UNIWERSYTET JANA DŁUGOSZA W CZĘSTOCHOWIE
Gubernaculum et Administratio 1(29)/2024, t. 1, s. 113–123

http://dx.doi.org/10.16926/gea.2024.01.01.08

dr Dávid TÓTH PhD.
https://orcid.org/0000-0002-2179-7587
University of Pécs, Faculty of Law
e-mail: toth.david@ajk.pte.hu

Recent Trends and Statistics in Financial Identity Theft: The Impact of Artificial Intelligence

Abstract

This research article examines the impact of artificial intelligence (AI) and digital technologies on financial identity theft, particularly in the context of the COVID-19 pandemic, which has accelerated online financial activities. Using a comparative analysis of statistical data from Hungary and global trends, the study explores how AI technologies like deepfake and morphing are reshaping the nature of identity theft. It posits that current Hungarian regulatory frameworks are inadequate to address these sophisticated challenges effectively. Reviewing legal literature and analysing recent statistics, this research aims to highlight emerging trends and suggest improvements for regulatory measures to combat financial identity theft better.

Keywords: Financial Identity Theft, Artificial Intelligence, Cybercrime, Hungarian Legal System, Digital Security.

Introduction

In this research article, I delve into the evolving landscape of financial identity theft, focusing on the profound impact of artificial intelligence (AI) and digital technologies. Prompted by the acceleration of online financial activities due to the COVID-19 pandemic, this study uniquely contributes to existing research by providing a comparative statistical data analysis, comparing the Hungarian context with the global trends.

Guided by two central hypotheses, this research posits that technological advancements related to AI have fundamentally transformed the methods of committing financial identity theft, significantly increasing its scale and complexity. Moreover, it suggests that the current regulatory frameworks in Hungary are inadequately equipped to address these evolving challenges effectively.

This paper explores the impact of artificial intelligence (AI) and digital technologies, such as deepfake and morphing, on financial identity theft. It aims to understand how these technologies are currently reshaping and may further evolve the challenges in identity theft. Additionally, the study evaluates recent statistical data to provide a clear view of emerging trends globally and in Hungary. The methodology combines a comprehensive review of legal literature with statistical data analysis, ensuring a thorough examination of how these technological advances are influencing identity theft.

1. The definition of financial identity theft

Financial identity theft occurs when someone's personal and financial information (such as their name, social security number, or credit card details) is stolen and then used for fraudulent activities with the intention of financial gain. The crime typically unfolds in two phases. In the first phase, the perpetrator illegally acquires personal and financial data through theft, phishing, skimming, etc. In the second phase, the data obtained is used for illicit activities, often called identity fraud in the literature. An example is when someone opens a credit account or purchases using someone else's bank card information without their consent. The primary motive behind financial identity theft is to gain monetary benefit. It's essential to emphasise that this form of crime only occurs when the theft and misuse of the victim's personal information happen without their knowledge or consent.[1]

No specific legal provision directly addresses this criminological concept in the in-force Hungarian criminal law. Typically, in cases of financial identity theft, the following legal statutes are likely to be identified:

— Crimes related to cash substitute payment instruments,[2]
— misuse of personal data,[3]
— information system fraud.

---

[1] I have elaborated more on the definitions in my following article: D. Tóth, *Személyiséglopás az interneten* [*Identity Theft on the Internet*], [in:] "Büntetőjogi Szemle", Vol. 9, 2020/1, pp. 113–119.

[2] I.L. Gál, A pénz- és bélyegforgalom biztonsága elleni bűncselekmények [*Crimes Against the Security of Money and Stamp Transactions*], [in:] P. Polt (ed.), *Új Btk. kommentár: 7. kötet, Különös rész* [*New Criminal Code Commentary: Vol. 7, Special Part*], Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., Budapest, 2013, pp. 193–224.

[3] E. Dániel, A. Péterfalvi, *A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata* [*Criminal Law Protection of Personal Data in Hungary and the Related Practice of the National Authority for Data Protection and Freedom of Information*], [in:] M. Görög, A. Menyhárd, A. Koltay (eds.), *A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül* [*Personality and Its Protection: The Implementation of Article VI of the Fundamental Law within the Hungarian Legal System*], ELTE ÁJK, Budapest, 2017, pp. 405–420.

This crime can have numerous negative consequences for the victims, including financial losses, reduced creditworthiness, and various legal complications.

