perspective, ransomware poses the biggest threat [Morgan, 21.10.2019].This type of attack is a form of a malware that locks the user out of their files or their device, then demands a payment to restore access. It is estimated that in 2021 global losses caused by ransomware may have reached as much as 20 billion USD.

5. Actions undertaken by banks and state administration in order to decrease the number of cyber attacks

During the COVID-19 pandemic, state administration, including the Polish Financial Supervision Authority and the Office of Competition and Consumer Protection were in charge of the issue of cybersecurity. In February 2021 the Chairman of the Polish Financial Supervision Authority in the letter addressed to the banking sector emphasised that financial services providers are obliged to follow the policy 'security first'. In fact, it meant that the issue of security was to be given priority over any other issues [Boczoń, 16.02.2021]. While introducing new services, financial institutions should take into consideration current attack tendencies, methods used by cybercriminals, but also potential risks connected with the provider's planned activities, not only in relation to the customers, but also in relation to the potential impact of those activities on the entire sector of banking services.

The KNF Chairman's letter is an example of the so called 'soft' recommendation. Although, unlike recommendations which are issued by the KNF Authority, it was not binding on banks, in fact it is of similar importance. It is a proof of how important the issues of cybersecurity and education are. Most institutions react to new forms of attacks on a day-to-day basis, informing their users by placing appropriate announcements and alerts on their websites. According to KNF, those activities are not sufficient, they do not bring expected effects, which is reflected by the scope of successful attacks on users

of bank services, and the level of frauds related. The KNF take the view that banks should not focus on their customers exclusively, but they should rather run a broad campaign connected with cybersecurity [Forsal.pl, 15.02.2021].

In 2021, the President of the Office of Competition and Consumer Protection initiated explanatory proceedings in order to examine how banks deal with customers' complaints connected with money thefts from bank accounts, and also what authentication methods they use. Eighteen banks were summoned to present explanations and documents related to this type of cases [UOKiK, 19.07.2021]. The reason for this action was a gradually growing number of consumers' complaints connected with money thefts from accounts, or financial obligations resulting from an identity theft. The customers reported to the Office of Competition and Customer protection problems of losing their savings, and banks rejecting the complaints. The very notifications concerned scammers pretending to be bank Help Line employees, using fake website of the bank, or using spy software in order to obtain data. The explanatory proceedings concerned, in fact all the biggest commercial banks in Poland. The evidence collected over a year allowed to bring a charge of infringing collective interests of consumers against five banks. During the explanatory proceedings, the President of the Office of Competition and Consumer Protection established that banks could have misled their customers responding to complaints concerning unauthorised transactions. It is extremely important, as for infringing collective interests of consumers, the banks may be imposed a fine of up to 10% of its turnover. [UOKiK, 18.07.2022]. At the same time, at the beginning of 2022, the Office of Competition and Consumer Protection launched a countrywide social campaign 'If you lose your data, you will lose your money!' It also warned against the attempts of money and data thefts. [UOKiK, 05.12.2022].

Conclusions

During the COVID-19 pandemic cybercrime in Poland significantly increased. This fact is confirmed by the data provided by Narodowy Bank Polski, supported by numerous customers' complaints to the Financial Ombudsman, to the Office of Competition and Consumer Protection, and the number of cases investigated by the police. The analysis of those cases shows a huge dynamic of the crime increase. Banks did not manage to handle the increased number of cyber attacks. It posed a serious challenge, as it is difficult to introduce security measures against new types of attacks, even more because criminals used sociotechniques combined with 'spoofing'. On the other hand, state institutions, the Polish Financial Supervision Authority included, often took action too late,

and did not take into account the market context. Financial institutions started to put more emphasis on cybersecurity education. However, the growing number of cybercrimes is a proof that the actions taken have not brought the desirable effects. Banks undertook those actions not only because of the growing financial losses, but first and foremost, because of the rising risk of reputation loss, including the rise in image risk, the rise in operation risk and the rise in legal risk.

