Understanding Identity Theft and Fraud

Boro Merdović[1], Biljana Jovanović[2]

[1]Ministry of Internal Affairs of the Republic of Serbia,
Belgrade Police Directorate
[2]Ministry of Defense of the Republic of Serbia, Belgrade

Article Information[*]

Review Article • UDC: 343.525:004
Volume: 21, Issue: 2, pages: 17–43
Received: May 23, 2024 • Accepted: June 20, 2024
https://doi.org/10.51738/Kpolisa2024.21.2r.17mj

Author Note

Boro Merdović https://orcid.org/0000-0002-6619-5934
Biljana Jovanović https://orcid.org/0009-0007-0952-8978
We have no known conflicts of interest to disclose
Corresponding author: Boro Merdović
E-mail: boro.merdovic@gmail.com

[*] Cite (APA): Merdović, B., and Jovanović, B. (2024). Understanding Identity Theft and Fraud. *Kultura polisa, 21*(2), 17–43, https://doi.org/10.51738/Kpolisa2024.21.2r.17mj

Abstract

Identity theft and identity fraud represent the fastest-growing forms of computer crime, having significant consequences for individuals, corporations, and financial institutions. The advancement of science and technology has endangered personal security and created opportunities for criminals to easily and deceitfully obtain financial benefits or jeopardize the security of corporations and major financial institutions. As a relatively new form of computer crime, identity theft has necessitated the alignment of criminal legislation with the emerging situation. The goal of this paper is to clarify the terminological ambiguities present in this field and highlight the current relevance of the issues related to identity theft and fraud associated with identity theft. By reviewing relevant scientific literature and applying quantitative and qualitative content analysis, comparative analysis, and comparative and historical methods, we will emphasize the importance of clear and precise definitions of identity theft and its legal incrimination. We will point out the different forms of identity theft, the most common ways it occurs, the consequences it causes, and the possibilities for prevention. Research results have shown that identity theft is expanding and that there is a need for harmonizing joint measures at an international level. Also, based on the obtained results, we can conclude that it is necessary to undertake educational measures for vulnerable categories of the population to minimize the consequences of this form of crime. Practical implications of this research indicate the need for developing a greater number of studies in this field, with particular focus on specific forms of identity theft and identity fraud.

Keywords: identity theft, identity fraud, phishing, computer crime

Understanding Identity Theft and Fraud

Introduction

The information era has brought undeniable advantages and many new opportunities, but it has also opened the door to some negative consequences that we must understand and address. The misuse of information technology and computer systems represents a serious problem, especially in the context of computer crime, which can have a broad social impact. This technological development requires appropriate legal and ethical frameworks that will protect user rights and curb abuses. The incrimination and regulation of information technologies are necessary steps in this direction. The rapid growth in the availability of information and communication technologies (ICT) has increased the amount of confidential information at risk, exacerbating the potential for financial and reputational losses for companies and consumers through identity theft and fraud.

Identity theft and fraud related to identity theft have become significant and growing problems worldwide. The internet has enabled the monitoring of communications, analysis of photographs, and access to users' personal data, often without their consent or knowledge. By disclosing their personal data, users contribute to the formation of digital traces that can be misused in various ways. These data can be used to cause harm, extortion, identity theft, and various forms of cybercrime. There is considerable confusion among the public about what is meant by identity theft.

When an average citizen hears the words "identity theft," what typically comes to mind are abuses related to payment cards, whether it involves counterfeiting the cards themselves or their misuse and withdrawal of financial funds from the victim's account. The literature contains many different definitions of identity theft and identity fraud, and popular media often use these terms without attempting to define them. A 2006 study showed that 29% of Canadian consumers agreed with the statement: "I have heard a lot about identity theft, but I'm not sure what it means" (Ipsos-Reid, 2006). However, the reality of identity

theft is more complex. Although sometimes used interchangeably, identity theft and identity fraud are two different things. Identity theft involves stealing a person's personal information (name, social security number, account numbers, etc.), while identity fraud involves the misuse of that information to obtain illicit financial or other benefits. While most frauds involve direct communication between the victim and the perpetrator as a necessary condition, identity theft is unique in that it usually does not involve any contact or relationship between the victim and the perpetrator. In this regard, it is not surprising that there are recommendations to keep identity theft outside the domain of fraud to avoid further conceptual confusion (Beals, DiLiema, & Deevy, 2015).

Identity theft causes losses to victims that can be personal, corporate, or societal. The Fraud Prevention Service based in the United Kingdom (CIFAS, 2010) has reported a drastic increase in cases of identity theft and the resulting financial losses. Although identity theft is a serious form of computer crime, it also represents a much more tedious and prolonged process of compensation and damage elimination, as it takes a lot of time, whether it involves reputation, rating, or businesses of individuals or corporations. Cole and Pontell (2006) have shown in their research that identity theft and fraud related to cybercrime are the fastest-growing in America. However, when analyzed, the situation represents a global phenomenon, and every economy worldwide faces it. When calculating damage and consequences, it is a difficult and tedious process to consider, as the impact of cybercrime and identity theft has far greater effects than can be calculated or imagined (Allison et al., 2005). Given that it represents a global problem, international entities have taken it seriously and undertaken numerous steps to counteract this form of computer crime.