The COVID-19 pandemic and the ensuing lockdowns had a global impact on people's lives, necessitating many to stay home, work remotely, and maintain online connections. This shift increased dependence on technological tools and time spent in cyberspace, steering criminals towards more online activities and taking advantage of new opportunities presented by the crisis. According to a Hootsuite report in January 2023, individuals spent an average of 6 hours and 37 minutes online daily, approximately a third of their day. Concurrently, as the world's population (8.01 billion in January 2023) grew, so did the number of internet users, surpassing 5.16 billion globally, many of whom are active on social media.[4]

Cybercrime was already a growing issue pre-pandemic, but the crisis gave it a significant boost. The increased online population presented more considerable profit opportunities for criminals. Additionally, lockdown-induced anxiety and fear made people more susceptible to scams and frauds. A particularly concerning trend was the surge in phishing attacks, where fraudsters used fake websites and emails to extract personal data, such as passwords and credit card details.[5]

There was also a rise in malicious software attacks, with hackers employing viruses, worms, trojans, ransomware, and spyware to infiltrate and damage personal computers. Stolen data could then be used for various malicious purposes, such as accessing bank accounts or extorting victims. In some cases, criminals even exploited the pandemic to cover their nefarious activities, such as selling counterfeit medical equipment and drugs at exorbitant prices.

Business-targeted frauds also increased, with scammers exploiting people's fears and uncertainties during the widespread economic disruptions. For instance, in April 2020, the IT service provider Cognizant suffered a ransomware attack, resulting in the theft of sensitive company data.

The pandemic also heightened risks for vulnerable online populations, including children and older people. With schools closed and many seniors relying on online shopping for essentials, these groups spent more time online, becoming more susceptible to various online threats, including file-sharing abuses, inappropriate content, and grooming.

To mitigate the risks of cybercrime, individuals and businesses can take several steps. Good cyber hygiene practices, such as using strong passwords, avoiding suspicious links and downloads, and regularly backing up critical data, are essential for individuals. Two-factor authentication and keeping software up to date can also reduce the risk of cyberattacks. On the other hand, businesses might consider implementing cyber security training programs for employees,

---

[4] https://wearesocial.com/uk/blog/2023/01/digital-2023/ (accessed on: 02.07.2023).

[5] M. DeLiema, D. Burnes, L. Langton, *The Financial and Psychological Impact of Identity Theft Among Older Adults*, [in:] "Journal of Elder Abuse & Neglect", Vol. 32, 2020/4-5, p. 343–362. https://doi.org/10.1080/08946566.2020.1809788.

conducting regular vulnerability tests of their systems, and preparing incident response plans for cyberattacks.

In summary, while the pandemic presented new challenges in cybercrime, it highlighted the importance of proactive measures to protect oneself and organisations. By remaining vigilant and adhering to best practices in cybersecurity, we can reduce the risk of falling victim to these attacks, contributing to a safer and more secure online world.

2. The factors contributing to identity theft

Gupta and others[6] researched the factors contributing to the rise of identity theft. They highlighted the following factors:

— Political and economic factors: The authors argue that the financial and political instability in developing countries increases the likelihood of identity theft. An example of this is when illegal immigrants use forged passports.
— Social factors: How people communicate and their careless handling of personal data also contribute to identity theft. The authors believe that lower education levels and irresponsible use of social media platforms play a role in the spread of identity theft.
— Technological factors: Using the internet and digital technologies facilitates identity theft. A vast amount of personal data is available online, and sophisticated criminal techniques make it easier to acquire this information illegally.[7]

In my view, these factors are relevant and important in addition to the previously mentioned digitalisation trend.

3. The recent trends of financial identity theft

3.1. Statistics on financial identity theft during the pandemic

The pandemic presented significant security challenges for financial institutions and banks. Due to lockdowns, developing and widely implementing online banking was necessary. Remote and online transactions required institutions to adopt new security rules and software for customer identification. Cybercriminal groups exploited security vulnerabilities in online banking,[8] as illegally ac-

[6] Gupta, C. M., Kumar, D., *Identity Theft: A Small Step Towards Big Financial Crimes*, [in:] "Journal of Financial Crime", Vol. 27, 2020/3, pp. 897–910.

[7] Gupta, C. M., Kumar, D., *Identity Theft: A Small Step*…, pp. 897–910.