Bibliography:

1. Bank Millenium, *Bank Millenium – ponad 2 mln aktywnych klientów, rekordowy wzrost organiczny w czasie integracji z Euro Bankiem,* 20.10.2019; https://www.bankmillennium.pl/pl/o-banku/centrum-prasowe/informacje-prasowe/-/news-info/bank-millennium-ponad-2-mln-aktywnych-klientow-rekordowy-wzrost-organiczny-w-czasie-integracji-z-euro-bankiem-28-10-2019?news_articleId=27660806
2. Boczoń W., *Ich bezczelność, wasze pieniądze. Oszuści zbroją się na 2019 rok* , 29.01.2019; https://www.bankier.pl/wiadomosc/Ich-bezczelnosc-wasze-pieniadze-Oszusci-zbroja-sie-na-2019-rok-7638567.html
3. Boczoń W., *KNF pisze list do banków ws. cyberbezpieczeństwa. Przypomina o zasadzie „security first" i zwraca uwagę na praktyki budzące wątpliwości*, 16.02.2021; https://prnews.pl/knf-pisze-list-do-bankow-ws-cyberbezpieczenstwa-przypomina-o-zasadzie-security-first-i-zwraca-uwage-na-praktyki-budzace-watpliwosci-456808
4. Boczoń W., *Plaga fałszywych stron internetowych. Tak oszukiwano Polaków w 2021 r.*, 13.01.2022; https://www.bankier.pl/wiadomosc/Plaga-falszywych-stron-internetowych-Tak-oszukiwano-Polakow-w-2021-roku-8257190.html
5. Boczoń W., *Raport: Liczba użytkowników bankowości mobilnej – II kw.* 2022, 09.11.2022; https://www.pb.pl/raport-liczba-uzytkownikow-bankowosci-mobilnej-ii-kw-2022-1168995
6. Cote S., *The Future of Sales Follow-Ups: Text Messages* , 4.10.2019; https://www.gartner.com/en/digital-markets/insights/the-future-of-sales-follow-ups-text-messages
7. Deloitte, *PSD2 – Jakie zmiany dla dostawców usług płatniczych weszły w życie 14 września 2019 r.?*, 20.09.2019; https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/PSD2-jakie-zmiany-czekaja-dostawcow-uslug-platniczych-od-14-wrzesnia-2019.html
8. Duszczyk M., *Zmasowane cyberataki na instytucje finansowe w Polsce*, 23.02.2022; https://www.parkiet.com/finanse/art35742811-zmasowane-cyberataki-na-instytucje-finansowe-w-polsce

