Stojković Numanović Katarina[*]
https://orcid.org/0000-0003-4288-9525
Merdović Boro[**]
https://orcid.org/0000-0002-6619-5934
Živaljević Dragan[***]
https://orcid.org/0009-0005-3829-4344

UDK: 343.522:343.09.02
Review article
DOI: 10.5937/ptp2304138S
Received: 08.10.2023
Approved for publication: 08.11.2023
Pages: 138–154

FORGING PAYMENT CARDS AND CYBERCRIME

ABSTRACT: Payment card forging and high-tech crime are deeply rooted problems in today's society. These sophisticated forms of crime utilize advanced techniques and high-tech tools to illegally access financial resources and commit fraud. Payment card forgery involves the creation of fake copies of debit or credit cards with the intent of conducting illegal financial transactions. Access to card data is achieved through various methods, including skimming (illegally collecting card data), phishing (fraud through fake emails or web pages), or the physical theft of cards. Simultaneously, high-tech crime encompasses a wide range of activities aimed at the misuse of digital technologies and networks to achieve financial gain or harm to individuals, companies, or states. These crimes often include computer fraud, cyber-attacks, and digital fraud. This paper aims to highlight the importance and seriousness of payment card forgery, explore different methods and patterns of these criminal activities, and emphasize their specific connection with high-tech crime. Different methodologies were applied in the research including quantitative and

[*] LLM, PhD candidate at the Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad, Serbia, e-mail: katarina.stojkovic1986@gmail.com
[**] LLD, Research Associate, Ministry of Internal Affairs of the Republic of Serbia, Police Department for the City of Belgrade, Serbia, e-mail: boro.merdovic@gmail.com
[***] LLD, Associate Professor, National Security Academy, Belgrade, Serbia, e-mail: zivaljevic@gmail.com

qualitative content analysis, comparative analysis, as well as descriptive and analytical statistics. The obtained results clearly indicate the growing importance of this problem both in the legislative and in the criminological contexts, with a constant increase in the number of committed criminal acts. Additionally, the research highlights the inextricable link between payment card forgery and various forms of high-tech crime, which often intertwine and together constitute an overarching challenge to the justice system and the security of society. Finally, the paper will consider various strategies and methods that society and the state can use to counter the spread of these criminal activities. The ultimate goal is to preserve the safety and integrity of the financial system and protect the interests of individuals.

Keywords: *payment card forgery, cybercrime, financial fraud, skimming, phishing.*

1. Introduction

From the introduction of the Internet until the present day, the Internet has become an essential tool in all aspects of society and business. From the beginning, computers and Internet technology have developed and advanced, and their impact on business and commerce operations is enormous (Featherly, 2016). The expansion of the digital world and the use of the Internet as a trading platform represents a significant change in the way companies communicate with their customers and conduct their operations. This includes online payments for business and trade transactions, which has become normal in the modern business environment. The Internet has enabled companies to penetrate new markets, expand their business networks and create more efficient ways of communicating with customers. However, this kind of technological development and progress also brings new challenges in the form of information security and privacy, as well as easier connection and realization of specific cybercrime actions, through internet platforms and advanced communication technologies (Živaljević, 2022, p. 12). Overall, the development of the Internet and the digital world has a profound and far-reaching impact on the way business and commerce operations are conducted, a constantly changing and evolving field. The Internet, automation of business activities, electronic banking, ATM transactions, payment card payments, internet payments, use of POS terminals and the like, represent new scientific

and technical achievements that make banking business modern and efficient (Pantić, 2018, p. 393).

One of the indispensable technological achievements of the financial sector are payment cards, which have become the basic means of payment. A payment card is a modern cashless payment instrument that performs three functions: cashless payment means, user crediting instrument and generally accepted international and national means of payment. It is a type of identification that authorizes the owner for cashless payment (Zečević, 2009, p. 305). Payment cards are technologically advanced instruments for cashless payment and financial transactions that allow users to make payments and transactions without using cash. This type of card represents a modern way of payment, where the card user warrants to pay the amount to the card issuer, while the seller of goods or services has the right to collect that amount from the card issuer. Cards are not a substitute for money but enable practical and quick financial transactions.

