IDENTITY THEFT: A MODERN "GATEWAY" CRIME

*Jana Ilieva , page 93-102

March, 2017; 2 (1)

It's so very simple to be anyone you please, on any given morning you awake."

James Rinaldo Jackson

ABSTRACT

Each year, millions of people are becoming victim of identity theft - a modern type of crime that consists of abuse of one's identity in order to acquire property gain. The growing trend of this type of crime has stimulated many authors to qualify it as "epidemic" or "national crisis", asking the national jurisdictions to react with taking over of appropriate legal measures and regulations, which do not pass by the Republic of Macedonia. However, the concern and the responsibility for preserving the identity and for protection of the personal data, remains in the hands of individuals and their self-awareness and knowledge of which depends on whether and to what extent, they will be ready to protect their identity.

Key words: identity theft, data protection, privacy, Republic of Macedonia, crime

***Assoc. Prof. Jana Ilieva PhD**
University of Tourism and Management, Republic of Macedonia

e-mail:
j.ilieva@utms.edu.mk

Article type:
1.02 General scientific articles

UDK: 343.71:347.18(497.7)

Date of received:
November 25, 2016

Date of acceptance:
February 5, 2017

Declaration of interest:
The author reported no conflict of interest related to this article.

1. INTRODUCTION

The virtual world is becoming an important part of the peoples' work and personal life, their organization and the modern social community. It creates and promotes continuous revolutionizing of the information technology. This is particularly evident in the last few decades, which are marked with versatile connectivity of information technologies achievements in telecommunications with the material operations of the people. Computer Technologies growing rapidly has become an indispensable part of modern life. (Solak and Topalogly, 2015). With the emergence and spread of the Internet - the global information and communications network the fundamental infrastructure of a virtual world is being developed and this connects and engages people, integrates economies and spreads the culture and education of the mankind.

Advancements in information and communication technologies (ICT) inextricably bring new threats to the end-users and society (Luiijf, 2014)

The spread of information technology in the world, however, has a negative side: it opens the door to antisocial and criminal behavior in a way that it was impossible, so far. Computer systems offer new and highly sophisticated opportunities for breaking the law, and create a potential to commit traditional types of crimes in non-traditional ways. Especially it is the people's privacy that is hit the most, hence the scope of its protection moves from material and spatial to the field of information and communication protection. Lately, the dominant role of this information - communications privacy is being emphasized, as well as ensuring that in the globalization process, individuals will realize their material and other interests, while keeping to themselves what they do not want to share with other people.

The rapid IT development set new challenges for the law. These challenges do not fit within the traditional legal categories, but lately, they appear for example in criminal law, intellectual property law, contract law, etc. One such challenge the phenomenon of identity theft has gained widespread media coverage and has grown to be a major concern for payment providers and consumers alike. (Kahn & Zegara, 2015). Due to the technological advancements and the almost ubiquitous use of computers and the Internet, identity theft is a crime that can occur practically anywhere. (Farina, 2015)

It is a crime that consists of unlawful seizure and personal data abuse through which a person is identified (such as Social security number, Credit card no. etc.), in order to gain illegal profit and / or the realization of other criminal purposes. According to the Identity Theft Assumption and Deterrence Act of 1998 (ITADA), the United States Department of Justice defines the act of identity theft as: knowingly transfer[ing] or us[ing], without lawful authority, any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal Law, or that constitutes a felony under any applicable State or local law. (Morris, Kercher and Johnson, 2006).

Or with other words - Identity theft is stealing someone's name and reputation for attaining financial gain. Someone else's identity will allow the criminal to obtain a false identity and then benefit in his own favour at the expense of the person whose identity is stolen. For example - taking bank loan with other name, buying an apartment or car with someone else's funds. In all genuine cases, this type of crime is carried out without the consent of the person whose identity has been usurped. After collecting the personal information of a victim, the attacker can create a fake identity to impersonate this victim and cheat the victim's friends in order to destroy the trust relationships on the on-line social networking sites (He, Chen et al., 2014).

Most often, the perpetrators of this type of crime acquire personal information through access to personal documents or information that will lead to the key attributes of one's identity that will enable its abuse. These information are: identification number, credit card number, passport number, etc. All these information in today's age of IT - communication expansion, become easily accessible for everyone. Thus, if ever personal data were stored in dusty archives, now they can be easily obtained from certain data basis (proprietary data services), or become widely available online. Social networks (Facebook, Twitter, etc.) that operate in a manner of creating user profiles where people register by entering personal data into mandatory and voluntary fields - widely available, is the best food for this type criminals.

