NOWA KODYFIKACJA PRAWA KARNEGO. Tom XLII
AUWr No 3768 Wrocław 2016

DOI: 10.19195/2084-5065.42.3

The issue of crimes committed with some electronic payment devices

Rafał Cieśla

Department of Forensic Sciences
Faculty of Law, Administration and Economics, University of Wrocław

It is a commonplace that the internet is one of the most powerful tools at the disposal of contemporary societies; it is also one of the most dynamically developing ways of information transfer. Access to information is the most important and desirable aim of human aspirations. The internet is still developing very dynamically, thus defying any efforts at determining the limits of its advancement; it creates infinite opportunities in various areas, while its great potential affects all aspects of human existence. For years the internet has also been the medium for financial transactions involving electronically regulated cash flow. Many of these transactions are carried out with the use of payment cards, which for many people constitute an obvious alternative to traditional transactions involving cash. The history of payment cards elsewhere in the world goes back to the beginning of the previous century, but in Poland they came into use much later, i.e. in the mid-1990s. The development of the internet, and especially the speed of data transfer which it offers, have greatly facilitated the transactions involving payment cards. This fact poses a question concerning the security of such transactions. The popular and universal character of online payments, not necessarily with the use of payment cards, resulted in the emergence of crime involving identity theft and conducting illegal transactions.

One of the most widespread is phishing[1] — one of the most damaging, which also very often involves payment cards. Phishing is not limited solely to the internet; it may occur in other situations, such as face to face or telephone conversations or transferring information via text messages (SMS or MMS). In general terms, phishing consists in illegal acquisition of sensitive data, such as personally identifiable information and related biographic data, biometric data, website passwords, payment or credit card numbers, their expiry dates, CVC, CVV codes[2], etc. The perpetrators resort to the methods of social engineering and usually assume appearances of credibility, most frequently posing as a trustworthy person or institution urgently asking for this kind of information. Phishers perform complex manipulations aimed at their victims. Typically, they present a form to be filled in on the webpage, send an email or an instant message — all deceptively similar to genuine ones — and thus potential victims, making their sensitive data[3] available in good faith, are not aware that they will be intercepted by a phisher. The beginnings of this interesting albeit dangerous phenomenon go back to the late 1980s. It was described for the first time in 1987. The very name "phishing" appeared much later — in 1996 — in a hacker magazine "2600". "Phishing" is a coinage of two words: "fishing" and "phreaking" por. przypis 1 (i.e. deceiving telecommunication systems). The first instance of phishing was recorded in late 1995. Wares[4] communities using the AOL network[5] specialised in forging credit card numbers. But when their internet provider introduced appropriate security measures, they began intercepting card details from other users. Phishers posed as AOL staff members and sent messages to potential victims asking them to reveal their passwords. The reason for that usually quoted the need

[1] Combination of words "fishing" and "personally identifiable information"; it is sometimes referred to as "password harvesting".

[2] Verification code (Card Verification Value, Card Verification Code, Card Verification Number).

[3] These include the first name, family name, address of residence, the PESEL number (Polish equivalent of the Social Security/Insurance Number), identity card number, payment card number and expiry date, card verification code.

[4] Wares (a corrupt form of "software) — in IT jargon an umbrella notion for all kinds of IT products or licences, mainly shareware or adware distributed illegally, especially after copy protection is disabled.

[5] America Online — an internet provider.

to "verify your account" or "confirm billing information". The phenomenon of illegal acquisition of data soon became such a big problem on AOL that they added a line on all instant messages stating: "no-one working at AOL will ask for your password or billing information". AOL did not deal successfully with the phenomenon until late 1997. Phishers were quick to realise that if simple social engineering worked in one network, it may be successfully implemented in another on a much greater scale[6].

An interesting and effective instance of phishing was the theft of personally identifiable information from e-gold customers in 2001. Immediately following the attack on the World Trade Centre[7], hackers contacted the customers requesting confirmation of their personally identifiable information due to a possible outbreak of war in the territory of the United States and the need to protect the national economy. It confirmed the effectiveness of criminal implementation of social engineering in the theft of important information. Three years later most of the institutions combating cybercrime agreed that phishing constitutes one of the greatest threats for the data network[8].

