DOI: 10.5604/01.3001.0014.3291 ASEJ ISSN: 2543-9103 ISSN: 2543-411X (online)

# Threats of identity theft in cyberspace - case study

Wojciech Jakubiec[1]

[1]Department of Law and Social Science Bielsko-Biala School of Finance and Law
*Cz. Tańskiego 5, 43-300 Bielsko-Biała* – Poland

***Abstract*— We can certainly say that identity theft on the Internet is a growing criminal phenomenon. The perpetrators' actions are most often motivated by financial gain. The article discusses selected issues concerning so-called Internet fraudsters. In particular, it draws attention to the actions taken in cyberspace and the risks that accompany such decisions. I point out that the most vulnerable to identity theft are elderly people who do not even know basic security procedures. The article not only draws attention to the dangers themselves but also describes the way criminals act. It also states that in order to minimize the risks faced by network users, attention should be paid to training needs related to with security in cyberspace. An important aspect of this is to draw attention to the risks associated with personal data improperly stored on electronic media integrated into the Internet.**

**Index Terms — cyber security, loss of documents, identity theft, personal security**

## I. INTRODUCTION

This publication aims at presenting the growing problem of identity theft in cyberspace, to which customers of companies providing small amounts of financial support are most often exposed. Especially the elderly who do not know the mechanisms used by perpetrators of Internet crimes (Nastuła 2020 p. 4). The article illustrates the risk of placing a scanned document on the Internet. It draws attention to the real consequences of identity theft.

A threat that has emerged with the development of Internet services is undoubtedly the ease of obtaining short-term financial support - via available Internet networks. The danger lies in the illegal use of documents (identity card or passport) to obtain financial support. Here it should be noted that each of these documents is a so-called database. It contains not only basic information such as first name or first and last names but also more detailed data such as: surname at birth, first names of parents, date and place of birth, sex, copied image of the holder, number PESEL number, citizenship. Therefore, the loss of even a copy of a document will cause many difficulties for its holder. What often happens on the Internet. Certainly, it can be assumed that the theft of a copy of such a document is aimed at obtaining financial support (Widiyanti, Hendrawaty 2019)

The "identity card" document on the territory of Poland was created in the times of the Second Polish Republic. The first one served as a passport and was mainly used to cross the border. It was a piece of paper folded in half containing a photograph, data on reading and writing skills, religion and a short description. At the same time, the identity of persons was established on the basis of this document. This made it possible to keep proper records and increased the internal security of the state. The document was issued against payment and only to interested persons. The obligation to have an identity card in Poland was first introduced by the Germans. This obligation was maintained after the Second World War, when for lack of it one could face penal sanctions. Initially it took the form of a green booklet, in the 1970s additional document security measures were introduced, and only in 2001 it took the form of a plastic card with modern security features. Today's identity card has many modern security features. Such as: variable level of engraving, kinegram, microprint, CLI effect, kineprint effect, latent drawing, optically variable ink. All these security features are designed to protect the document from forgery and illegal use. A wide range of modern security features is to guarantee security and prevent forgery of the document. This is why the current legal situation, which allows the legal use of a document scanner, poses a threat in terms of identity theft, which often takes place when credit is being stolen (Borokhvostov 2019 p. 59) The perpetrators no longer need to forge a document and it is enough to obtain a copy of it, which is also much easier to rework, e.g. by changing a photograph.

## II. DISCUSSION

Short-term loans are usually offered by quasibank institutions. As a rule, they do not operate on the basis of the Banking Law Act and do not have to meet certain conditions. In order to obtain such a credit or loan, it is enough to have access to the Internet, know basic personal data and scan your ID card or passport. The application for a short-term credit

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 24, No 2 (2020), 5 pages
DOI: 10.5604/01.3001.0014.3291
Received: 15.05.2020; Accepted: 23.06.2020

Regular research paper: Published 06.2020
Corresponding author's e-mail: w.jakubiec@poczta.fm

agreement is usually completed by means of an electronic form. The action boils down to creating a customer profile in one of the databases belonging to quasibank companies. What happens without an actual meeting with the customer, everything is done via an IT network.