The mere fact that they became holders of alien identity has opened the door to criminals to carry out a number of criminal activities that are difficult to detect.

Although, as mentioned, the main goal in this type of crime is acquiring financial gain, often, criminals steal someone's identity to escape from incrimination. False identities thus, can be used for illegal immigration, espionage and terrorism, in unlimited occasions

In the past few years, this type of crime has become a serious threat to all and everyone and fastest growing financial crime in the world. It is assumed that every 79 seconds, someone's identity has been stolen, in the world. In 2015, the FTC received over 490,000 consumer complaints about identity theft, representing a 47 percent increase over the prior year, and the Department of Justice estimates that 17.6 million Americans were victims of identity theft in 2014. (Federal Trade Commission, 2016)

The upward trend of this crime prompted many authors to refer to as "epidemic" or "national crisis." Failure to authenticate equals cybercrime. This is the sole reason for the world's most prolific criminal activity and it is a byproduct of the creation of the Internet and the ensuing 'electronification' of our world. (Edwards, 2014)

2. HISTORY OF IDENTITY THEFT

It is often perceived that identity theft is a modern kind of crime that occurs parallelly with the IT development, especially in the past few years, however, the appearance of this type of crime occurs long time back, with the introduction of a social security number in late 1936. When was the first time, the US authorities have introduced this number, their aim was to record earnings of each employee and provide flow in the pension fund. It took a long time to convince the mass that this number is not a national identity document. For this reason, it was added a legend to the bottom of the card reading "FOR SOCIAL SECURITY PURPOSES - NOT FOR IDENTIFICATION. Unfortunately, that was not the case.

In 1961, the Federal Agency for civil servants began to use this number as identification for all employees at the federal level. Next year, the Public Revenue Office started to use this number as an identification number for all taxpayers. Law on tax reform of 1976 gave the power of states to use this number in their programs for state aid, driving licenses, vehicle registration and taxation. Over time, this issue has become universal means of identification. Soon this number

became identifier for driving licenses, tax returns, medical records, enrollment in college, banking and credit and many other purposes.

So, over the time, the Social Security number became universally recognized as the US citizens' "gateway" to personal and financial information. However, when President Franklin Delano Roosevelt signed the Social Security Act in 1935, he was unable to foreseen the future of the social security number and its possible connection with fraud and crime. Within a year, the first social insurance cards were distributed to the employees and not much later the first abuse of these cards appeared. Hilda Schroeder Vitcher is the first victim of identity theft long before the abuse of credit and credit cards occurred. Her social security number was the most used and the most abused number ever issued.

In 1938, the manufacturer of wallets "Ferre" from Lockport, NY, came toidea to put a copy of the social security card in every manufactured wallet as a marketing trick, and among other things, to show that these cards could very easily "fit in" the wallets. The CEO decided to use a copy of the actual card, belonging to his secretary Hilda Schroeder Vicher but with "specimen" label in red colour placed diagonally. Thousands of these wallets were immediately sold across the country. Each card contained the social insurance number with Ms. Vicher facsimile. And it took a short time to abuse the number. Almost thousands of people started to use it and up to 1943, more than 5,700 people have used this number as it was their own. Although the Social Security Administration announced that it is unacceptable to use somebody else's number, it did not stop the abuse. Administration had to annul the number of Vitcher and give her a new one. However, her first number remained abused through the time, so in 1977 there were 12 registered users of this number. Totally, the Department has detected more than 40,000 people who have used the number of Hilda Schroeder over the years. But how many times that number have been used for fraudulent purposes remained unknown.

Accepting credit cards by the general public prompted many interrelated crimes that have evolved over the years. In the early years of credit card fraud, the perpetrators usually, street thieves and prostitutes stole wallets or purses, in order to abuse them later. Transaction reports, were sent by traders to companies that manage credit card processing by mail, and then to the real owners of cards. This crime has often been carried out and by providing false information and data to the banks, in order to obtain credit cards.