As it was mentioned above, initially phishing was used mainly to acquire access to email accounts to send spam (unwelcome advertisements and emails)[9]. At present phishing attacks most frequently target bank accounts, auction websites, credit cards and social networking services.

Phishing also concerns payment cards, where the most frequent crime so far is skimming[10]. A short discussion of this online crime should begin with comparing and contrasting transactions in the real world and on the internet.

To begin with, a basic difference between the use of payment cards on the internet and carrying out a transaction in a cash point or a payment terminal consists in a physical presence of the card in the acceptor's[11]

[6] M. Gajewski, *Phishing — łowienie naiwnych*, www.chip.pl (access: 4.02.2016).

[7] The attack took place on 11 September 2001.

[8] M. Gajewski, op. cit.

[9] A. Żesławska, *Phishing — co to jest?*, www.kartyonline.pl (access: 7.01.2016).

[10] Skimming — a crime consisting in illegal copying of the magnetic strip or chip on a credit card.

[11] Acceptor — the subject who concludes an agreement with a merchant or the acceptor's bank to accept payments by card for the provided goods or services, www.mastercard.pl (access: 19.03.2015).

point at the moment of completing a transaction. The acceptor does not see the card in cyberspace, and thus this type of transaction is referred to as a CNP[12] online transaction. Another difference is the direct contact between the seller and the buyer. The third is the delay of the moment of delivery of the purchased goods, which differs from that in cash point transactions or the transactions conducted in electronic terminals. The delay may be longer or shorter, depending on the speed of data transmission. The card holder purchases certain goods or services on the internet. A difference also emerges in the case of cash point transactions and POS[13] transactions, which result in the acquisition of goods, execution of payment for services or additionally cash withdrawal (cash back service[14]). The last significant difference is the environment of the transaction. In an online transaction the user goes online via electronic appliances and telecommunication connections. The cyberspace ensures quite a high level of anonymity for the subjects carrying out transactions, but one of the consequences of entering the virtual reality is a possible acquisition of data transferred during a transaction by unauthorised subjects, even though the techniques providing their security are constantly being improved. The transactions carried out on the internet and in other environments by payment cards are targeted for the acquisition of data which may enable third parties to carry out illegal transactions. The data in question may be acquired in various ways[15].

The perpetrators operating on the internet aim at acquiring the data which they will later be able to use in subsequent transactions, and especially the information about cards and their holders. For this purpose they use various, more or less sophisticated methods of acquiring the

[12] Card Not Present.

[13] Point of Sale.

[14] A bank service allowing a card holder to withdraw cash while doing shopping. This transaction may only be conducted when the customer pays for the purchased goods, prior to which he or she declares a withdrawal of an additional amount in cash. The transaction is possible for all the holders of debit VISA and MasterCard cards issued by those banks which offer the cash back service. A customer may withdraw a maximum of 200 PLN in one transaction, which is usually free of charge and if not, it is charged less than when withdrawing cash from a cash point not belonging to the bank issuing the card.

[15] R.W. Kaszubski, J. Grodzicki *Bezpieczeństwo płacenia kartą w Internecie*, www.bezgotowkowo.naszemiasto.pl (access: 10.02.2016).

precious data. The first of the methods used on the internet is phishing mentioned above. It consists in sending an email asking to visit a webpage indicated. The recipient is appropriately motivated (e.g. by the need to verify the data of the payment card to extend its validity, reactivate it, add a new attractive application, improve the security of online transactions, etc)[16]. The email is to be credible for the recipient and allay his or her suspicions, therefore it displays certain features misleading the card holder, e.g. it may imitate genuine emails sent by the card issuer. After clicking the link attached to the email, the card holder is redirected to a webpage where he or she will be asked to disclose the card details. The page is deceptively similar to the issuer's genuine webpage, while its address practically does not differ from the genuine one. In reality it is a webpage created by the perpetrator whose email encouraged the card holder to enter and not the genuine one. The data revealed by the holder are intercepted by the phisher, who in this way acquires information about someone else's payment card which may later be used to carry out online transactions at the card holder's expense. The problem may be illustrated with a few examples of phishing from Poland. One of the first, from the 1990s, consisted in creating a webpage carrying a logo of one of the banks. The bank customers received information that on that page they may verify their credit balance (after providing certain data). When payment card holders revealed these data, an announcement appeared claiming a server overload and temporary inaccessibility of data. At that time the revealed data were transferred to the webpage's author. Even though it happened more than ten years ago, the cooperation between banks and law enforcement bodies resulted in blocking the webpage and apprehending the perpetrator[17]. Another example may be more sophisticated emails, where the fraudsters informed the recipients that someone had used their data in a fraud and asked them to verify their personally identifiable information for security reasons, allowing the users 72 hours; otherwise their accounts would be blocked[18]. Yet another example of phishing was an attack on a prominent bank in Poland carried out in