Over time, payment cards have evolved and improved. In the beginning, people were skeptical due to a lack of understanding on the purpose and benefits of payment cards. However, over time the advantages of using these cards was recognized and was reflected through several things:

- *Greater security*: using payment cards provides a higher level of security compared to carrying cash. When cash is lost or stolen, the money is usually lost forever. With a payment card, users can report the loss or theft, and the financial institution can take protective measures and compensate the damage.
- *Saving time*: payment cards enable faster and more efficient payment. Users simply present a card or use contactless options to make a payment, eliminating the need to count cash and return change.
- *Ease of use*: payment cards are easy to use and practical for everyday transactions. In addition, most stores and online stores accept payment cards as a means of payment, making them widely available. One of the increasingly common forms of payment is through a mobile phone, to which a payment card is connected, so its physical presence is not necessary.

The rapid growth of e-commerce has resulted in an increasing number of online shopping. These customers depend on credit cards as a payment method or use mobile wallets to pay for their purchases. Thus, credit cards have become the main form of payment in the e-world. With billions of transactions occurring daily, this is a fertile field for criminals to generate

profit by finding different ways to attack and steal credit card information. Criminal organizations and individuals are constantly making efforts to bypass security measures, abuse payment cards, and thereby obtain material benefits for themselves. Given the ubiquitous use of cards, abuse of payment cards is a serious challenge in modern society. In order to identify unauthorized or suspicious activities and reduce the risk of misuse, it is important to take a series of preventive measures, and apply a vigilance and monitoring of transactions. In addition, financial institutions and merchants implement various security measures to protect data and prevent card misuse. The following text will list the most common forms of misuse and payment card forgery, the legal regulations that regulate this type of criminal behavior, and global measures which are implemented in domestic legislation.

Increasing technological developments such as the increased use of neural networks and the use of artificial intelligence (AI) are also affecting card issuers and banking services. AI chat tools can write malicious code very quickly, in most cases even faster than defense software can identify that code. Today, AI is paving the way in designing new methods to better manage next-generation credit card fraud detection by supporting increased approval rates, minimizing declined transactions, and enabling the proactive monitoring of credit limits (Cherif, Badhib, Ammar, Alshehri, Kalkatawi & Imine, 2023, p. 146). From all of the above, we can conclude that a person who commits the criminal offense of abuse and fraud by using a payment card is very familiar with the technique and technology of using payment cards, which tells us that this crime is mostly committed by professionals. The execution of this form of criminal offense requires technical and technological means and knowledge, which classifies it as a high-tech crime or cybercrime.

2. Methods of misuse and payment card forgery

The oldest form of criminal offense related to payment cards refers to the classic form of the criminal offense of theft. During the earliest stages of development of this payment technique, confiscation of a payment card, and its misuse, was the first form of a criminal offense related to payment cards. Only later, due to the improvement of the protection measures and security of payment cards and banking systems, other forms of criminal activities related to various forms of fraud such as fraudulent procurement, unauthorized account access, takeover or identity theft, and other forms of financial manipulations developed. Two types of credit card crime that are directly related to classic forms of crime are account takeover and *skimming*.

When taking over an account, the criminal surreptitiously gathers key information about an individual. This can be done by stealing and then returning wallets, purses, or even breaking into buildings where the victim lives (houses, apartments, hotel rooms). The next step is to contact the card issuer, where the perpetrator presents himself as the actual and legitimate card owner and requests a change to the card address. A new card is then requested and sent to the new address. Skimming is the theft of credit card information during a legitimate transaction. Often, a double keyboard is placed on the keyboard itself, which records all the necessary data to create a fake payment card, as well as the Lebanese loop – when a strip of X-ray film is placed in the mouth of the card reader to hold the card so that the transaction is prevented (Matijašević, 2013). A merchant or employee obtains a person's credit card number by looking at receipts or using an electronic scanner. Any additional identity data such as PIN numbers, postal codes, and security codes are also downloaded. Scanners can be placed over legitimate ATMs, allowing criminals to steal from bank customers.