9. DW, *Banki. Nadchodzi największa fala zamykania oddziałów*; https://p.dw.com/p/3ua7l, 08.06.2021.
10. Finextra, *Lloyds, Santander, Barclays, TSB demand Google, Facebook reimburse online fraud victims*, 25.07.2022; https://www.finextra.com/newsarticle/40697/lloyds-santander-barclays-tsb-demand-google-facebook-reimburse-online-fraud-victims
11. Forsal.pl, *KNF: banki powinny lepiej edukować swoich klientów w kwestii cyberbezpieczeństwa*, 15.02.2021; https://forsal.pl/finanse/finanse-osobiste/artykuly/8096464,knf-banki-lepiej-edukowac-swoich-klientow-w-kwestii-cyberbezpieczenstwa.html
12. Frączyk J., *Tysiące pracowników banków na bruk. Zastępują ich technologie*, 12.10.2019; https://www.money.pl/banki/tysiace-pracownikow-bankow-na-bruk-zastepuja-ich-technologie-6433287045900417a.html
13. ING Bank Śląski S.A. *Wyniki finansowe i biznesowe za II kwartał 2022 roku*, Warszawa, 4 sierpnia 2022 roku., https://www.ing.pl/_fileserver/item/xq2t6xq
14. KNF, *Zachowaj ostrożność - telefon Twoim kluczem do finansów! [Analiza Blackrock - ProteGo Safe]*, 09.02.2021; https://www.knf.gov.pl/dla_rynku/CSIRT_KNF?articleId=72548&p_id=18
15. Konieczny P., *Uwaga! Ktoś podszywa się pod BLIK*, 31.01.2022; https://niebezpiecznik.pl/post/uwaga-ktos-podszywa-sie-pod-blik/?more
16. KPMG, *Barometr cyberbezpieczeństwa. COVID-19 przyspiesza cyfryzację firm*, dostęp: 12.2022; https://home.kpmg/pl/pl/home/media/press-releases/2021/03/media-press-barometr-cyberbezpieczenstwa-covid-19-przyspiesza-cyfryzacje-firm.html
17. KPRM, *Projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej*, dostęp 12.2022; https://www.gov.pl/web/premier/projekt-ustawy-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej
18. Macierzyński M., *Mobilny VIP w Raiffeisenie,* 06.03.2009; https://prnews.pl/mobilny-vip-w-raiffeisenie-55980
19. Maison D., *Postawy Polaków wobec obrotu bezgotówkowego – raport z badania 2021 i analiza porównawcza z danymi z 2009, 2013 i 2016 roku*, Narodowy Bank Polski, Warszawa 2021; https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/obrot-bezgotowkowy-2021.pdf
20. Marciniak A., *Badanie Mastercard: W pandemii Polacy częściej korzystają z cyfrowej bankowości*, 20.11.2020; https://newsroom.mastercard.com/eu/pl/news-briefs/badanie-mastercard-w-pandemii-polacy-czesciej-korzystaja-z-cyfrowej-bankowosci
21. Marszycki M., *Rząd ogłasza trzeci stopień alarmowy, a KNF ostrzega instytucje finansowe przed cyberatakami*, 23.02.2022; https://itwiz.pl/rzad-oglasza-trzeci-stopien-alarmowy-a-knf-ostrzega-instytucje-finansowe-przed-cyberatakami/

22. Morgan S., *Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021*, 21.10.2019; https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
23. NBP, *Informacja o transakcjach oszukańczych dokonywanych przy użyciu bezgotówkowych instrumentów płatniczych w II kwartale 2022 r.*, 10.2022; https://www.nbp.pl/systemplatniczy/informacja-o-transakcjach-oszukanczych-2022q2.pdf
24. NBP, *Karty płatnicze*; https://www.nbp.pl/home.aspx?f=/systemplatniczy/karty_platnicze.html [dostęp: 12.2022a]
25. NBP, *System BLIK, Inform12acja o liczbie i wartości transakcji w kolejnych kwartałach – od 2015 r.;* https://www.nbp.pl/systemplatniczy/dane/files/BLIK.xlsx [dostęp 12.2022b]
26. PAP, *Rzecznik finansowy: rocznie dochodzi do ok 250 tys. kradzieży środków z rachunków bankowych*, 09.09.2021; https://www.pap.pl/aktualnosci/news%2C943659%2Crzecznik-finansowy-rocznie-dochodzi-do-ok-250-tys-kradziezy-srodkow-z
27. PE, *Cyberbezpieczeństwo: główne i nowe zagrożenia*, 27.01.2022; https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia-w-2021-r-infografiki
28. Policja.pl, Uwaga na oszustwa przy pomocy OLX oraz Whatsapp , 23.09.2021; http://zoliborz.policja.waw.pl/r5/aktualnosci/103731,UWAGA-NA-OSZUSTWA-PRZY-POMOCY-OLX-ORAZ-WHATSAPP.html
29. PRNews.pl, *Badanie: rośnie rola banków w walce z cyberzagrożeniami*, 18.11.1021; https://prnews.pl/badanie-rosnie-rola-bankow-w-walce-z-cyberzagrozeniami-463104
30. PWC, *Do 2027 wartość rynku e-commerce w Polsce wzrośnie o ponad 94 mld zł do 187 mld zł*, 11.07.2022; https://www.pwc.pl/pl/media/2022/2022-07-11-do-2027-wartosc-rynku-e-commerce-w-polsce-wzrosnie-o-ponad-94-mld-zl-do-187-mld-zl.html
31. Rzecznik Finansowy, *Rzecznik Finansowy ponownie pyta banki o nieautoryzowane transakcje*, 29.07.2021; https://rf.gov.pl/2021/07/29/rzecznik-finansowy-ponownie-pyta-banki-o-nieautoryzowane-transakcje/
32. Rzecznik Finansowy, *Rzecznik Finansowy zbada „kredyty na klik”*, 20.04.2022; https://rf.gov.pl/2022/04/20/rzecznik-finansowy-zbada-kredyty-na-klik/
33. Sikorski M., *Już prawie 3 mln klientów PKO BP aktywnie korzysta z Blika. Jeszcze pięć banków ma przynajmniej milion „blikowiczów”*, 24.08.2022; https://www.cashless.pl/12287-blik-liczba-uzytkownikow-2-kw-2022