[8] Ozik G., Sadka R., Shen S., *Flattening the Illiquidity Curve: Retail Trading during the COVID-19 Lockdown,* [in:] "Journal of Financial and Quantitative Analysis", Vol. 56, 2021/7, pp. 2356–2388.

quiring bank card details could lead to substantial financial damages.[9] Wronka Cristoph summarised that financial identity theft became easier than pre-pandemic conditions, as criminals often exploited identification difficulties arising from online banking, causing economic losses. [10]

Statistical data support these observations. Over the past years, several statistics have been published regarding identity theft. According to a study by Javelin Strategy, identity theft in 2020 could be characterised by the following:

— The damages caused by identity theft were estimated at 43 billion USD in 2020. Criminals typically target consumers directly with false offers, phishing emails, and phone calls.
— The number of identity fraud victims decreased by 10% to 49 million, but the average loss per victim increased by 42% to 1100 USD.
— Common perpetration techniques included phishing, vishing, smishing, and impersonation.
— The most common types of identity-related fraud were linked to Covid-19 relief and unemployment benefits.[11]

The following year's data comes from a report by the Federal Trade Commission (FTC) for 2021. According to their report, there were 2.8 million complaints to the FTC. Frauds caused damages to increase by 70% compared to the previous year, estimated at 5.8 billion USD. The report noted nearly 1.4 million complaints specifically related to identity theft. [12]

There have also been several studies about identity theft in 2022. Last year, over 1 million Americans (precisely 1,107,209) reported to authorities that they were victims of identity theft. The nominal value of the damages remained similar, causing about 43 billion USD in losses. 27% of the cases were related to administrative documents or benefits during the pandemic. Georgia had the highest incidence of identity theft. The most affected age group was between 30 and 39 years. An analysis of the victims' income revealed that 51% had annual incomes over 75,000 USD, indicating that wealthier social groups were targeted. 14% of the victims reported losses exceeding 10,000 USD due to identity theft.[13]

---

[9] Hawdon J., Parti K., Dearden T.E., *Cybercrime in America amid COVID-19: The Initial Results from a Natural Experiment*, [in:] "American Journal of Criminal Justice", Vol. 45, 2020/4, pp. 546–562.

[10] Wronka C., *Impact of COVID-19 on Financial Institutions: Navigating the Global Emerging Patterns of Financial Crime,* [in:] "Journal of Financial Crime", Vol. 29, 2022/2, pp. 476–490.

[11] *2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis,* Javelin Strategy, [online] available at https://javelinstrategy.com/research/2020-identity-fraud-study-genesis-identity-fraud-crisis (accessed on: 07.02.2023).

[12] *New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021*. Federal Trade Commission, [online] available at https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0 (accessed on: 07.01.2023).

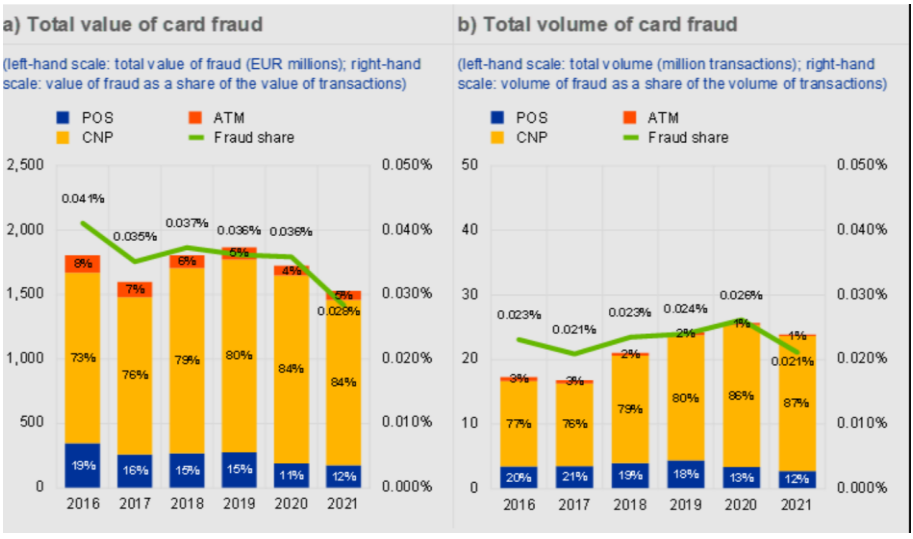
[13] "Identity Theft Statistics," Finmasters, [online] available at https://finmasters.com/identity-theft-statistics/ (accessed on: 07.01.2023).