Thus, the crime has changed from outright card theft to downloading card information. Even as the rate of outright theft has declined, as seen in crime reports compiled by the Federal Bureau of Investigation (FBI), the incidence of remote, online theft using credit cards and other personal identity information has skyrocketed (Ross, 2013, p. 107). One of the terms that is used in this area of crime, and which can be found in domestic and foreign literature, is carding. Carding has emerged as a significant form of cybercrime that encompasses various frauds associated with the misuse of payment cards. This practice involves the unauthorized use of stolen or forged credit card information for financial gain. The evolution of technology has enabled the expansion and complexity of carding, posing significant challenges to global financial security and privacy.

Carding encompasses various tactics and strategies used by cybercriminals to exploit credit card information. The process usually includes:

- *Data collection:* cybercriminals obtain credit card information through a variety of methods, including hacking into merchant databases, using malware to steal data, or launching phishing campaigns. These methods provide important information such as card numbers, expiration dates, and CVV codes.
- *Data verification:* the stolen data goes through a verification phase to ensure its accuracy and potential for misuse. This step includes verifying whether the card has been reported stolen and that there are sufficient funds for a transaction.

- *Production of forged cards*: after data is verified, criminals use the stolen data to create counterfeit physical or virtual cards that closely resemble legitimate ones.
- *Unauthorized transactions:* with counterfeit cards, criminals initiate fraudulent transactions, which may include purchasing goods and services, withdrawing cash from ATMs, or transferring funds to other accounts.

The growth of the online market and the anonymity provided by the Internet have made it possible for stolen credit card information to be distributed. Criminals buy and sell this data, which contributes to the proliferation of carding networks and makes it a global issue.

Phishing is a sophisticated fraud technique, increasingly used in the digital age, to trick users into gaining access to their personal, financial, and sensitive information. This type of attack is based on psychologically manipulating users to get them to reveal their confidential information such as passwords, credit card numbers or personal identification information. Phishing attacks have become more frequent due to the increasing number of mobile phone users who use mobile services on a daily basis, such as online banking and e-commerce that require sensitive user information (Marforio, Masti, Soriente, Kostiainen, & Capkun, 2016). One way is in the form of text messages that redirect users to illegitimate websites asking them to enter personal information that attackers can access (Shahriar, Zhang, Dunn, Bronte, Sahlan, & Tarmissi, 2019, p. 179). Another significant problem for mobile phone and Internet users is downloading prepackaged applications, when prompted by a mobile device, without knowing that it contains harmful phishing malware (Cui, Jourdan, Bochmann, Couturier, & Onut, 2017).

Thus, a phishing technique is a form of Internet fraud that is often used for the unauthorized collection of user personal information. This process usually involves the following steps:

- *Creating fake messages:* attackers start by creating fake emails, text messages or even social networks that send messages to users. These messages often look authentic and often pose as messages from well-known companies, banks, government agencies or other trusted sources.
- *Creating urgency or fear:* In order to get users to react quickly, attackers often utilize urgent or fear tactics.
- *Displaying fake links:* Phishing messages often contain links to fake or malicious websites. These pages are often designed to look identical

to the original web pages, which can trick users into entering their personal information.
- *Data collection:* when a user clicks on a fake link and enters their information, attackers collect this information and misuse it. The misuse can include identity theft, accessing bank accounts or sending malware to users' devices.
- *Social Engineering:* phishing attacks often use manipulation and social engineering to overcome user suspicion. This may include using personal information, names or other data to create the impression that the message is legitimate.

Identity theft is a special form of criminal activity that is closely related to cybercrime. Identity theft is a multifaceted cybercrime that involves the unauthorized use of personal information for the purpose of fraud. There are different definitions of this phenomenon and, considering the seriousness of the problem, it has also been addressed by international institutions and organizations. The 12th UN Congress on Crime Prevention and Criminal Justice in 2010 defined it as the misuse of personal data for the purpose of committing fraud. Similarly, the Organization for Economic Cooperation and Development (OECD) defines identity theft as the unauthorized acquisition, transfer, possession, or use of personal data for the purpose of fraud or other criminal activity (OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft, 2007, p. 3). The process of identity theft usually begins with learning an individual's personal information without their knowledge or consent. Data is obtained through deceptive means, theft, or criminal activity. After that, the stolen information is used for various criminal activities, often involving financial gain for the perpetrators (Milošević & Urošević, 2009). Identity theft usually consists of three elements: the manner of execution of the act itself (modus operandi), the goal of the attack and the motivation of the perpetrator (Vilić, 2019, p. 45). The emerging forms of identity theft, viewed in a narrower sense and according to the location of personal information and the means and techniques used for its illegal acquisition, can be classified into three broad groups (Đukić, 2017, p. 102): identity theft using classic methods and outside ICT systems and networks; identity theft from personal computers and mobile devices in a network environment; identity theft from ICT systems and networks.