[16] R. Kaszubski, Ł. Obzejta, *Karty płatnicze w Polsce*, Warszawa 2012, p. 401.
[17] R.W. Kaszubski, J. Grodzicki, op. cit.
[18] http://www.e-platnosci.23.pl/scam_ebay_spoof_email.htm (access: 20.02.2016).

2010[19]. A false message was sent from a "counterfeited" address service@pkobp.pl, while a link leads to the webpage: Hxxp://ool-44c3ed12.static.optonline.net/pkobp.pl/, where the victim was asked to give his or her credit card number, the CVV[20] code and PIN[21]. Another example was an attack on the customers of another Polish bank, who received puzzling emails. After clicking a hyperlink, the unaware customer was redirected to a false website. The emails were sent in two series. The emails from the first series came from Polish servers and were written in faulty English[22]. The other series was prepared more carefully, the emails came from servers located abroad and therefore the hyperlinks could be active for much longer. Still, it was relatively easy to discover the deceit, because the emails lacked Polish type characters. Additionally, after a mouse pointer hovered above the hyperlink, the real address appeared, which unequivocally proved a foreign location[23].

Another form of phishing consists in sending a card holder a letter via traditional post which includes a type of information carrier to be used with a personal computer, laptop, etc., e.g. a CD (now less frequently) or a pendrive. Just like a webpage in the phishing version the letter is deceptively similar to that from a respected institution. The letter includes information encouraging the addressee to use the carrier to find out about the company's new offer or watch a film. After the carrier was connected with the computer, a programme was activated which stole the data (e.g. a Trojan) and if the computer had an internet connection, the data were sent to the perpetrator. This is a variety of a phishing strategy, because the card holders using them on the internet are now better informed on possible dangers[24].

Another example of phishers' creativity is the so-called phone phishing (or vishing), which consists in phoning a card holder and asking him or

---

[19] P. Konieczny, *Uwaga na fałszywe e-maile PKO*, www.niebezpiecznik.pl (access: 5.01.2016).

[20] Card Verification Value.

[21] Personal Identification Number; P. Konieczny, op. cit.

[22] M. Ziarek, *Phishing, pharming i sieci zombie — to czego nie wiesz o swoim komputerze*, www.viruslist.pl (access: 8.10.2016).

[23] Ibid.

[24] R. Kaszubski, Ł. Obzejda, op. cit., p. 402.

her to provide the details of his or her card[25]. An unaware card holder may provide the information required for the commitment of another fraud.

Card holders constitute the most susceptible link in the transaction chain exposed to the attack of fraudsters in the crime involving the use of payment cards on the internet and skimming. Therefore, it is vital that they are informed about the ways of committing this sort of crime. While carrying out transactions involving payment cards, the principle of cautious approach should be followed, because no technical security devices will compensate for lack of caution. Perpetrators know the principles of social engineering, which they use to manipulate card holders, exploiting human weaknesses, e.g. greed, fear, gullibility, curiosity or carelessness[26]. One of the main aspects of human nature is greed, which is exploited by fraudsters. Easy money, winning a lottery, exploiting loopholes in online payment are based on the principle "to start with, give us a little money, later you'll get millions". Obviously, there is no "later", which should always be remembered. A frequently exploited weakness is fear. The messages reaching the "easily intimidated", e.g. "click this hyperlink or your account will be blocked", "if you don't text this number, your account will be deleted within 10 minutes after reading this email" exploit fear — an emotion, which forces them to do what they are told without thinking., while it is sufficient to remember that no bank will block an account or a payment card in this way. No bank, no card issuer, no subject from an online auction website will request clicking a hyperlink and providing personally identifiable information. And first of all, no-one will exert time pressure and encourage impulsive behaviour. All the messages of this type, attempting to frighten and exert pressure on a user should be rejected as potentially dangerous. There is also a good side to human nature, which perpetrators deliberately try to exploit. It should be remembered that all the requests for help arriving as spam constitute fraud. No charity will send spam and ask for detailed personally identifiable information. Sometimes the internet users send money to fraudsters out of pure curiosity. The pace of life on the internet is much

[25] www.americanexpress.com (access: 10.11.2014).