Despite the fact that these institutions do not operate on the basis of banking law, they are obliged to conclude a fully reliable contract. So the customer is verified. The first and essential activity is to establish identity on the basis of Polish law. To establish the identity, you need an identity card or passport. Quasibank companies have allowed such verification also via the Internet (this may require additional authorisation. e.g. transfer of a symbolic amount from the bank account of the same person). This involves a high risk. This is done in such a way that the applicant enters the data in the application (form) together with the details of the document and in some cases sends a scan of the document to establish identity. Of course, in order to obtain financial support even in the short term, it is necessary to meet the other requirements as well as to indicate income in order to establish creditworthiness, i.e. to verify the economic situation of the future borrower (in the case of not large amounts, no certificate of employment and income earned on this account or a decision to grant a pension is required). Other data that are verified are the situation concerning other financial liabilities, such as the determination of the costs of running the household, repayment of other liabilities resulting from the current debt or financial arrears, which have a direct impact on the ability to fulfil the concluded contract within the deadline set in the schedule. The issue of financial support payment is also important. It may take the form of: payment by postal order or transfer to a designated bank account and payment from the cash register. What usually happens when a representative of the company pays out money to the customer.

The "Report on the study of short-term loan agreement templates" published on the Internet defines a short-term loan, the so-called "momentum". Short-term loans, so called "momentum" belong to the group of micro-loans, which means that the amount of the loan granted to the consumer on their basis is relatively small, from PLN 50 to PLN 4,000, for a short period of time from 7 to 60 days, and it is usually repaid in one instalment. Loans of this type are offered mainly by non-banking entities, much less frequently by banks. A characteristic feature of this product is its relatively easy availability. The basic method of distribution and conclusion of a loan agreement of the "momentary" type are electronic channels: through a website, a phone, including more and more often by means of specially dedicated mobile applications, or by means of SMS exchange. Definitely less often an agreement can be concluded directly at the entrepreneur's branch. Websites enable the consumer to submit an application usually after establishing an individual customer profile. They are also equipped with loan cost simulators, thanks to which the consumer can use special sliders to set the expected parameters of the loan, such as its amount and term of repayment, as well as get acquainted with the loan costs calculated by the simulator: the total cost of the loan, the total amount payable and the actual annual interest rate (RRSO). All entrepreneurs offering loan agreements covered by the survey have websites through which you can apply for a loan. ("Report from the study of short-term loan contract templates").

Establishing one's identity is unequivocally understood and boils down to the basic aspect, which is to confirm that the person in possession of a given document (or a copy thereof) is that person. In this particular case, it is a guarantee that the credit will not be taken out on another person.

The very issue of copying a document raises many doubts. Objections to such banking practices appeared at the end of last year. In the opinion of Bielak-Jomaa, the Inspector General for the Protection of Personal Data, published on the office's website, she stated that the time has come to discuss the advisability of copying or scanning identity cards and other documents confirming our identity. The bank's right to collect customer data is not synonymous with the right to copy them.

The Polish Bank Association also pays attention to protecting our own identity. We should be aware that not only losing an identity card but also its temporary loss may contribute to our problems in the future. Often criminals do not need the original document - all they need is a copy of it or data from which they can make replicas of the document. So we should not leave the documents unattended or as a pledge e.g. in a rental shop. Documents or data derived from them can be used in many situations, and the imagination and scenarios of criminals' actions in this area are extremely developed. We should also be careful where we place information about us and what type of data it is. Criminals monitor portals for the data they need to commit a crime. Often they also extort them by, for example, fake job offers, offers of intermediation or impersonating e-commerce entities. Criminals who have our personal data may, for example, extort a loan in our name or take a momentary loan from a loan company. Otherwise, a stolen identity may be used to run a fake business or to extort goods from other entrepreneurs, as well as money from customers under the pretext of providing the service. Criminals can also rent and sell a car in our name or sign several contracts with a telecommunications operator, receiving branded mobile phones in return. Problems related to the use of our identity may reach us after several months or even years. Unfortunately, proving a crime is extremely burdensome and lengthy. A very important activity after losing an identity document is to reserve it. When you reserve the proof, you report it to the System with restricted documents. In a few minutes the information will reach all banks in Poland, the Polish Post Office and mobile phone operators. Your identity is safe and no one will be able to confirm it on the basis of your document. For the prudent, it is also worth considering launching the BIK Alert service, which will inform us about attempts to use our identity for credit purposes. (Barbrich 2020, p. 21), (ZBP Cyberbezpieczny wallet - report).