3. International legal regulations and implications for domestic legislation

The development of technology and the expansion of the use of more secure chip credit cards have brought with them increasingly sophisticated forms of fraud related to Internet banking, credit (payment) cards and identity theft. These forms of crime are often carried out without the need to show a physical card, which makes it even more difficult to detect and suppress them. This presents new challenges, for European and Serbian legislation, in order to protect the individual as well as the entire financial and banking system.

In order to improve measures aimed at preventing such abuse, there was a need to strengthen the legal framework of the European Union. One of the first steps towards that end was the Council Framework Decision 2001/413/PUP, often referred to as the Framework Decision on Cybercrime. It represents an important legal instrument adopted by the European Union (EU) to combat cybercrime, including crimes related to cashless means of payment. This Framework Decision was adopted in 2001 and represents one of the first steps in regulating this increasingly important aspect of criminal law within the context of the digital revolution. It covers a wide range of crimes, including misuse of payment cards, identity theft and other forms of fraud related to cashless payments. The decision provides the definitions for key terms and sets certain standards for prosecuting and sanctioning the perpetrators of these crimes. In addition, it promotes cooperation between member states during the investigation and prosecution of these crimes. This legal instrument represents an important step in creating a legal basis for the fight against cybercrime in the EU and improving the security of cashless means of payment. However, given rapid technological progress, the legal framework is continuously evolving in order to adequately respond to new threats and challenges in the digital world. The EU saw the need to adopt new legal instruments that will be binding on member states and improve international cooperation in this field. In this context, Directive 2019/713/EU was adopted, which represents another key legal instrument of the EU related to the fight against cybercrime and the protection of cashless payment means. It represents an innovation of the framework decision from 2001 and enacts significant obligations for member states, serving as a foundation for domestic criminal legislation, both present and future. The most important features of this legal instrument are:

- updating the existing EU legislation in the field of security and protection of cashless payment means, with a focus on preventing and combating fraud and forgery related to digital forms of payment.

- specifies a wide range of crimes and forms of fraud related to cashless payment instruments, including digital payment methods such as payment cards, mobile wallets, electronic money and cryptocurrencies, providing clear and precise definitions of associated terms.
- special emphasis is placed on international cooperation between member states in relation to the investigation, prosecution and exchange of information on crimes related to cashless means of payment,
- foresees certain penalties for natural persons who commit criminal acts related to cashless payment instruments, prescribes minimum and maximum penalties in order to allow flexibility in sanctioning.
- a special novelty refers to online applications and support for victims of these types of crimes.
- The Directive requires the EU Commission to periodically report to the European Parliament and the Council on the progress made in bringing national legislation into line with this Directive.

Serbia tried to implement some of the above into its domestic legislation following the recommendations and the assumption of international obligations. The analysis of current criminal legislation associated with forgery and misuse of cashless payment instruments makes it clear that the legislator has prescribed a special criminal offense against the economy related to the abuse of payment cards (Article 243 CC), as well as other criminal offenses that can be subsumed under criminal offenses related to fraud and forgery of cashless payment instruments from the Directive (Pavlović, 2022, p. 38). The Criminal offense of Forgery and abuse of payment cards (Article 243 of the CC RS) is the basic criminal offense that regulates this issue. The difference, in reference to the Directive, is that in domestic legislation, incriminations are found in different parts of the Criminal Code, while in the Directive they are precisely and clearly defined in one place. The specificity of the criminal acts related to the abuse of payment cards is reflected in the fact that it sublimates several forms of criminal acts. It represents a property crime, a crime related to abuses in the economy, contains elements of crimes against legal traffic (forgery). In this context, it is difficult to classify it in a certain category. In recent times, especially after the COVID-19 pandemic and the sudden increase in contactless card payments, it has also taken on elements of computer crime. Perpetrators can be individuals or organized criminal groups. It can also have a local character but also a transnational one, where the action is carried out in one country while the consequences occur in another, which requires the continuous cooperation of police and judicial