Very few countries have enacted criminal legislation that specifically regulates and sanctions identity theft as a criminal offense, although most countries treat identity theft as a form of unlawful data access, fraud, forgery, copyright infringement, or as an act preceding the commission of another criminal offense. Serbia falls into the latter category. The current criminal legislation of Serbia does not specifically incriminate the act of identity theft through the use of the internet and

social networks. In the event of any form of identity theft, the provisions of the Criminal Code relating to computer fraud, fraud, forgery and misuse of payment cards, unauthorized use of another person's name and other special designations of goods or services are applied. According to data from the Ministry of Internal Affairs of the Republic of Serbia, when it comes to computer crime and cases related to identity theft, more than 90% of cyberattacks are committed in the same way: through phishing campaigns. The most common criminal acts include fraud, criminal acts against sexual freedom involving minors, the display, acquisition, and possession of pornographic material and the exploitation of minors for pornography, stalking, endangering safety, unauthorized access to protected computers, computer networks, and electronic data processing, computer fraud, computer sabotage, and others (E-kapija, 2020). According to the 2020 Identity Fraud Study conducted by Javelin Strategy & Research, there were 13 million cases related to identity theft and associated fraud in 2019, with total damages amounting to $16.9 billion. Prosch (2009) notes that nearly 86 million data breaches occurred in the first quarter of 2008 in the United Kingdom, while the latest Kroll report (2019) showed that 33% of Indian companies reported data abuse and fraud in the last 12 months. The damage caused by identity theft can range from one dollar to trillions. It is not just about the amount but also about the time and costs involved in recovering it.

In the following text, we will attempt to clarify numerous ambiguities and confusion that arise in defining this form of computer crime. The aim of this paper is to answer questions about how identity theft occurs, what factors influence this type of criminal act, what society and individuals can do to prevent identity theft, and what should be done if identity theft occurs. We will also provide recommendations on what should be done to mitigate financial losses and data compromise for individuals and financial institutions. In a separate section, we will highlight the problem of uniformly defining this phenomenon so that successful prevention and suppression measures can be taken at an international level to prevent financial losses and all other consequences arising from identity theft and associated fraud.

Concept and Definition of Identity Theft

Identity theft represents a specific form of computer crime. Computer crime is distinct in many ways compared to other criminal acts, to which legislation until a few years ago had not adequately responded. Among the numerous legal solutions that have been employed, there is a lack of consistency and often not even the minimum required complementarity to successfully prosecute an offense. On the other hand, computer crime has a pronounced transnational dimension – such acts are typically committed in an international context, involving more than one country directly or indirectly (Komlen-Nikolić et al., 2010). Identity theft, as part of computer crime, also lacks an adequate definition that satisfies all stakeholders and legal systems. As previously mentioned, some criminal legislations do not recognize identity theft as a separate criminal offense. Consequently, numerous definitions exist, often representing a significant obstacle in combating this form of crime, which undoubtedly causes numerous consequences for individuals, corporations, and society as a whole.

Mercuri (2006) defined identity theft as "the use of someone's identity without their knowledge to transfer or use information to commit a criminal act that is illegal in the eyes of the law." According to the definition of identity theft provided by Gross & Acquisti, identity theft consists of "the unauthorized use of personal data (date of birth, current residence, phone number, occupation, personal photos) that have become publicly available" (Gross & Acquisti, 2005, p. 80). Identity theft can also be defined as the unauthorized collection, transfer, retention, or use of information relating to a natural or legal person for the purpose of committing further criminal acts such as theft, fraud, and other similar criminal acts through computer systems and networks (Abdul Manap, Abdul Rahim & Taji, 2015, p. 599). Identity theft begins with the acquisition of personal data about a person, carried out without the knowledge and consent of that person, through deception, theft, or fraud, and continues with the use of the collected data to commit criminal acts that in most cases are related

to the acquisition of unlawful property benefits by individuals who misuse the stolen identity (Nikolić – Ristanović & Kostantinović – Vilić, 2018). Roberts considers that identity theft "includes the online appropriation of identity tokens (e.g., email addresses, websites, and combinations of usernames and passwords used to access systems), usually for financial gain" (Roberts, 2008, p. 2).

Identity theft can be viewed in a narrow and broad sense (Đukić, 2017):

- In a narrow sense, it is the illegal procedure of obtaining data about one or more individuals.
- In a broad sense, besides obtaining data about individuals, identity theft includes their use or sale on the black market, transfer to other individuals, and further use for committing other criminal activities.

Identity theft usually consists of three elements: the method of committing the act, the target of the attack, and the motive. The most common modus operandi includes physical methods such as computer theft, illegal removal of data carriers, theft of electronic mail, use of internet search engines and file-sharing systems, hacking attacks. The most common targets of identity theft attacks are identification numbers (e.g., unique citizen number, social security number), personal numbers (passport number, credit or debit card number), usernames, and passwords on various internet accounts. Motives are directed towards obtaining property benefits, concealing someone's true identity, or as a preparatory act for committing another criminal offense.

Numerous international organizations have focused their attention on this type of computer crime precisely because it causes significant damage to individuals and companies worldwide. The UN has defined identity theft as "the misuse of another person's personal data with the intention of fraud" (UN, 2010, p. 12). The Organization for Economic Co-operation and Development (OECD) has also defined identity theft through its strategic documents and the ways in which it can be carried out, thereby contributing to the fight against this form

of crime. According to the OECD, identity theft occurs when a perpetrator obtains, transfers, possesses, or uses personal data of a natural or legal person in an unauthorized manner, with the intention to commit fraud or another crime, using methods such as sending and activating malicious programs, sending deceptive email content, or directing individuals to fake websites that deceive visitors into recording their personal data (OECD, 2007). The Council of Europe has defined identity theft as the misappropriation of another person's identity without their knowledge or consent (Council of Europe, 2013).