[26] D. Gudkowa, *Oszustwa internetowe oraz jak się przed nimi bronić: poradnik dla opornych*, securelist.com (access: 11.10.2016). Cf. https://security.intuit.com/phishing (access: 8.09.2016).

faster than in the real world; increasingly more frequently we do a few things at a time, e.g. we work, read emails, check the news, chat with friends on social networking sites, listen to music, etc., which distracts and relaxes vigilance[27].

It is worth noting that according to the international anti-phishing organisation APWG[28] in the first half of 2013 about 30 thousand webpages were discovered, which were designed to acquire our data illegally. In the first half of 2014 their number increased to over 40 thousand. The situation is similar in the case of illegal phishing email campaigns[29].

At present there is a number of ways of protection against phishing; some of them are technological innovations, others are web portals supporting their users and trailing phishers, but the best is good practice and advice offered by various subjects supporting the combat on phishing. It is worth noting that absolute protection against phishing is impossible unless we resign from online banking and the use of payment cards, which seems hardly possible these days. A few years ago the Polish Bank Association proposed guidelines for the card holders in order not to become the victim of phishing when carrying out online transactions. Following them will undoubtedly limit a number of crimes committed by those who try to interfere with the flow of electronic money[30]. The guidelines are as follows: remember that banks never ask their customers about their passwords and other confidential data and never request their updating. Banks never attach to their emails links to transaction processing webpages; letters, emails and phone calls concerning such matters are to be treated as an attempt to swindle confidential information. Do not reply to them, providing your confidential data. Contact your bank immediately and inform it about it. Check on your bank's webpage how it protects its website. Follow the security procedures published there each time you log in. Whenever irregularities occur, contact the bank. The computer or

[27] Ibid.

[28] Anti-Phishing Working Group.

[29] *Phishing: stracisz nie tylko pieniądze. Twój smartfon zostanie żołnierzem cybermafii*, www.serwisy.gazetaprawna.pl (access: 28.02.2016). See also an APWG (Phishing Activity Trends Report) report from 2014 and next eg. 2016 (July–September) at: www.antiphishing.org (access: 27.02.2016).

[30] www.abp (access: 2.03.2016).

phone with online connection must have continuously updated antivirus software installed. It is also necessary to activate essential modules in the security package, such as antivirus software, email scanner or firewall. Switching them off to reduce the system load is a mistake frequently made. Make online payments only from "reliable computers" and not from the computers accessible by general public, such as those in internet cafes or the university. Contact your internet provider to make sure that their services are distributed via secure channels. Pay careful attention to the quality and security of online services provided by your provider. If you have any doubts, ask them about the quality of security which they offer. Install only legal software on your computer. The software from unknown sources, including that downloaded with the use of Peer-to-Peer (P2P) applications, may be prepared by hackers and may include viruses or other types of malware. It is recommended that the computer is periodically scanned, especially before the bank's webpage is accessed and any transaction is conducted. The detection efficiency of most antivirus programmes when their antivirus monitors are on is the same as that of antivirus scanners and a computer does not need to be scanned. However, antivirus monitor's detection of some programmes is lower than that of a scanner, which results in gaps in the security system. Update the operating system and the applications essential for its functioning, e.g. browsers. Hackers are constantly looking for weaknesses in the software, which they subsequently exploit to commit offences. Producers of operating systems and applications publish "patches" which remediate and mitigate their products' vulnerability to attack. Do not open emails and attachments from unknown sources. The attachments often include viruses and software which enable spying your activity. Avoid webpages offering very attractive content or opportunities; especially dangerous are the webpages offering pornographic content. Seemingly innocent pages offering "freeware" may also be very dangerous, because hackers often attach malicious software to them. After logging into the transaction system, do not go away from the computer and after finishing work, log out and close the browser. If unusual messages, requests to reveal personally identifiable information or passwords appear when logging in, notify your bank about it. Do not access your bank's webpage via links in incoming emails. For this purpose use the address which the bank gave you