From the above, we may conclude the thesis "identity theft occurs by extension the World Wide Web or Internet" is not entirely true. With the expansion of the global global network, this kind of crime - identity theft becomes the most massive and most widespread, but its occurrence dates long time ago. Popularization of telephone communications has also contributed to the intensification of identity theft. In fact, this kind of crime begins with getting information from telephone scams and searches through the trash bins looking for personal data or other documents that may lead to important financial information. Phone scams have become the easiest way of breaking into someone's identity because victims almost always voluntary, though unwittingly give away their personal information. Most often the victim receives a call for wining a prize which of course is fraud. This information is often seemingly inconspicuous, but refers to the telephone number, date of birth, and sometimes the perpetrators are bold enough to ask for a bank account number.

Another identity theft technique is home or workplace trash search. This way, one can easily obtain bank account number or information, which will lead to one's identity

Besides these seemingly basic ways to access personal data, identity thieves are taking advantage of modern technology to perform this type of crime. Thus, they recently started using devices that can scan and store credit card numbers, in order to carry out their illegal acquisition (technique of so-called "skimming").

However, identity theft is mostly widespread through the Internet communication network. There are number of frauds perpetrated through emails and scams perpetrated through mobile phones where thieves use various tricks so victims can disclose their personal information. "Phishing" format is the best example. In this case, thieves presenting themselves usually as bank officers try to trick the victim to give certain information related to their credit cards, send emails or use pop-up ads, hoping to lure victims to detect certain personal data.

3. TYPES OF IDENTITY THEFT

We are all exposed to the risk of identity theft, since we all possess something very important wanted by the criminals: our name and reputation. The theft of one's life through the intrusion into his personal and financial information, may contribute to long-term consequences for the victim and his family. It is therefore important to identify and enumerate all the important forms in which this wrongdoing occurs.

The first way is called "Account takeover" and is the easiest and simplest way for the perpetrator to reach its goal. That's when the perpetrator possesses someone's credit card or card number or date of expiry and uses them for procurement of services or products.

This is a very successful way of performing this type of crime, because the owner of the credit card usually observes its purchases in the monthly report, or when using the card he will be informed that he has reached the maximum limit hence he has no funds available.

The second type of identity theft is called "Application fraud" or literally "scam." In this type of fraud, the perpetrator should have access to personal data of the victim, such as social security number, full name, address, workplace, the driver's license, birth date, etc.. Certainly not all of them are required to perform the work, but a large part or a combination of two or three of the above can be used for successfully achieving its goal and gaining illegal profit.

4. RISKS AND CHALLENGES IN THE REPUBLIC OF MACEDONIA

The Republic of Macedonia signed the Stabilization and Association Agreement with the European Union, which, inter alia, stipulates the obligation for harmonization of the national legislation with the EU standards and establishment of independent supervisory authorities to control and enforce the application of these standards in practice. The Law on Personal Data Protection based on the EU standards is passed as well as many international documents in this sphere are ratified.

In practice, unlike the other developed countries, the situation in the country is significantly better and calmer. According to numerous experts, particularly in the areas of security in the banking sector, this situation is alike due to the poor initial development of the non-cash payments in the country. However, the proliferation of Internet users and especially the increase in internet commerce, creates fertile ground for development of this type of crime.

The notion "identity theft" does not exist in the Criminal Code of the Republic of Macedonia, but there exist an article 149 - Misuse of personal data which integrates and regulates the identity theft. The respective paragraphs 1 and 2 of this article reads: A person who collects, processes or uses personal data from a citizen without his permission, contrary to the conditions determined by law, shall be punished with a fine, or with imprisonment of up to one year. The punishment from item 1 shall apply to a person who penetrates a computerized information system of personal data, with the intention of using them in order to attain some benefit for himself or for another, or to inflict some harm upon another. When preparing Criminal Action for the crimes of article 149 of the Criminal Code, the following crimes are included as well: Defraud (article 247), Computer fraud (article 251-b), Making, procuring or selling counterfeiting means, etc.

The Law on Personal Data Protection protects the law of the natural persons only thus the legal entities are not grant a privacy protection.

Statistically speaking, if one looks at the figures that have been recorded by the Ministry of Internal Affairs, where numbers clearly show an increase in identity theft or credit cards frauds, although their scope from global aspect, can serve as a school example of a country with a low level of sophisticated crime.