By synthesizing most definitions, we conclude that identity theft represents a form of computer crime incriminated by existing legislation, involving fraud through the use of personal and financial data from computers or other devices (smartphones, tablets) obtained via fake emails or websites, with the aim of obtaining unlawful property benefits through misrepresentation.

Risk Factors and Forms of Identity Theft

As with other forms of crime, computer crime is influenced by certain factors that facilitate its manifestation and complexity. These factors can be divided into several categories such as political, economic, social, and technological. Transition and developing countries face political and economic instability, business risks, and disorganized social systems, which provide fertile ground for the growth of computer crime, including identity theft. According to UNHCR reports (2007), numerous migrations occur each year as people from developing or undeveloped countries legally or illegally move to developed countries. This large influx of population increases pressure on the host country, leading to a rise in criminal acts related to identity theft (forgery of IDs, documents, etc.) (Passel, 2006).

Among social factors, habits and communication patterns are often key reasons for the theft of personal data. The level of digital literacy and knowledge of social media usage are crucial in maintaining privacy and security in the virtual environment. Institutions and companies take various precautionary measures to protect their confidential information and maintain the privacy of their users.

Modern individuals spend more time on social media than in the real world (Bjelajac & Filipović, 2020), making them more susceptible to the risk of personal data theft. Virtual interactions become dominant while real, deeper connections diminish. People often care more about the number of likes on their posts than about real relationships with their closest ones (Gupta & Kumar, 2020). This lifestyle makes it easier for criminals to identify potential victims, as users often share their personal information without much thought about the consequences.

Technological factors often include the internet and social networks as well as online shopping. Another significant factor contributing to identity theft is the skills an individual must possess to commit this type of criminal behavior. Generally, computer crime is characterized by the possession of skills related to working with computers and computer networks. In identity theft, these skills are refined over time and become increasingly sophisticated. Required skills typically include information theft, knowledge of financial matters such as loans and card information. Additionally, skills and knowledge about forging watermarks, holograms, magnetic chips, and magnetic strips are needed (Gill, 2017). Besides knowledge, the necessary equipment to perform certain criminal activities is also required.

In addition to practical skills for executing identity theft, certain social and intellectual skills are needed. Depending on the form of identity theft, the perpetrator must possess skills that enable them to remain undetected in a given environment. Research has shown that the first attempt at identity theft often involves entering someone's office and the ability to present oneself as someone else, which is the most challenging part, as they must control their emotions and facial expressions to extract certain information while appearing calm and normal without arousing suspicion (Bourke et al., 2012). They also need to be emotionally stable, with strong self-confidence and certain acting skills, including dressing, manner of speaking, etc. (Copes & Vieraitis, 2012).

In domestic literature, works focusing on the criminogenic factors of identity theft are rare. Discussions about the criminogenic factors of computer crime are more common. One such classification

divides them into exogenous and endogenous factors of computer crime (Vilić, 2017):

- Exogenous criminogenic factors include the speed of information technology development, the number of users, computer illiteracy, confusion and lack of adaptation to new technological changes, lack of awareness about the security risks of using the internet, anonymity (pseudo-anonymity) of users, the mismatch between normative and real, inadequate technical equipment and insufficient knowledge of how devices function, protection of information systems, personnel and material problems of authorities responsible for preventing this form of crime, and lack of education about internet security.
- Endogenous factors are represented by the effect of online disinhibition, which manifests in six points: dissociative anonymity, invisibility, asynchrony, dissociative imagination, solipsistic introjection, and minimizing authority. However, it is also indicated that the desire for abuse and establishing power over others, internet addiction syndrome, and lack of self-control are internal factors leading to the occurrence of computer crime.

One of the most highlighted and research-proven risk factors for identity theft is online shopping. The most common form of victimization was the theft of existing credit card or bank account identity. Those who engage in daily online shopping were more than five times more likely to fall victim to credit card/bank account identity theft than those who do not shop online (Burnes, DeLiema & Langton, 2020).

When discussing identity theft, it most commonly refers to the misuse of data and personal identity for financial gain. However, financial identity theft is just one type of identity crime. In addition to this form, the literature often encounters medical identity theft, child identity theft, abuse and forgery of payment cards, identity theft for tax fraud, selling personal data on the dark web, and similar activities.

Financial identity theft most commonly occurs when new online shopping accounts or new bank accounts are opened in the victim's name. This theft can be executed through various methods, including stealing physical documents, technical manipulations, or accessing data on the victim's computers or mobile devices. Credit card-related identity theft is one of the most prevalent forms of identity theft. In our region, it is also dominant among other forms of computer crime. While microchips in credit cards have supposedly helped curb direct purchase fraud, mobile and online transactions have now taken the lead. Fraud and identity theft where the payment card is not physically used have surged in recent years. Cases where the card is not physically lost or used for payment, yet money is taken from the account, are increasingly common. The victim usually learns of the fraud when they receive a message from the financial institution that a transaction has been made. The money is typically withdrawn somewhere abroad, where the victim most often has never been. One of the terms used in this area of crime and found in both domestic and foreign literature is "carding." Carding has emerged as a significant form of cybercrime encompassing various frauds related to the misuse of payment cards. This practice involves unauthorized use of stolen or forged credit card data for financial gain. The evolution of technology has enabled the expansion and complexity of carding, posing significant challenges to financial security and privacy worldwide (Stojković et al. 2023).