when signing the contract for opening and running your account. Avoid using the "Bookmarks" (Firefox) or "Favourites" (Internet Explorer), because there are harmful objects which can modify the addresses stored there. Never use search engines to find your bank's login page. The links found in this way may lead to false pages or pages containing viruses. Before logging in, check if the access is safe. Your bank's website's address should begin with "https://" and not "http://". The absence of "s" denotes the absence of data encryption, i.e. your data are transmitted in open text, which exposes you to great danger. Check the validity of the certificate. Before you type in the identifier or login and password, check if the connection with the bank uses encoding. If you find the symbol of a padlock, click it twice to check if the certificate is valid and if it was issued for your bank. If the certificate is invalid, if it was not issued for your bank or if it cannot be verified, do not access the page. Do not reveal to anybody your identifier and password. The identifier is a confidential number assigned by the bank, which you cannot change. Do not write down passwords and change them regularly — ideally once a month, but if the system does not force you to do this, change your password at least once every two months, using a combination of capitals, small letters and digits. Check the dates of your last successful and unsuccessful logging into the system. Use your bank's helpline — you have the right to use it any time if you have any doubts concerning security of the online transactions. Be careful when you reveal your card's number. Do not reveal it to anyone who has called you, even if the caller tells you that there is a problem with computers and asks you for verification. Companies never call to ask for a payment card number. If you have been called, do not reveal your card number if you are not sure if the other person is trustworthy. Do not reply to emails asking for information about your card. Do not reply to emails asking you to access a webpage to verify data, including those concerning the card. Do not reveal the information about your card on webpages which are not safe, e.g. webpages of unknown companies offering brand-name goods at very attractive prices. Before you fill in your card number in the form on a webpage, make sure that the data are properly secured (i.e. the page's address begins with https and the webpage has appropriate certificates — this information is provided by the browser at the status bar at the bottom). Do not write the

PIN code on the card and do not keep it together with the card. Not only is it illegal, but also if your card is stolen and used to carry out a transaction, the bank will not be obliged to compensate for the loss. Protect your card's number and other confidential codes which facilitate carrying out a transaction, e.g. PIN, CVV2 or CVC2 — the last three digits of the number on the strip with your signature on the other side of the card. Perpetrators may acquire them, photographing or filming your card with a mobile phone. Do your online shopping in renowned shops. In the case of less-known websites, check their credibility by calling them and verifying their offers, transaction and complaint procedures. Make sure that you are not on a webpage impersonating your bank's/shop's page (similar name and design used to mislead you and swindle your money). Read the shop's regulations, and especially the information concerning the security of transactions. Before carrying out a transaction, make sure that the data are transmitted via a secure connection with the use of SSL/TLS[31] protocol.

The guidelines above may restrict the unwanted access to the card holder's data. Yet, what is to be done when a phishing attack has already taken place? Everyone who cares about security of their money should routinely monitor their transactions. If any discrepancy is detected, this fact should be immediately reported to the card issuer, e.g. the transactions which were not consciously carried out by a card holder or those where the amount of money differs from that actually involved in the transaction. This may help to identify the perpetrator and protect the card holder against loss. If there are more than one transaction of this kind, the card should be deactivated[32].

The discussed crime is a natural consequence of the development of retail payment market involving payment cards. The common use of

[31] Secure Socket Layer/Transport Layer Security.

[32] According to Polish law, the card issuer assumes responsibility for all the transactions carried out by the card from the moment its loss is reported. According to the act on payment services, maximum responsibility of the card holder (for the transactions carried out before its loss is reported) amounts to the equivalent of 150 euro and 50 euro in the case of contactless payment transactions on condition that the contract on issuing the card and the card's regulations, which constitute the contract's integral part, are abided by. The Act on payment services of 19 August 2011 with subsequent amendments (Journal of Laws, Dz.U. 2011 no. 199 item 1175).

electronic money and the increasing living standards encourage perpetrators, who are looking for technologically weakly protected markets. Not all known crime involving payment cards has reached alarming proportions in Poland, but due to the ongoing technological development their increase should be reasonably expected.