3.2. The so-called Card-Not Present Frauds

Misuse of bank cards in the online space is referred to in Anglo-Saxon literature as the so-called It is referred to as Card-Not-Present (CNP) fraud, i.e., bank card fraud that takes place in a non-physical space. This type of abuse has become the majority compared to ATM or bank card frauds in the physical space. The value of cardless fraud in the European Union increased by 4.3% in 2019 compared to the previous year, reaching 1.50 billion euros. This amount accounted for 80% of the total value of card fraud. Most cardless fraud is related to cross-border transactions, especially within the European Union's Single Payments Area (SEPA). Between 2015 and 2019, the value of cardless fraud increased by 15.9%.

According to the European Central Bank report, almost half a million (precisely 459,297) cases of bank card fraud were received in 2020.[14] In 2021, however, CNP fraud decreased by 12.1 per cent compared to 2020. The amount of damage caused by the scam was 1.28 billion euros. Enhanced security regulations, such as customer authentication, have significantly reduced CNP fraud in the SEPA region. Despite the decrease in CNP frauds in the European Union, the European Central Bank emphasises in its report that there will still be challenges in developing online payment systems to prevent future crimes.[15]

Figure np. 1: Total Value and Volume of Card Fraud in the SEPA Region (2016–2021)"



Source: https://www.ecb.europa.eu/pub/cardfraud/html/cardfraudreport202305/ecb.cardfraudreport202305.en_img0.png?9c100455fefc0818c7d43d3f64416f5c (accessed on 01.07.2023).

[14] https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html (accessed on: 01.07.2023).

[15] https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html (accessed on: 01.07.2023).

The diagram above shows how the rate of bank card fraud has developed in the EU annually. Among these, CNP fraud stands out significantly, with a rate of 87 per cent in 2021. This is followed by fraud on POS terminals, ranging between 10-20 per cent annually, and ATM fraud is the most minor proportion.

Research conducted by Yenal and others highlights the significant role of technology in CNP fraud. Smartphones and publicly accessible computers can be particularly risky for these frauds. They also noted that outdated mobile devices are often less secure than traditional computers, making them more vulnerable to criminal exploitation. Regular software updates can help prevent these types of fraud.[16]

4. Criminal statistics in Hungary

Since Hungary does not have a specific legal framework for identity theft, obtaining a precise picture of its prevalence is challenging. However, the following points have been highlighted about financial identity theft-related crimes:

Table no. 1. Annual Statistics of Crimes Related to Financial Identity Theft[17]

NUMBER OF CRIMES/YEAR	2019	2020	2021	2022
Counterfeiting of cash substitute payment instrument	52	784	1	12
Aiding in the Counterfeiting of cash substitute payment instrument	1	0	0	0
Misuse of cash substitute payment instrument	246	218	134	136
Misuse of personal data	1478	942	1078	2185
Information system fraud	2624	3400	2681	4084

Source: https://bsr.bm.hu/Document (accessed on: 01.07.2023).

With the misuse of cash-substitute payment instruments now secondary to fraud involving information systems, the latter's frequency has notably increased in criminal statistics. In 2022, there was a marked rise in incidents of

[16] Akdemir, N., Serkan Y. *Card-not-Present Fraud Victimization: A Routine Activities Approach to Understand the Risk Factors.*" [in:] "Güvenlik Bilimleri Dergisi" 9, 2020/1. pp. 243–268.

[17] https://bsr.bm.hu/Document (Accessed on 01.07.2023).

personal data misuse, a significantly noteworthy trend. Concurrently, there has been a substantial uptick in the fraud rate committed using information systems.

It is important to remember that, particularly in cases of online crimes, there is a high degree of latency, especially for crimes related to identity theft. This means that many such crimes may go unreported or undetected.

5. Artificial intelligence and identity theft

The potential challenges of identity theft in the future include deepfake and morphing technologies.

With the dynamic development of artificial intelligence, identity theft could reach a new level of danger, where not only identification data but also the physical appearance of individuals can be falsified. This applies to technologies like deepfake and morphing, both used for manipulating digital images or videos but in different ways and for other purposes.