Medical identity theft most commonly occurs in the USA because the health insurance system is designed in such a way that stealing and abusing someone else's data enables the perpetrator to receive healthcare. Medical identity theft occurs when someone uses another person's name, and sometimes other parts of their identity, such as insurance information, without that person's knowledge or consent, to obtain medical services or uses that person's identity information for false claims about medical services (World Privacy Forum, 2024). Medical identity theft is one of the hardest types of identity theft to resolve and can cost much more than financial identity theft. If criminals are treated in the victim's name, incorrect medical records can lead to delayed

treatment, wrong prescriptions, or incorrect diagnoses, affecting the victim's ability to receive adequate healthcare and insurance in the future (Rocha, 2013). Medical identity theft is the least researched and documented type of identity theft in the literature.

Child identity theft is also a form of identity theft that has long-lasting and significant consequences for the victim. Child identity theft is much easier and less noticeable because parents, due to their busyness, do not pay much attention or regularly check the child's identity (Beltran, 2013). Criminals use children's personal data to open bank accounts and other financial manipulations because children's data are not exploited in society as is the case with adults. It remains undetected for many years and is one form of so-called synthetic identity theft, which involves a fictitious identity. Criminals create a new identity by combining real and fake data (a real personal identification number with a fake name and surname). Typically, children's or deceased persons' data are used for this type of identity theft.

Selling information about individuals' identities from certain financial institutions for a fee is one way to collect the necessary data for creating false identities or abusing existing ones. This is, of course, just a small part of the pervasive corrupt forms and activities (Bjelajac, 2015 & Bjelajac, 2008). Some employees in such institutions abuse their positions and enable individuals from criminal backgrounds to access protected databases with client information. The dark web or darknet serves as a highly profitable market where criminals can buy such data, whether stolen or obtained through corrupt actions. Additionally, individuals with ICT knowledge and skills breach security systems and access financial institutions' databases, collecting information about clients (personal data, account numbers, PIN codes, etc.) for further fraudulent activities.

How Does Identity Theft and Fraud Occur?

Identity theft and fraud typically unfold in several stages. One model explaining identity theft and fraud outlines three phases (Sproule & Archer, 2007):

- Information gathering

- Creating a false identity
- Criminal acts committed using the false identity

According to this model, the initial phase involves gathering identity information, which entails obtaining personal data about another person without their authorization. There are numerous ways criminals can obtain someone's identity information. These include stealing or finding lost personal documents (passport, ID card, credit card), phishing, skimming, eavesdropping or secretly viewing personal data when the person is using it, hacking into databases of certain institutions, using malicious software, and intercepting wireless data transmissions containing identity information. As we can see, identity information can be obtained physically (through theft), electronically, through interaction with the victim, or a combination of these methods. Most of these methods of acquiring identity information are illegal and criminalized by law, while some methods are not subject to criminal prosecution (finding documents or papers with information).

One of the most commonly used methods for obtaining information about a person is phishing. The term "phishing" comes from the English word "fishing," which metaphorically describes the process by which unauthorized users lure internet users to voluntarily reveal their confidential information. It is mainly carried out without contact (most often via email or telephone). It represents a form of social engineering in which the attacker tries to fraudulently obtain confidential information from the victim by falsely presenting themselves as a trusted person (Jagatic et al., 2005). The term phishing is used to describe the process of illegally collecting sensitive information obtained by deception in cyberspace, where the attacker presents themselves as someone trustworthy who has the right and need to handle such information. Traditional phishing involves creating fake websites that are visually identical to the originals, with the purpose of capturing confidential personal data. Phishing attacks involve activities where unauthorized users use fake email messages and fake web pages of financial organizations to entice the user to reveal confidential personal information. This primarily refers to data such as credit card numbers, usernames, PIN codes, etc., although

there are other alternatives (Dinarević & Softić, 2021). Phishing can be carried out in various ways and typically involves three execution phases (OECD, 2007, p. 17):

- In the first phase, the perpetrator sends an email to the potential victim, appearing to be from the bank the victim uses or from another organization that might be close to the victim and could request certain personal information.
- The second phase begins when the victim reads the email, responds to it, or forwards the message to the appropriate fake website, leaving certain personal data.
- The third phase involves forwarding the victim's data directly to the perpetrator, who uses the obtained data to commit another illegal or criminal act, which is usually considered a fraud.

One form of phishing is *pharming*. Pharming is a complex form of internet fraud that focuses on manipulating the *Domain Name System (DNS)* to redirect users to fake websites to steal their personal or financial information. This fraud technique differs from phishing in that it does not require active user participation, such as clicking on suspicious links in emails. Instead, pharming uses technical flaws or malicious software to change DNS records so that users are redirected to fake sites instead of legitimate ones. Simply opening such an electronic message can download a computer virus, Trojan, malware, or key generator onto the victim's computer, stealing all the victim's important data – passwords, usernames, and credit card numbers used on that computer (Beal, 2016).