34. Sikorski M., *W ciągu roku liczba kart dodanych do cyfrowych portfeli płatniczych, takich jak Apple Pay czy Portfel Google wzrosła o ok. 3 mln,* 26.08.2022; https://www.cashless.pl/12302-apple-pay-portfel-google-liczba-kart-dodanych-2-kw-2022
35. Tpay, *Jak Polacy lubią płacić online? Konsument 2.0*, 2022; https://tpay.com/user/assets/files_for_download/jak-polacy-placa-2022.pdf?utm_source=blog&utm_medium=reklama&utm_campaign=raport2022&utm_id=raport-merchanci
36. Trendmicro, *Czym jest smishing?*, dostęp 12.2022; https://www.trendmicro.com/pl_pl/what-is/phishing/smishing.html
37. UKE, *Numeracja. Tablice Zagospodarowania Numerami*, dostęp 12.2022; https://numeracja.uke.gov.pl/
38. UOKiK, *„Stracisz dane, stracisz pieniądze!" – kampania Prezesa UOKiK*, 05.12.2022; https://finanse.uokik.gov.pl/nieautoryzowane-transakcje/stracisz-dane-stracisz-pieniadze-kampania-prezesa-uokik/
39. UOKiK, *Nieautoryzowane transakcje bankowe – postępowania*, 19.07.2021; https://finanse.uokik.gov.pl/nieautoryzowane-transakcje/nieautoryzowane-transakcje-bankowe-postepowania/
40. UOKiK, *Transakcje nieautoryzowane – zarzuty wobec 5 banków*, 18.07.2022; https://finanse.uokik.gov.pl/nieautoryzowane-transakcje/transakcje-nieautoryzowane-zarzuty-wobec-5-bankow/
41. Wittenberg A., Rutkowska E., *Za cyberkanty siedzą nieliczni. Czy można to zmienić?*, Dziennik Gazeta Prawna, 19.12.2022.
42. Zagańczyk M., *Uważaj na fałszywą aplikację Kwarantanna domowa! Wykrada dane do konta w banku*, 05.02.2021; https://www.telepolis.pl/wiadomosci/bezpieczenstwo/uwazaj-na-falszywa-aplikacje-kwarantanna-domowa-wykrada-dane-do-konta-w-banku
43. Związek Banków Polskich, *NETB@NK Raport Bankowość internetowa i płatności bezgotówkowe*, *IV kwartał 2010*; https://www.zbp.pl/getmedia/77dc757a-bdf9-44cc-a4d1-d2999fd9c42a/Raport_Netbank_Q4_2010
44. Związek Banków Polskich, *Raport NETB@NK, Bankowość internetowa i moblina, płatności bezgotówkowe, 2 kwartał 2022*; https://www.zbp.pl/getmedia/1d8430f0-7634-45f6-b754-3ae1cb1cffa6/Raport-Netbank_Q2-2022-(1)
45. Związek Banków Polskich, *Raport NETB@NK, Bankowość internetowa i moblina, płatności bezgotówkowe, 2 kwartał 2020*; https://www.zbp.pl/getmedia/aef02d51-5f69-45bc-9d0b-3637159d14b4/Raport-Netbank_Q1-2020