Under the influence of European law, including the SEPA project[33], the magnetic strip — now considered a technologically weak protective device — is being replaced by a microprocessor. Undoubtedly, a much better solution is the authorisation of transaction with the PIN code[34]. Even though this solution has been in use for many years[35], many POS (Point of Sale) terminals still accept the magnetic strip, which causes the risk discussed above. Apart from legal regulations, combating the crime targeting payment cards should also involve the development of security technology. Unfortunately, the latter is inevitably accompanied by the development of technology facilitating crime, therefore good practice in using the payment cards and following the guidelines recommended by financial institutions or card issuers are of great significance. The crime involving payment cards is very complex and dynamic, while a great

[33] Single Euro Payments Area (SEPA) is the area where citizens, entrepreneurs and other subjects may make cashless euro payments within the European Union between EU countries and within them following the same rules and on the same conditions. At present SEPA regulations function in Poland as a voluntary agreement of banks but from 1 November 2016 on the basis of the provisions of the Regulation SEPA (Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009) every bank will be obliged to make payments in euro according to SEPA regulations. Cf. the document, *Kilka słów o ramach funkcjonowania kart płatniczych SEPA*, www.sepapolska.pl (access: 27.02.2016). The SEPA Instant Credit Transfer Scheme Rulebook, https://www.europeanpaymentscouncil.eu (access: 5.12.2016).

[34] Personal Identification Number.

[35] The EMV standard was created in the mid-1990s and since then it has been gradually introduced in the form of a chip in payment cards. At present, the cards with only a magnetic strip are practically out of circulation. EMV comes from the first letters of the cards: Europay, MasterCard, Visa; it is an international standard responsible for authorisation of card payments in shops and service points. The usual procedure involves a combination of the chip and PIN code. The card holder's identity is verified by providing the PIN code. www.kortaccept.se (access: 27.02.2016).

number of places where cards are used is responsible for the fact that the crime evolves with the application of new technology.

An important aspect of the crime focusing on payment cards is its international character; its prosecution also involves international co-operation.

Progress in the technology of online and electronic payment is so fast that it is not always carefully thought out and tested. Therefore, not all new functions actually benefit the users. Knowing the characteristics and types of offences as well as following the rules of payment card use offer a chance of defence against the crime. It is also important that the users may decide what technology they want to use. In Poland until recently the so-called "new technologies", which include the option of contactless payment[36], were automatically added, while a card holder had no possibility of deactivating it. Now many banks offer this option. To restrict the scale of crime committed with the use of payment cards, banks have recently begun to introduce biometric technologies involving scanning and verification of fingerprints or the pattern of blood vessels under the skin of fingers. Hopefully, the proposed solutions will increase the security of transactions and will hinder illegal acquisition of personally identifiable information.

Summary

It is a commonplace that the internet is one of the most powerful tools at the disposal of contemporary societies; it is also one of the most dynamically developing ways of information transfer. Access to information is the most important and desirable aim of human aspirations. The internet is still developing very dynamically, thus defying any efforts at determining the limits of its advancement; it creates infinite opportunities in various areas, while its great potential affects all aspects of human existence. For years the internet has also been the medium for financial transactions involving electronically regulated cash flow. Many of these transactions are carried out with the use of payment cards, which for many people constitute an obvious alternative to traditional transactions involving cash. The history of payment cards elsewhere in the world goes back to the

[36] Contactless payment, NFC (Near Field Communication) payment. Cf. the report of the Office of the Financial Supervision Authority, *Analiza poziomu bezpieczeństwa kart zbliżeniowych z punktu widzenia ich posiadaczy*, Warsaw 24 June 2013, www.knf.gov.pl (access: 5.05.2016).

beginning of the previous century, but in Poland they came into use much later, i.e. in the mid-1990s. The development of the internet, and especially the speed of data transfer which it offers, have greatly facilitated the transactions involving payment cards. This fact poses a question concerning the security of such transactions. The popular and universal character of online payments, not necessarily with the use of payment cards, resulted in the emergence of crime involving identity theft and conducting illegal transactions.

Keywords: crime, electronic payment devices, phishing, skimming, SEPA.