authorities at the international level. The basic provisions of the criminal offense of Forgery and abuse of payment cards from article 243 of the CC foresees several provisions and positions that regulate this field. Paragraph 1, of this criminal offense stipulates that: whoever forges a fake payment card or who alters a genuine payment card with the intention of using it as genuine or who uses such fake card as genuine shall be punished with imprisonment of six months to five years and fined. If the perpetrator obtained an illegal material benefit (paragraph 2) or if that benefit exceeds one million and five hundred thousand dinars (paragraph 3), foreseen high prison sentences which can be 12 years, including a fine. The punishment from paragraphs 2 and 3 of this article shall apply to a perpetrator who commits the act by unauthorized use of someone else's card or confidential data that uniquely governs that card in payment transactions, or a perpetrator who acquires a fake payment card with the intention of using it as a real one, or a perpetrator who obtains data with the intention of using it to create a fake payment card (paragraph 5), which perpetrator will be punished by a fine or imprisonment of up to three years. This incrimination foresees confiscation of forged and fraudulent payment cards (paragraph 6). As we can see, this article criminalizes and sanctions actions related to forgery, abuse of payment cards, production of fake cards, as well as misuse of client data. In domestic practice, we most often encounter the crime of theft in which the card is stolen and then misused by the perpetrator of the crime by withdrawing money or paying in facilities where a PIN for the card is not required.

However, more and more often these forms of crime are taking on transnational elements, whereby jurisdiction is transferred to international criminal legislation and institutions. When solving international legal matters, priority is always given to international documents, so only if some issues are not part of one of the signed international treaties, the provisions of domestic laws are applied (Merdović, Stojković Numanović & Dragojlović, 2023, p. 104). In this regard, international legal and police cooperation in combating this form of cyber and financial crime is of crucial importance.

4. How to prevent abuse and fraud with payment cards?

In the fight against criminals, IT (software) and technical (space and hardware) protection is constantly being improved with the sphere of interest increasingly becoming access to the desired data through employees, regardless of whether it is company insiders or poorly trained, inattentive and or negligent employees. The criminals' level of professional competence

and applied methods are constantly developing and improving, which makes the danger of large material and other types of damage suffered by victims of cybercrime real; therefore, the protection of data that is, or can be, the target of criminal attacks, is of great importance (Đukić, 2017, p. 100). Payment cards, as a practical payment method, provides speed, simplicity, and practicality, thus facilitating everyday transactions. However, at the same time, criminals have recognized the opportunity to exploit the vulnerabilities of these systems. To counter these challenges, financial institutions and security experts are continuously developing sophisticated fraud detection and prevention techniques. This includes analyzing transactions to identify unusual activity, using algorithms to detect anomalies, and machine learning models to recognize patterns of behavior that indicate fraud (Basnet & Doleck, 2015). In addition, visual analytics play an increasingly important role in identifying exceptions and fraudulent activities.

The introduction of new technologies and innovations brings numerous benefits while also posing new security challenges. A comprehensive approach that combines technology, user education and effective fraud countermeasures is essential to maintaining the integrity and trust in the financial system. The banking system and financial institutions strive to preserve their credibility and trust by developing specific methods to counter specific methods of abuse, forgery and fraud related to payment cards and cashless payments (Barker, D'amato & Sheridon, 2008, p. 402). In this context, there are a number of methods and techniques that financial institutions use to detect such frauds. We most often encounter, in scientific and professional literature, the following mechanisms and methods for the prevention and detection of payment card fraud:

- Transaction analysis: Tracking and analyzing transactions is a key method in fraud detection. Identifying suspicious transactions that differ from normal patterns can indicate potential fraud.
- Exceptions and anomalies: Finding exceptions and anomalies in transactions can help detect unusual activity. Using anomaly detection algorithms makes it easier to identify transactions that stand out from the norm.
- User profiling: Monitoring the usual habits of the user enables the recognition of suspicious activities. Changes in payment or purchase patterns that differ significantly from normal behavior may indicate potential fraud.