Making a copy of your ID card or passport is the easiest way to obtain personal data. Placing a scan of the document in cyberspace also makes it possible to obtain this copy by unauthorized persons. Whether this will take place in case of hacking into a particular Internet network (company or other organization), a particular computer or hacking into the mail

account from which the scanned document was sent. Different types of intrusions taking place in cyberspace often do not evoke similar feelings as for example the theft of a document, which often happens to ordinary citizens who do not have sufficient knowledge of what to do in this case. The issue of stealing a document turns out to be simple. Everyone knows that such a fact should be reported and the document should be withheld. However, in the case of theft of a scanned identity card or passport, the original owner is often unaware that a cash or instalment loan agreement can be made via a copy of the document. If this happens, the owner of the document is not aware of such an event. He is completely unaware of it. The conclusion of the contract is very fast. Companies providing financial support verify applications very quickly and in case of acceptance of the application, the funds are paid out. The agreement and its attachments are sent to the indicated address, often untrue, and only after the period when the borrower fails to fulfil the agreement, most often defaulting on payment of instalments, the institution providing financial support contacts the owner of the document or it takes place even later after court decisions concerning enforcement and seizure of property. In such a case, the victim is in a difficult and complicated situation, the explanation of which takes a lot of time. During this time the victim is in a difficult economic situation. He cannot take out loans because he is a debtor. The perpetrator has directed his first suspicions at him, which has led to a disguise of the crime at least in the first period.

Therefore education should play a very important role. Its dynamics should match the services offered in cyberspace in terms of financial support. Here the Association of Polish Banks in its own publications rightly draws attention. Europeans believe that the risk of becoming a victim of a cyber-attack is increasing, even though potentially dangerous situations do not happen to us often. Compared to other European Union countries, Poland performs quite well in the opinion of customers - 23% of respondents from Poland replied that they experienced attempts to defraud private information (including access to a computer and internet banking) via e-mails and phones. The highest number of attempts to extort confidential information is recorded by Danish residents (66%)(source), which does not necessarily indicate that the highest number of attacks is carried out in this country. Danes feel that they are the best educated on cyber security in Europe, so they are more likely to identify fraudulent attempts. In Finland, a country where 93% of the population uses e-banking, a third say they were in a situation that potentially threatened online security. In Poland this percentage is 38% (Barbrich 2018, p. 13), (ZBP Cyberbezpieczny portfolios - report).

Using the network means contact with many services and mechanisms that a typical user is not aware of. The Internet, which can be observed on a daily basis (websites and applications), is only a way of presenting content. Much of the cyberspace remains inaccessible to us. With the spread of Internet services to almost all areas of life, the global network is no longer a sphere of communication specialists, it has become a universal tool, used by the average user for work, study and entertainment. During the 22nd Secure 2018 conference, organized by Scientific and Academic Computer Network (so called: NASK and CERT Polska) in Warsaw on October 23-24, 2018, it was stated that over 90 percent of technological threats do not concern network servers, but consumer devices connected to the Internet and end user applications. (Rylski 2018, p. 82), (Technological threats)].