Another reason for the low rate of this crime is the fact that the Republic of Macedonia with the liberalization of the telecommunications market several companies providing Internet connections began to operate. These companies can locate and observe the "crime scene" and thus very easy to find the perpetrators who tried to perform the act over Internet or telephone network.

As for the Republic of Macedonia, it is essential to mention the functioning of the Directorate for Personal Data Protection (established June 22, 2005) which, in order to deliver its primary objectives is in close conjunction and cooperation with the Ministry of Interior. These two institutions for several

years intensively follow the upward trend of identity theft in the country and take appropriate measures. Hence, according to experts in the Directorate, this crime will have its flourishing and largest strike at a time when Macedonia will become a member of the European Union, especially when Macedonia will join the EU monetary union. They believe that Macedonia can expect a significant increase in this type of crime as well as a qualitative leap, a gradual sophistication of this crime. Especially due to the fact that as mentioned, in the country there is still a high degree of confidence in non-cash payments by citizens.

5. CONCLUSION

Globally, this type of crime makes damages in the amount of 6 to 60 billion dollars.

The data indicate that in the area of security, especially in combating and eradication of identity theft in the world we will surely follow upward trends in its growth.

Especially in recent years the global fight against this type of crime has increased mainly in the creation of systems to control the holders of information, control their handling and processing operations and further personal data operations. During this in certain countries data protection is significantly enhanced. There are new measures, new incriminations, special police units, special prosecutors, severe penalties and criminal policy, however, the focus of the struggle for the protection of personal data is not part of the repressive but of the preventive sphere. Hence, the regulations defins clear rules for handling personal data, regulates how they should be treated and if necessary destroyed. They determine who and to what extent can have access to foreign data, and in some cases “permanent record” is required. And what is most important, because they insist on real, not only paper protection, independent state bodies are formed, with an aim to monitor and ensure the achievement of the established rules in real life. Almost everywhere, they are equipped with the necessary resources, sometimes powerful, sometimes less powerful, but never meaningless. In this regard, the data from any of the former Yugoslav repblics show that their personal data protection laws are harmonized with the EU standards, and in the field of supervision and care more than 20 people work, which confirms the commitment of these countries to comply with the European trend of protection. into the

The Republic of Macedonia closely monitors the crime - identity theft. The international legal practice and trends related to the personal data protection and creation and implementation of legislation designed to prevent this type of crime are regularly monitored and promoted. However, as a conclusion it should be noted that the legislation in the virtual world, regardless of its thoroughness and stringency, is insufficient instrument for the protection of people's privacy. It is essential the legal protection to be combined with various forms of self-regulation, self-help techniques and information education. Thus, the care and responsibility for the privacy and personal data protection, is transformed in the hands of individuals, from whose knowledge and awareness depends how far they will be able to keep their private life i.e share with others.

6. BIBLIOGRAPHY

1. B. Z. Hea, C. M. Chenb, Y. P. Sua, H.M. Suna /2014/, A defence scheme against Identity Theft Attack based on multiple social networks, Expert Systems with Applications, Vol. 41, Issue 5, pp. 2345–2352
2. C. Edwards /2014/, Ending identity theft and cyber-crime, Biometric Technology Today, Volume 2014, Issue 2, pp. 9–11
3. C. M. Kahn, J. M. L. Zegarra /2016/, Identity Theft and Consumer Payment Choice: Does Security Really Matter? Journal of Financial Services Research, Vol.50, issue 1, pp.121-159
4. D. Solak & M. Topaloglu /2015/, The Perception Analysis of Cyber Crimes in View of Computer Science Students, Procedia - Social and Behavioral Sciences, Vol. 182, pp. 590-595
5. E. Luiijf /2014/, New and emerging threats of cyber-crime and terrorism, Cyber Crime and Cyber Terrorism Investigator's Handbook, pp. 19-29
6. K. Farina /2015/, Cyber Crime: Identity Theft, International Encyclopedia of the Social & Behavioral Sciences, pp. 633-637
7. R. Morris, G. Kercher and M. Johnson /2006/, Identity Theft: A Research Report, The Crime Victims' Institute Criminal Justice Center Sam Houston State University, http://www.crimevictimsinstitute.org/documents/id_theft_report.pdf, accessed April 4, 2017
8. https://www.ftc.gov/news-events/press-releases/2016/01/ftc-announces-significant-enhancements-identitytheftgov, accessed April 1, 2017