- Geo tracking: Tracking the locations of transactions and comparing them to the usual places where the user makes purchases can help identify suspicious transactions that take place in unusual places.
- Malicious patterns: Identifying malicious patterns of behavior such as rapid the succession of transactions, large sums of money, or purchases in unusual categories, can be a sign of fraud.
- Machine learning models: The use of machine learning algorithms enables automated fraud detection. Historical data is used to train models to recognize patterns that indicate fraud.
- Multi-criteria analyses: Combining different criteria and methods for analyzing transactions can increase accuracy in fraud detection.
- Comparison with reference bases: Checking transactions against a list of known scams or suspicious entities can quickly identify potential fraudsters.
- Expertise: Security and forensics experts can provide in-depth analysis of transactions and recognize suspicious activity that other methods might fail to identify.
- Visual analytics: Data visualization helps identify exceptions and patterns in an intuitive way, making fraud detection easier.

Combining multiple methods and techniques can provide the best results in detecting payment card fraud. It is important that financial institutions regularly monitor transactions, use advanced analytical tools and implement protection strategies to reduce the risk of fraud. Financial institutions pay great attention to the education of clients so that they can recognize certain forms of fraud such as skimming, phishing, carding, *etc*. Thus, in case of phishing, preventive activities are most often aimed at increasing attention and educating users about recognizing suspicious messages and links. This includes a number of activities such as: carefully checking the e-mail address or phone number of the sender, avoiding opening suspicious links to which the received message refers, messages contain errors in grammar and spelling which can often indicate that the message is not authentic, caution with messages in which a quick response is required or a reward is promised. When it comes to carding, financial institutions and merchants apply multiple layers of protection (Sullivan, 2014):

- EMV (Europay, Mastercard, Visa) technology: Chip and PIN technology was introduced to increase security by creating dynamic transaction codes, reducing the usability of stolen data. The main feature of EMV technology is the replacement of traditional magnetic strips on

cards with microchips (EMV chips). These chips generate unique codes for each transaction, making card cloning significantly more difficult. In addition, EMV cards require the entry of a PIN (personal identification number) or a signature by the user, which further increases the security of transactions.
- Multi-factor authentication: Many platforms use multi-factor authentication, requiring additional verification, beyond a simple password, to access an account.
- Transaction tracking: Financial institutions use sophisticated algorithms to detect unusual transaction patterns and behavior, flagging potential fraud for further investigation.

As we can see, international financial institutions are trying to develop special global mechanisms and techniques so as to be able to ensure the security of transactions, data and finances of companies and individual. Misuse and forgery of payment cards has a special characteristic, in terms of damage, which can be twofold – material and reputational. Material damage refers to the specific loss of funds, while reputational damage indicates the loss of clients' trust in the bank. Citizens are usually only inflicted with material damage, which is not achieved through violence or threats. An effective fight against this form of crime requires a comprehensive approach that includes the further development of the protection system related to payment cards, as well as the proactive action of banks and financial institutions in protecting their clients. Preserving confidence in the financial system and protecting against fraud are becoming a priority in order to contain damage and preserve the stability of financial markets.

5. Conclusion

In the era of digital technologies and the Internet, payment cards and cashless payment methods have become the leading method of financial transactions in the modern digital society. This form of payment brings with it many benefits, but it also opens the door to various criminal activities, abuses, and frauds. Due to these risks, the fight against these crimes requires comprehensive measures, including legal regulation, technical protection systems and the training of personnel in the banking sector, in order to recognize and prevent fraud attempts and the misuse of payment cards. Organized criminal groups and cybercriminals pose a serious threat to banking systems and financial institutions around the world. The international scientific and

professional community is increasingly focusing on the prevention of such forms of crime and the reduction of the damage they can cause to individuals and the financial system as a whole. The consequences of payment card abuse and cyber fraud can be far more serious than financial losses. They can damage the reputation of financial institutions and lose the trust of clients. Fraud and attacks on the security of banking systems are a modern challenge that must be solved at the global level. This requires the application of sophisticated technological solutions and innovative legal regulations.