The most common failings in the precautions to be taken by Internet users include the absence of antivirus programs, simple passwords and access logins to different services and sometimes they are the same or very similar. In addition to this narrow directory, it should be noted that it is important to store the data stored on the network securely for proper protection. It is a breach of security to leave messages with data and attachments. Because in the case of breaking the security features of a mail account, the perpetrator will additionally obtain the data that enable the conclusion of e.g. a credit agreement - identity theft will occur. For the proper security of data storage, the aspect of data encryption with the use of appropriate programs designed for data encryption is important. The current programs guarantee a safe scope of data encryption. Because even in case of data theft, the perpetrator will not be able to read the data.

Most often the victims of identity theft are ordinary users. Unfortunately, they do not have proper knowledge how to defend themselves against identity theft. However, attacks aimed at individual users do not consist in classical breaking through security measures, i.e. so-called computer hacking. The most frequent method will be phishing attacks. Rylski rightly pointed out that phishing attacks are a socio-technical method. A significant part of attacks in cyberspace does not consist in active breaking of security or engaging malicious software. On the other hand, there is a rapidly growing number of socio-technical attacks that use ignorance, inattention or routine behavior of the user to persuade him to take specific actions that compromise the security of the device or account. A common form of Internet scams is phishing (a combination of the words “password harvesting” and “fishing”). The perpetrators carefully prepare an “encouragement”, which can be for example a website, an e-mail or a simple message sent via instant messenger. A specific feature of the phishing technique is to create an impression of rush, a necessity to take immediate action, which usually boils down to clicking on the proposed link (Rylski 2018, p. 85), Technological threats, (sp.zsprzinia.pl).

The risk of identity theft in the form of a copy of an identity card or passport can be divided into two groups, depending on the perpetrator’s method of operation - way of obtaining a copy of the document.

The first category includes persons who have lost a copy of a document as a result of deliberate action by third parties who have lawfully acquired possession of a copy of the document. These will be persons who possess a copy of the document, with the consent of the owner. They shall act expeditiously by deliberately disposing of that copy or making it available to unauthorised persons. Defining this action seems quite simple. The perpetrators will be the persons making the data available, most often for financial gain. The actions taken by these persons

will be conscious and carried out against the will of the owners of the documents, in violation of internal regulations governing safe collection and storage of data.

The second category will be persons who lost their ID card scan as a result of criminal activity consisting in hacking into the Internet and data theft. In this case, there is not only a breach of the security of the IT network but also a breach of the security of individual Internet accounts, such as hacking a mailbox. Breaks into computer networks are a huge threat for both ordinary users and owners of computer networks. There are many types of Internet crime. One of the most common form of this crime is taking over an account on Internet platforms used to sell various types of goods. The perpetrator, after taking over such an account, has the opportunity to act as the account owner. Of course he does it against his will and his action is aimed at achieving financial benefits. The perpetrator's modus operandi has common features for this type of crime. I take over the account on the platform and the offender undertakes a fictitious sale of goods using the data of the real account owner. Having previously been able to administer it changes the way of paying for the goods. This is usually another bank account opened for another person, to which the perpetrator has full access. What comes down to having the data to manage electronic banking launched for a particular bank account. The common denominator of such crimes will be impersonation by the perpetrator of the account owner - I mask my own identity. The second identical component of the crime will be the need for the perpetrator to organize ways of withdrawing funds. What is connected with the necessity of launching a financial service - it is not possible without using the data contained in the identity card or passport together with the data of this document such as the name of the issuing authority, its series and expiry date.

As it appears from the situations described, the victim is most often found out after the fact when he fell victim to a crime. The development of the Internet and related financial services creates an excellent field for criminals. Not only is there an increase in Internet crime but also the transfer of the activities of criminal groups to the network. At the same time as the development of financial services, criminals have improved their methods of operation in parallel with the implementation of network (financial) service safeguards. In December 2015, at a conference organized at the Police Headquarters in Warsaw, it was announced that in 2014, there were attempts to defraud, using stolen identities, loans totalling PLN 400 million.