Unlike traditional phishing, which uses general methods of sending fake emails to many users hoping someone will take the bait, spear *phishing* is a targeted and personalized fraud. Spear phishing is a sophisticated internet fraud technique that focuses on targeting specific individuals, organizations, or user groups. Attackers conducting spear phishing carefully research their targets to create convincing and personalized messages. This research may involve gathering information about the victims through social networks, internet

searches, or even hacking email accounts. Once they gather enough information, the perpetrators use this data to personalize their messages, often using names, positions, or company information to appear authentic.

A special type of attack that uses text messages or SMS to execute fraud is *Smishing*. Typical smishing techniques involve sending messages to mobile phones via SMS that contain links the user can click on or a callback phone number the user can call. Smishing is particularly dangerous because it uses direct communication via mobile devices, where users might not be as cautious as on other platforms such as email. Vishing is another form of internet fraud that combines telephone call technology with the aim of manipulating the user to reveal sensitive information or perform unwanted actions. The name comes from the combination of the words "voice" and "phishing," indicating that vishing uses voice communication to commit fraud, unlike traditional phishing, which relies on email. A typical vishing scenario involves receiving a phone call from an attacker who falsely represents a legitimate institution or company, such as a bank, tax office, or tech support (Newman, 1999). The attacker may use various manipulation techniques, such as false promises, threats, or creating an urgent situation to get the user to reveal sensitive information such as usernames, passwords, credit card numbers, or personal data.

One of the techniques of identity theft most commonly associated with payment cards is skimming. It is a process in which, using a device known as a "skimmer," information from the victim's card is illegally copied when it is used on a specific device (Gupta & Kumar, 2020). This attachment is usually connected to a machine such as an ATM or a card payment device and copies all the card data during its use. Often, an additional device, such as a hidden camera, is used to record the user's PIN entry. At first glance, a skimming device may look like an ordinary card payment device, but the key difference is that it copies the card information and transmits it to the criminals instead of sending it to the bank, as is usually the case. This activity allows criminals to illegally access the victim's financial resources, often leading to identity theft or financial losses.

Artificial intelligence (AI) is a new method used for identity theft and fraud. It has advanced to the point where it can independently create certain malware used to steal information and personal data. AI offers multiple advantages when it comes to analyzing and predicting human behavior, institutional behavior, or the functioning of business and financial systems, thereby enabling the identification and exploitation of vulnerabilities (Filipović et al., 2023). As the latest form of information technology development, besides all the advantages it brings, it has provided criminals with another tool for carrying out their criminal activities, among which identity theft and fraud hold a special place.

Overview of Legal Regulations

The international community, along with the scientific and professional public, has recognized identity theft as a serious and expanding problem affecting numerous individuals and financial institutions. As part of high-tech crime, many international documents address identity theft and fraud associated with identity theft. Significant international organizations, such as the UN, EU, Council of Europe, Organization of American States (OAS), International Telecommunication Union (ITU), and specialized crime-fighting organizations Interpol and Europol, have contributed to the fight against this type of crime. Numerous conventions, declarations, and other acts have been harmonized at the international community level to combat identity theft and mitigate its consequences. Despite many documents, there is no consensus among member states on the definition of identity theft, its forms, and ways of criminalizing it.

Legislation in some countries defines identity theft as a separate criminal offense (USA, UK, France), while many EU countries (Austria, Bulgaria, Belgium, Hungary, Greece, Germany, Ireland, Italy, Netherlands, Poland, Romania, Spain) do not recognize identity theft as an independent criminal offense but incorporate it into the acts of other crimes. These countries enable the prosecution of identity theft perpetrators through other legal acts that complement criminal law. Serbia belongs to this group and does not prescribe identity theft as a

separate criminal offense in its Criminal Code. The current Criminal Code of the Republic of Serbia from 2006 includes a special section on criminal offenses against the security of computer data, which contains the following criminal acts: damage to computer data and programs (Article 298), computer sabotage (Article 299), creation and introduction of computer viruses (Article 300), computer fraud (Article 301), unauthorized access to a protected computer, computer network, and electronic data processing (Article 302), preventing and limiting access to a public computer network (Article 303), unauthorized use of a computer or computer network (Article 304), and creation, acquisition, and provision of tools for committing crimes against computer data security (Article 304a). These criminalizations aim to protect the use of information technology for permissible purposes and ensure the proper functioning of information technology (Stojanović, 2016). Besides these criminal offenses, if identity theft occurs, the Criminal Code provisions related to fraud (Article 208), forgery and misuse of payment cards (Article 243), and unauthorized use of another's business name and other distinctive marks of goods or services (Article 238) are also applied.

Therefore, there is no unified description of the act of committing the criminal offense of identity theft, which poses a problem in international cooperation and information exchange with other countries. Although Serbia has ratified and accepted numerous international conventions and documents, it has not fully implemented their conclusions and recommendations. The Law on the Organization and Competence of State Authorities for Combating High-Tech Crime regulates the jurisdiction of state authorities in dealing with cases related to identity theft, thus somewhat facilitating the fight against this form of crime.