Given the growing importance of digital transactions, it is essential to constantly improve security systems and constantly monitor new techniques and tactics utilized by criminal groups. Only through a comprehensive approach that includes legal, technical, and educational measures, can we effectively combat this type of crime and preserve the integrity of financial systems.

Stojković Numanović Katarina
Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu, Srbija

Merdović Boro
Ministarstvo unutrašnjih poslova Republike Srbije, Policijska uprava za grad Beograd, Srbija

Živaljević Dragan
Akademija za nacionalnu bezbednost, Beograd, Srbija

FALSIFIKOVANJE PLATNIH KARTICA I VISOKOTEHNOLOŠKI KRIMINALITET

REZIME: Falsifikovanje platnih kartica i visokotehnološki kriminal predstavljaju duboko ukorenjene probleme u današnjem društvu. Ovi oblici kriminala primenjuju sofisticirane tehnike i visokotehnološke alatke kako bi ilegalno pristupili finansijskim resursima i izvršili prevare. Falsifikovanje platnih kartica podrazumeva proces stvaranja lažnih kopija debitnih ili kreditnih kartica sa ciljem izvođenja nezakonitih finansijskih transakcija. Pristup podacima sa kartica vrši se korišćenjem različitih

metoda, uključujući skimming (ilegalno prikupljanje podataka sa kartica), phishing (prevara putem lažnih e-mailova ili web stranica) ili fizičku krađu kartica. Paralelno, visokotehnološki kriminal obuhvata širok spektar aktivnosti usmerenih na zloupotrebu digitalnih tehnologija i mreža radi postizanja finansijske koristi ili nanošenja štete pojedincima, kompanijama ili državama. Ovi oblici kriminala često podrazumevaju računarske prevare, sajber napade i digitalne prevare. Ovaj rad ima za cilj da istakne značaj i ozbiljnost problema falsifikovanja platnih kartica, istraži različite metode i obrasce ovih kriminalnih aktivnosti i naglasi specifičnost njihove veze sa visokotehnološkim kriminalom. U istraživanju su primenjene različite metodologije, uključujući kvantitativnu i kvalitativnu analizu sadržaja, komparativnu analizu, kao i deskriptivnu i analitičku statistiku. Dobijeni rezultati jasno ukazuju na rastući značaj ovog problema kako u zakonodavnom tako i u kriminološkom kontekstu, uz konstantan porast broja izvršenih krivičnih dela. Osim toga, istraživanje ističe neraskidivu vezu između falsifikovanja platnih kartica i različitih oblika visokotehnološkog kriminala. Ovi oblici kriminala često se prepliću i zajedno čine sveopšti izazov za pravosudni sistem i bezbednost društva. Na kraju, u radu će biti razmotrene različite strategije i metode kojima se društvo i država mogu suprotstaviti širenju ovih kriminalnih aktivnosti, sa ciljem očuvanja bezbednosti i integriteta finansijskog sistema i zaštite interesa pojedinaca.

***Ključne reči**: falsifikovanje platnih kartica, cyber kriminal, finansijske prevare, skimming, phishing.*

References

1. 12th UN Congress on Crime Prevention and Criminal Justice. (n.d.) Downloaded 2023 September 11, from https://www.unodc.org/documents/crimecongress/12thcrimeCongress/Documents/A_CONF.213_18/V1053828e.pdf
2. 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment Downloaded 2023 September 11, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001F0413
3. Barker, K. J., D'amato, J., & Sheridon, P. (2008). Credit card fraud: awareness and prevention. *Journal of financial crime*, *15*(4), pp. 398-410. https://doi.org/10.1108/13590790810907236