A spectacular example of this type of crime was the scamming of the amount of 6.5 million PLN from the bank by a resident of Krakow using a document with a different identity. In Warsaw, a man using someone else's ID card tried to withdraw 800 thousand PLN from the bank. Whereas 80 thousand zlotys was lost by an inhabitant of Stalowa Wola using the "grandson or granddaughter" method. In December, pensioners from Warsaw's Wola uncritically spent 500 thousand zlotys on fraudsters. As far as counterfeiting of documents is concerned, in 2012 there were over 29.5 thousand such incidents.

In 2014, the police recorded 13 316 cases of using another person's document and 30 392 crimes related to document forgery and 42 880 cyber-crimes. The first nine months of 2015 saw an increase by as much as 110 percent in the number of reported bank frauds (2.5 thousand in 2014, compared to 4 thousand in 2015) (Szafrański, 2016), (Theft of personal data growing threat biznes.interia.pl).

## III. CONCLUSION

Modern technologies allow criminals to be more creative. It is also a growing social problem. The police also have achievements in combating this type of crime. In the last days of December 2015, a criminal group involved in the extortion of cash credits on the basis of stolen data was reported to have broken up.

Suspects were extorting data from people to whom they first offered fictitious employment and then robbed it from documents and data to bank accounts. Five people were detained in this case, residents of Dolnośląskie Province, one of whom was a minor. On the basis of the obtained data and documents, the perpetrators were defrauding loans, and the injured people found out about the fact that they had become the so-called poles after receiving a call to repay the loans. Such fraud is punishable by up to 8 years' imprisonment. (Szafrański, 2016), (Theft of personal data growing threat, biznes.interia.pl)

In the current situation, the development of financial services available to all Internet users is observed. A financial institution outstrips the speed and availability of obtaining financial support. With small amounts, the procedures are very simplified. An ordinary customer, especially a senior citizen, does not know the procedures that allow him/her to protect his/her identity on the Internet. Most often, the average customer receives signals that he or she must have a telephone and e-mail to communicate with the credit institution. Unfortunately, a significant proportion of citizens are not aware of the risk of identity theft in this way. These people do not often use security features, current anti-virus and other programs to protect individual computers. Therefore, it is worthwhile to discuss the implementation of new legal regulations that will make it impossible to conclude credit agreements at least without a single identification by a representative of the institution providing financial support. What will actually affect the security of identity theft, as the customer will be at least as familiar with the basic security rules for protecting his or her identity and stealing data on the Internet.

## IV. REFERENCES

Borokhvostov , V., Skurinevska , L. and Lutsik, J. (2019) "Information and financial technologies of hybrid wars: methodological approaches to the analysis of the content, occurrence, response and prevention", *Journal of Scientific Papers «Social development and Security»*, 9(6), pp. 56 -. doi: 10.33445/sds.2019.9.6.5.

Nastuła, A. (2020) "Dilemmas related to the functioning and growth of Darknet and the Onion Router network", *Journal of Scientific Papers «Social development and Security»*, 10(2), pp. 3-10. doi: 10.33445/sds.2020.10.2.1.

Widiyanti, M.; Hendrawaty, E.; , D. 2019. Antecedents of economic convergence in asean countries: foreign direct investment, trade, government size, population and economic convergence, *Journal of Security and Sustainability Issues* 9(2): 431-445. https://doi.org/10.9770/jssi.2019.9.2(6)

Raport z badania wzorców umownych pożyczek krótkoterminowych, fedaercja-konsumentow.org.pl,

Ławrowski P., (2016), *Uważaj komu dajesz dowód osobisty takie mogą być tego konsekwencję*, finanse.wp.pl,

Barbrich P. et all. (2020), Raport ZBP *Cyberbezpieczny portfel*, Edycja III, www.zbp.pl,

Barbrich P. et. all, (2018), Raport ZBP *Cyberbezpieczny portfel*, www.zbp.pl,

Rylski A., (2018), *Zagrożenia technologiczne*, sp.zsprzeginia.pl,

Szafrański, B. (2016), Kradzież danych osobowych narastające zagrożenie, biznes.interia.pl,

*Kopiowanie dokumentów tożsamości rodzi zagrożenie dla bezpieczeństwa danych*, archiwum.giodo.gov.pl.