Consequences and Prevention Possibilities

The consequences of identity theft are multifaceted and significant, affecting both the individual victim and the entire system and society. Although few studies have focused on the consequences of identity theft, most research has concentrated on the financial

impact on individuals. Studies conducted in the USA indicate that documented losses resulting from identity theft include financial and legal problems, primarily stemming from the recovery of financial assets and the protection of personal data. Compared to property crimes, identity theft tends to be more costly for the victim on average (Golladay & Holtfreter, 2017). The average amount lost due to property crimes is $915, whereas the average amount lost due to identity theft is $2,183. Identity theft victims experience more than double the losses compared to victims of property crimes, with direct and indirect losses estimated at around $24.7 billion in 2012 (Harrell & Langton, 2013). In addition to the financial losses suffered by individuals and financial institutions, identity theft also brings other significant consequences. Identity theft is not only a financial problem but also a deeply invasive experience that can have long-term effects on the victim's life and well-being. Victims of identity theft may face numerous legal issues, such as repaying loans and debts, criminal prosecution for offenses committed under their identity, difficulties in reissuing documents, job loss, and more. Identity theft also causes numerous emotional and physical effects on the victim, such as fear for personal safety, feelings of anger and betrayal, helplessness, shame, sleep disorders, inability to concentrate, frustration, and anxiety (Identity Theft Resource Center, 2014). For financial institutions and corporations, in addition to financial losses, one of the biggest problems caused by identity theft is the loss of reputation and rating, which is challenging to restore and always raises doubts among potential future clients. Therefore, most financial institutions implement significant security measures to protect their databases and user accounts. They also conduct numerous preventive activities aimed at showing how to avoid potential identity theft and how to act if data theft occurs. These activities are carried out at an international level, and several declarations and other legal acts dealing with high-tech crime, including identity theft, have been adopted. Preventive activities are usually focused on educating clients about the possibilities and methods of identity theft and providing guidance on how to prevent identity theft and minimize damage if it does occur.

The most common steps to reduce the risk of identity theft include:

- Creating strong passwords with a combination of different symbols, letters, and numbers. Also, using two-factor authentication when the system allows it, which can make hacking more difficult even if the perpetrators have the victim's username and password.
- Avoiding accepting and opening unsolicited messages, suspicious calls from unknown numbers, and not sharing payment card information, account details, or passwords online.
- Checking for spelling errors or incorrect domains in online links (for example, an address that should end in ".gov" but ends in ".com" instead), and ensuring the name is spelled correctly without any substitutions (like replacing a letter with a number).
- Not sharing sensitive information during online shopping and primarily shopping through reputable providers with good reviews. Using applications directly provided by sellers of certain goods and services is best.
- When paying by card in stores, using contactless payment methods is recommended.

If identity theft occurs despite all preventive measures, it is crucial to respond promptly and swiftly to prevent further potential misuse. In the event of financial losses, it is essential to notify the bank or corporation about the data compromise as soon as possible to block further unwanted transactions and change passwords and PIN codes.

Conclusion

The latest data on the consequences of identity theft and related fraud indicate that this type of crime is expanding worldwide. The damage caused by this criminal activity is enormous both for individuals and for states. With the advancement of science and technology, methods of execution are becoming more complex and sophisticated.

Criminals are finding new ways to obtain personal or financial information, which they often misuse for economic gain. Given the way business is conducted and the omnipresence of the internet, virtually everyone is at risk of becoming a victim of identity theft. Consequently, international institutions and stakeholders are making efforts to successfully combat cybercrime and identity theft. The results of this study indicate that regulatory frameworks are inconsistent and diverse, complicating international cooperation, evidence gathering, and prosecution of perpetrators of these crimes. It is essential to harmonize laws so that the nature of the criminal offense can be uniformly treated across all or most countries. Additionally, adequate training and continuous professional development of personnel involved in combating cybercrime are necessary to effectively respond to contemporary challenges and advancements in science and technology. The preventive activities of financial institutions and client education about the risk factors of identity theft are crucial in mitigating financial losses and victimization. Moreover, in cases of data compromise and identity theft, a significant procedure and protocol for victims to react and behave appropriately, whom to contact, and how to prevent or minimize consequences are essential. All of this necessitates continuous collaboration among all relevant societal actors (financial institutions, specialized state bodies within the prosecution, judiciary, and police) at the international level to achieve better results in preventing these forms of crime.

The lack of research in this field is a particular issue that the scientific community must address. The results and evaluation of studies and projects dealing with identity theft and fraud form the basis on which successful policies and measures for preventing and combating financial losses of individuals and corporations should be built.

References

12th UN Congress on Crime Prevention and Criminal Justice. (n.d.) Retrieved 15.4.2024. from https://www.unodc.org/documents/ crimecongress/12th-Crime-Congress/Documents/A_CONF.213_18/ V105 3828e.pdf

Allison, S. F., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice, 33(1)*, 19-29. https://doi.org/10.1016/j.jcrimjus.2004.10.007

Beal, V. (2016). "How to Defend Yourself Against Identity Theft", Retrieved 13.4.2024.http://www.webopedia.com/DidYouKnow/ Internet/ 2006/identity_theft.asp.

Beals, M., DeLiema, M., & Deevy, M. (2015). Framework for a taxonomy of fraud. *Financial Fraud Research Center*. https://www.finrafoundation. org/sites/finrafoundation/files/framework-taxonomy-fraud.pdf

Beltran, G. (2013), Trends in child identity theft. Identity theft resource center" Retrieved 14.5.2024 from www.idtheftcenter.org /Child-ID-Theft/trends-in-child-identity-theft.html.

Bjelajac, Ž. (2008). Korupcija kao vid organizovanog kriminala [Corruption as a form of organized crime]. *Pravo – teorija i praksa, 25*(3-4): 47–54.

Bjelajac, Ž. (2015). Korupcija kao izazov savremenog demokratskog društva [Corruption as a challenge of modern democratic society]. *Kultura polisa 12*(26): 43–57.