According to the Oxford Dictionary, "deepfake" is a technology that digitally modifies a person's appearance in a video to make them look like someone else. This also includes stealing someone's voice to generate fake audio recordings. Deepfake videos or audio recordings use artificial intelligence, particularly deep learning technology, to create images of false events or manipulate existing video footage. These "deepfakes" can create the illusion that someone said or did something they did not. This is achieved by training a machine learning model on a large amount of visual data (e.g., photos or videos of a person's face) and then using the model to create new images or videos that mimic the appearance and behaviour learned from the training data.

Morphing, on the other hand, is a technique that involves transforming or merging one image into another. In the case of faces, it usually involves blending two or more different faces to create a composite image that shares characteristics of the original images. This process consists of two steps: first, the "warping" step alters the shape of one image to match the other, and then in the "cross-dissolving" step, the colours of the two images are blended to create a smooth transition where one face appears to transform into the other. This technique allows merging two faces into a single image with characteristics of both original faces.[18]

One notable example of a crime related to deepfake was an incident in September 2019, when attackers used the voice of the CEO of a UK-based energy company. The attackers contacted the company's managing director using an AI-generated voice almost identical to the real CEO's. They instructed the

[18] Agarwala A., Nalini R., *Manipulating Faces for Identity Theft via Morphing and Deepfake: Digital Privacy*, [in:] "Deep Learning" 2023, Vol. 48, p. 223.

managing director to urgently transfer $243,000 to a specified account. The executive complied, and the money was transferred to a Hungarian account, which was then moved to Mexico and other locations, complicating identification. The fraudulent nature of the transaction was discovered too late, and the money could not be recovered. This case involved the use of deepfake technology, psychological manipulation (social engineering), and identity theft.[19]

Summary and conclusion

This research paper presented a comprehensive analysis of the escalating issue of financial identity theft, especially in the context of the COVID-19 pandemic, which has drastically increased internet dependency and online financial activities. As a scientific study, it examines the technological advancements and the adaptive measures financial organisations take to mitigate emerging security threats.

The pandemic has significantly expanded the scope of online banking, introducing substantial security challenges for financial institutions. These organisations have been compelled to implement new security protocols and customer identification software to safeguard against heightened risks. The analysis reveals that the damages from identity fraud have surged, highlighting substantial economic losses and legal challenges for the victims. Moreover, while physical card fraud incidents have dwindled, Card-Not-Present (CNP) fraud has notably increased. Continuous security developments, regular updates, and comprehensive user education are imperative to combat these threats. Users must recognise potential dangers and employ effective strategies to protect themselves against various forms of financial identity theft, including phishing, vishing, and smishing.

Artificial intelligence technologies such as deepfake and morphing are setting the stage for a new era of financial identity theft, where criminals can steal identification data and convincingly alter physical appearances in digital media. Deepfake technology utilises advanced machine learning to create or alter video and audio recordings, making it possible to fabricate realistic videos and audio of individuals saying or doing things they never did. Morphing blends multiple images to forge composite identities that bypass biometric security measures.

With the significant increases in various types of crimes related to identity theft, it is evident that the existing provisions in the Hungarian Criminal Code are inadequate to tackle this escalating issue effectively. This inadequacy impedes the successful prosecution of such crimes and creates a legal vacuum that

[19] Unusual CEO Fraud via Deepfake Audio Steals US $243,000 from U.K. Company, [online] available at: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company [accessed on: 02.07.2023].

demands urgent attention to ensure comprehensive individual protection. To enhance the legal framework and provide robust protection against identity theft, it would be wise to consider regulating this crime through specific legal frameworks incorporating successful strategies from foreign models (like in France). The absence of a distinct statutory provision for identity theft in the Hungarian Criminal Code complicates the application of existing laws to these crimes. Thus, I recommend the introduction of a particular statutory provision for identity theft to address these gaps effectively.[20]

Bibliography

„2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis, Javelin Strategy" [online] available at https://javelinstrategy.com/research/2020-identity-fraud-study-genesis-identity-fraud-crisis (accessed on: 07.02.2023).

Agarwala, A., Nalini, R. „*Manipulating Faces for Identity Theft via Morphing and Deepfake: Digital Privacy, „Deep Learning*", 2023, Vol. 48, p. 223.

Akdemir, N., Serkan, Y., *„Card-not-Present Fraud Victimization: A Routine Activities Approach to Understand the Risk Factors, „Güvenlik Bilimleri Dergisi",* Vol. 9, 2020/1, pp. 243-268.