4. Basnet, R. B., & Doleck, T. (2015). Towards developing a tool to detect phishing URLs: A machine learning approach. In *2015 IEEE International Conference on Computational Intelligence & Communication Technology* (pp. 220-223). IEEE. DOI: 10.1109/CICT.2015.63
5. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University-Computer and Information Sciences*. *35*(1), pp. 145-174. https://doi.org/10.1016/j.jksuci.2022.11.008
6. Cui, Q., Jourdan, G., Bochmann, G., Couturier, R., & Onut, I. (2017). Tracking phishing attacks over time. In *Proceedings of the 26th International Conference on World Wide Web*, (pp. 667–676). Perth, Australia. https://doi.org/10.1145/3038912.3052654
7. Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA Downloaded 2023 September 11 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0713
8. Đukić, A. (2017). Krađa identiteta-oblici, karakteristike i rasprostranjenost [Identity theft forms, characteristics and prevalence]. *Vojno delo*, *69*(3), pp. 99-116. DOI:10.5937/vojdelo1703099D
9. Featherly, K. (2016). *ARPANET: United States Defense Program*. Encyclopedia Britannica
10. Krivični zakonik [Criminal Law].*Službeni glasnik RS*, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 i 35/19
11. Marforio, C., Masti, R. J., Soriente, C., Kostiainen, K., & Capkun, S. (2016). Hardened setup of personalized security indicators to counter phishing attacks in mobile banking. In *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*, (pp. 83-92). https://doi.org/10.1145/2994459.2994462
12. Matijašević, J. (2013). *Krivičnopravna regulativa računarskog kriminaliteta* [*Criminal law regulation of computer crime*]. Novi Sad: Pravni fakultet za privredu i pravosuđe u Novom Sadu
13. Merdović, B., Stojković Numanović, K., & Dragojlović, J. (2023). Confiscation of property obtained from a criminal offense as a measure to fight against organized crime. *Kultura polisa*, *20*(1), pp. 87-109. https://doi.org/10.51738/Kpolisa2023.20.1r.87msnd
14. Milošević, M. & Urošević, V. (2009). Krađa identiteta zloupotrebom informacionih tehnologija [Identity theft by misuse of information

technologies]. In: Nešković, S. (ed.), *Bezbednost u postmodernom ambijentu – zbornik radova – knjiga VI* [*Security in a postmodern environment – Proceedings – book VI*] (pp. 53-64). Beograd: Centar za strateška istraživanja nacionalne bezbednost

15. 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.) Downloaded 2023 September 10 from http://www.oecd.org/sti/40644196.pdf
16. Pantić, S. (2018). Komparativna analiza krivičnog djela falsifikovanja i zloupotrebe platnih kartica [Comparative analysis of the criminal offense of forgery and misuse of payment cards]. *Godišnjak Fakulteta bezbednosti*, (1), pp. 391-409. https://doi.org/10.5937/GFB1801391X
17. Pavlović, Z. (2022) Falsifikovanje i zloupotreba bezgotovinskih instrumenata plaćanja i evropski standardi [Counterfeiting and abuse of non-cash payment instruments and European standards]. In: Kostić, J & Matić Bošković (eds.), *Digitalizacija u kaznenom pravu i pravosuđu – tematski zbornik radova međunarodnog značaja* [*Digitalization in Penal Law and Judiciary – Thematic Conference Proceedings of International Significance*] (pp. 31-43). Beograd: Institut za uporedno pravo ; Institut za kriminološka i sociološka istraživanja DOI: https://doi.org/10.56461/ZR_22.DUKPP.03
18. Ross, J. I. (ed.). (2013). *Encyclopedia of street crime in America*. Sage Publications
19. Shahriar, H., Zhang, C., Dunn, S., Bronte, R., Sahlan, A., & Tarmissi, K. (2019). Mobile anti-phishing: Approaches and challenges. *Information Security Journal: A Global Perspective*, *28*(6), pp. 178-193. https://doi.org/10.1080/19393555.2019.1691293
20. Sullivan, R. J. (2014). Controlling security risk and fraud in payment systems. *Federal Reserve Bank of Kansas City, Economic Review*, *99*(3), pp. 47-78
21. Vilić, V. (2019). Phishing and pharming as forms of identity theft and identity abuse. *Balkan Social Science Review*, *13*(13), pp. 43-57
22. Zečević M. (2009). *Bankarstvo* [Banking], Beograd: Evropski Univerzitet.
23. Živaljević, D. (2022). *Radikalizacija društva i terorizam, naučna monografija* [*Radicalization of society and terrorism*]. Beograd: Akademija za nacionalnu bezbednost; Službeni glasnik