Bjelajac, Ž., Filipović, A. (2020). Internet addiction disorder (IAD) as a paradigm of lack of security culture. *Kultura polisa, 17*(43): 239–258.

Bourke, P., Ward, T. and Rose, C. (2012),Expertise and sexual offending: a preliminary empirical model" *Journal of Interpersonal Violence*, Vol. 27 No. 12, pp. 2391–2414. https://doi.org/10.1177/ 0886260511433513

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive medicine reports, 17,* 101058. https://doi.org/10.1016/j.pmedr.2020. 101058

CIFAS (2010), *Identity Theft- Victims* [Internet], The UKs Fraud Prevention Service (CIFAS), London.

Cole, S. A., & Pontell, H. N. (2006). "Dont be low hanging fruit": Identity theft as moral panic. *In Surveillance and security* (pp. 125–147). Routledge. ISBN 9780203957257

Copes, H. & Vieraitis, L.M. (2012), *Identity Thieves: Motives and Methods*, Northeastern University Press, Boston.

Council of Europe (2013). Cybercrime Convention Committee – T-CY Guidance Note#4, Identity theft and phishing in relation to fraud, (n.d.) Retrieved 11.4.2024 from https://rm.coe.int/16802e7132.

Dinarević, M., & Softić, L. (2021). Razvoj, pojam i oblici cyber kriminala [Development, Concept and Forms of Cyber Crime]. *Pregled: časopis za društvena pitanja*/Periodical for social issues, 62(2), 125-141. UDK 004.738.5:343.9

Đukić, A. (2017). Bezbednost – Krađa identiteta-oblici, karakteristike i rasprostranjenost [Security – Identity Theft: Forms, Characteristics, and Prevalence], *Interdisciplinarni naučni časopis Vojno delo* br.3 */Interdisciplinary Scientific Journal Vojno delo no.3*, DOI: 10.5937/ vojdelo1703099D

Filipović, A., Bjelajac, Ž., Merdović, B. & Stošić, L. (2023). Some Aspects of the Criminal Potential of Artificial Intelligence. PaKSoM 2023, 41-47. ISBN: 978-86-82602-02-6

Gill, M. (2017). Learning from Offenders: Some Iatrogenic Effect of Crime Prevention Measures. In: LeClerc, B., Savona, E. (eds) Crime Prevention in the 21st Century.Springer, Cham. https://doi.org/ 10.1007/978-3-319-27793-6_4

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization:An examination of emotional and physical health

outcomes. *Victims & Offenders, 12(5)*, 741–760. https://doi.org/10.1080/15564886.2016.1177766

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. *In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 71-80)*. https://doi.org/10.1145/1102199.1102214

Gupta, C. M., & Kumar, D. (2020). Identity theft: a small step towards big financial crimes. *Journal of Financial Crime, 27(3)*, 897-910. https://doi.org/10.1108/JFC-01-2020-0014

Identity Theft Resource Center. (2014). Identity theft: The aftermath 2013. Retrieved 14.5.2024. from http://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf

Ipsos-Reid (2006). *Concern Over Identity Theft Is Changing Consumer Behaviour, Ipsos-Reid on Behalf of Capital One*.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2005). Phishing attacks using social networks. *Indiana University Human Subject Study*, 05-9892.

Javelin Strategy & Research, "2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis" https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis.

Komlen-Nikolić, L., Gvozdenović, R., Radulović, S., Milosavljević, A., Jeković, R., Živković, V., ... & Aleksić, I. (2010). Suzbijanje visokotehnološkog kriminala [Suppression of cybercrime]. *Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije/Association of Public Prosecutors and Deputy Public Prosecutors of Serbia, Beograd.*

Krivični zakonik Republike Srbije, [Criminal Law] "Službeni glasnik Republike Srbije" broj 85/2005, 88/2005-ispr., 107/2005-ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016.

Kroll (2019). Global Fraud & Risk Report 2019/2020. https://www.kroll.com/en/insights/publications/global-fraud-and-risk- report-2019.

Manap, N. A., Rahim, A. A., & Taji, H. (2015). Cyberspace identity theft: An overview. *Mediterranean Journal of Social Sciences, 6(4)*, 290. http://dx.doi.org/10.5901/mjss.2015.v6n4s3p290

Mercuri, R. T. (2006). Scoping identity theft. *Communications of the ACM*, 49(5), 17-21. https://doi.org/10.1145/1125944.1125961

Milošević, M., & Urošević, V. (2009). Krađa identiteta zloupotrebom informacionih tehnologija [Identity theft by misuse of information technologies]. *Bezbednost u postmodernom ambijentu–zbornik radova–knjiga VI [Security in a postmodern environment–Proceedings–book VI]*, 53-64.

Newman, J. Q. (1999). *Identity theft: The cybercrime of the millennium*. Loompanics Unlimited.

Nikolić-Ristanović, V., & Konstantinović-Vilić, S. (2018). Kriminologija [Criminology]. *Beograd: Prometej*.

OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft, Ministerial background report: DSTI/CP (2007)3/FINAL. (n.d.) Retrieved 15.4. 2024 from http://www.oecd.org/sti/40644196.pdf

Passel, J.S. (2006), *The Size and Characteristics of the Unauthorized Migrant Population in the US.* [Internet, Microsoft the Pew Hispanic Centre, Washington, DC https://www.procon.org/wp-content/uploads/ sites/40/immidoc6.pdf

Prlja, D., & Reljanović, M. (2009). Visokotehnološki kriminal–uporedna iskustva. [Cyber crime – comparative experiences], *Strani pravni život, (3)*, 161–194. https://www.strani pravnizivot.rs/ index.php/SPZ/issue /view/30

Prosch, M. (2009). Preventing identity theft throughout the data life cycle. *Journal of Accountancy*, 207(1), 58–62. https://doi.org/10.1080/ 15536548.2006.10855783

Roberts, L. D. (2008). *Cyber-victimisation in Australia: Extent, impact on individuals and responses.* Tasmanian Institute of Law Enforcement Studies. http://hdl.handle.net/20.500.11937/9773

Rocha, K. (2013), *Medical Identity Theft: The Basics*, The Identity Theft Resource Center.

Sproule, S., and N. Archer. (2007). *Defining Identity Theft*. Eighth World Congress on the Management of eBusiness, Toronto, IEEE. https://doi.org/10.1515/9780776619927

Stojanović, Z. (2010). „Krivičnopravni ekspanzionizam i zakonodavstvo Srbije". [Criminal law expansionism and Serbian legislation], *Stanje kriminaliteta u Srbiji i pravna sredstva reagovanja,(ur. Đ. Ignjatović), IV deo/State of crime in Serbia and legal means of response, (ed. Đ. Ignjatović, part IV, Beograd,* 32-48.

Stojković Numanović, K., Merdović, B., & Živaljević, D. (2023). Forging payment cards and cybercrime. *Pravo – Teorija I Praksa, 40(4)/Law – Theory and Practice, 40(4)*, 138–154. https://doi.org/10.5937/ ptp2304138S

UNHCR (2007), *Why Do People Move to Another Country?* [Internet], The United Nations High Commissioner for Refugees UNHCR, Geneva.

Urošević, V., Ivanović, Z., & Uljanov, S. (2012). *Mač u world wide web-u* [*A sword in the world wide web*], Beograd:Eternal mix.

Vilić, V. (2017). Cybercrime: *Basic criminological characteristics and legislation*. Lap - Lambert Academic Publishing – International Book Market Service Ltd., member of OmniScriptum Publishing Group. -166. ISBN 978-620-2-01800-5.

World Privacy Forum (2024). *Medical Identity Theft, Retrieved 11.5.2024* from https://www.worldprivacyforum.org/category/med-id-theft/

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala [Law on the Organization and Competence of State Bodies for the Fight against High-Tech Crime]"*Službeni glasnik Republike Srbije/ Official Gazette of the Republic of Serbia"* broj 61/2005 104/2009.

Zakon o organizaciji nadležnih organa u suzbijanju organizovanog kriminala, korupcije i drugih posebno teških krivičnih dela[Law on

the organization of competent authorities in the fight against organized crime, corruption and other particularly serious crimes] *„Službeni glasnik Republike Srbije/ Official Gazette of the Republic of Serbia*" br.42/02,27/03,39/03,67/03,29/04,58/04-dr. zakon/ state law, 45/05,61/ 05,72/09).

Zakonik o krivičnom postupku, [Criminal Procedure Code] "*Službeni glasnik Republike Srbije"* br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – odluka/ decision US i 62/2021 – odluka/decision US

Kako razumeti krađu identiteta i prevaru

Boro Merdović[1] i Biljana Jovanović[2]
[1]Ministarstvo unutrašnjih poslova Republike Srbije, Beograd
[2]Ministarstvo odbrane Republike Srbije, Beograd

Sažetak

Krađa identiteta i prevara identiteta prdstavljaju najbrže rastući oblik kompjuterskog kriminala koji ima velike posledice na pojedince ali i na korporacije i finansijske institucije. Razvoj nauke i tehnologije doveo je u opasnost ličnu bezbednost svakog pojedinca ali i stvorio mogućnosti kriminalcima da na lak i perfidan način dođu do imovinske koristi ili ugroze korporacijsku i bezbednost velikih finansijskih institucija. Kao relativno nov oblik kompjuterskog kriminala, krađa identiteta je prouzrokovala i potrebu usklađivanja krivičnih zakonodavstava sa novonastalom situacijom. Cilj rada je da razjasni terminološke nedoumice prisutne u ovoj oblasti i istakne aktuelnost problema krađe identiteta i prevare vezane za krađu identiteta. Pregledom relevantne naučne literature, primenom kvantitativne i kvalitativne analize sadržaja, komparativne analize i uporednog i istorijskog metoda, ukazaćemo na značaj jasnog i preciznog definisanja krađe identiteta i njegove zakonske inkriminacije. Ukazaćemo na različite oblike krađe identiteta, način na koji se najčešće dešavaju i posledce koje izazivaju kao i mogućnosti prevencije. Rezultati istraživanja su pokazali da je krađa identiteta u ekspanziji i da je neophodno usaglašavanje zajedničkih mera na međunarodnom nivou. Takođe, na osnovu dobijenih rezultata možemo zaključiti da je neophodno preduzeti mere edukacije ugroženih kategorija stanovništva kako bi se posledice ovog oblika kriminala svele na najmanju moguću meru. Praktične implikacije ovog istraživanja ukazuju na potrebu razvijanja većeg broja istraživanja iz ove oblasti sa posebnim osvrtom na pojedine oblike krađe identiteta i prevare identiteta.

Ključne reči: krađa identiteta, prevara identiteta, phishing, kompjuterski kriminal