Dániel, E., Péterfalvi, A. *„A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata,* [in:] M. Görög, A. Menyhárd, A. Koltay (eds.), *A személyiség és védelme: Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül*, ELTE ÁJK, Budapest, 2017, pp. 405-420.

DeLiema, M., Burnes, D., Langton, L*., The Financial and Psychological Impact of Identity Theft Among Older Adults, „Journal of Elder Abuse & Neglect",* Vol. 32, 2020/4-5, pp. 343-362. https://doi.org/10.1080/08946566.2020.1809788.

Gál, I. L. *„A pénz- és bélyegforgalom biztonsága elleni bűncselekmények"* [in:] P. Polt (ed.), Új *Btk. kommentár: 7. kötet, Különös rész, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt.,* Budapest, 2013, pp. 193-224.

Gupta, C. M., Kumar, D., *„Identity Theft: A Small Step Towards Big Financial Crimes"* Journal of Financial Crime, Vol. 27, 2020/3, pp. 897-910.

Hawdon, J., Parti, K., Dearden, T. E., *Cybercrime in America amid COVID-19: The Initial Results from a Natural Experiment,* „American Journal of Criminal Justice", Vol. 45, 2020/4, pp. 546-562.

https://bsr.bm.hu/Document (accessed on: 01.07.2023).

https://wearesocial.com/uk/blog/2023/01/digital-2023/ (accessed on: 02.07.2023).

[20] See further in: Tóth, D., *Az identitáslopás szabályozása angolszász államokban* [*Regulation of Identity Theft in Anglo-Saxon States*]*,* [in:] N. E. Baráth, J. Mezei (eds.), Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével 2020, Doktoranduszok Országos Szövetsége, Budapest, 2020, pp. 228-237.

https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html (accessed on: 01.07.2023).

https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html (accessed on: 01.07.2023).

„Identity Theft Statistics Finmasters" [online] available at https://finmasters.com/identity-theft-statistics/ (accessed on: 07.01.2023).

New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021. Federal Trade Commission, [online] available at https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0 (accessed on: 07.01.2023).

Ozik, G., Sadka, R., Shen, S., *Flattening the Illiquidity Curve: Retail Trading during the COVID-19 Lockdown,* „Journal of Financial and Quantitative Analysis", Vol. 56, 2021/7, pp. 2356-2388.

Tóth, D., *Az identitáslopás szabályozása angolszász államokban*, [in:] N. E. Baráth, J. Mezei (eds.), *Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével 2020,* Doktoranduszok Országos Szövetsége, Budapest, 2020, pp. 228-237.

Tóth, D., *Személyiséglopás az interneten,* „Büntetőjogi Szemle", Vol. 9, 2020/1, pp. 113-119.

„Unusual CEO Fraud via Deepfake Audio Steals US $243,000 from U.K. Company", [online] available at: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company (accessed on: 02.07.2023).

Wronka, C., *Impact of COVID-19 on Financial Institutions: Navigating the Global Emerging Patterns of Financial Crime*, „Journal of Financial Crime", Vol. 29, 2022/2, pp. 476-490.

Najnowsze trendy i statystyki w zakresie kradzieży tożsamości finansowej: wpływ sztucznej inteligencji

Streszczenie

Niniejszy artykuł badawczy bada wpływ sztucznej inteligencji (AI) i technologii cyfrowych na kradzież tożsamości finansowej, szczególnie w kontekście pandemii COVID-19, która przyspieszyła działania finansowe online. Wykorzystując analizę porównawczą danych statystycznych z Węgier oraz trendów globalnych, badanie to analizuje, jak technologie AI, takie jak *deepfake* i *morphing*, przekształcają naturę kradzieży tożsamości. Stwierdza, że obecne węgierskie ramy regulacyjne są niewystarczające, aby skutecznie sprostać tym zaawansowanym wyzwaniom. Przeglądając literaturę prawną i analizując najnowsze statystyki, niniejsze badania mają na celu podkreślenie pojawiających się trendów i sugerowanie ulepszeń w środkach regulacyjnych, aby lepiej zwalczać kradzież tożsamości finansowej.

Słowa kluczowe: kradzież tożsamości finansowej, sztuczna inteligencja, cyberprzestępczość, węgierski system prawny, bezpieczeństwo cyfrowe.