The Effect of the KiberPajzs Initiative on Fraud Detected in Electronic Payments in Hungary

Gabriella BIRÓ
Ludovika University of Public Service, Budapest, Hungary
biro.gabriella@uni-nke.hu

Abstract

The paper examines what effect the KiberPajzs initiative has on fraud detected in electronic payments in Hungary for the 2023-2024 period. First the current electronic payment fraud landscape of Hungary is described through cybercrime tendencies, the impact of digitalization on banking, and the regulatory background of electronic payments. Then the KiberPajzs initiative is introduced together with its related communicational, regulatory and law enforcement projects. Finally, the recent quarterly payment fraud data published by the Central Bank of Hungary is examined and the effects of KiberPajzs are evaluated. The author argues that the decrease in the number and value of fraudulent electronic transactions and the increase in identified failed fraud attempts coincide with the activities of the KiberPajzs initiative.

Index terms: cybercrime, electronic payments, financial education, fraud prevention, payment fraud

1. Introduction

With the increasing use of digital banking channels and the growing sophistication of tools available for cybercriminals to target their victims, the number and value of fraudulent electronic payments is on the rise worldwide. In Hungary, authorities, banks and other stakeholders have joint forces to counter this tendency and started the KiberPajzs (CyberShiled in English) initiative in 2022 as a coordinated effort to address the issue [1]. This paper seeks to describe the various aspects of the KiberPajzs initiative and show the effect it has been having on the number and value of fraudulent payments.

The question of what effect the KiberPajzs initiative has had on fraudulent electronic transactions in Hungary will be examined through the analysis of the quarterly payment reports regularly published by the Central Bank of Hungary (Magyar Nemzeti Bank - hereinafter referred to as MNB) [2]. These datasets are based on the quarterly regulatory reporting of payment service providers and commercial banks in Hungary and contain data on fraud and attempted fraud observed in card payments and the electronic payments systems. The scope of this paper is limited to electronic payments (credit transfers) and does not include card payment related data. Other sources of data are also available such as the 2024 Report on Payment Fraud by the European Central Bank [3] and the annual report of the Hungarian Financial Arbitration Board [4], but even though these confirm the identified trends, both reports have a different data frequency (half-yearly or annual) and larger time lag compared to the MNB data.

2. The Current Landscape of Electronic Payment Fraud in Hungary

Fraudulent transactions identified in electronic payments may fall into two basic categories: fraud cases conducted via the payment system - such as traditional scams utilizing electronic payments -, and payment fraud cases that are made possible because of the electronic channels such as phishing for electronic banking credentials. Both categories rely to some extent on the communication with potential victims and until recent years the Hungarian language provided a barrier to criminals that was difficult to overcome, because the majority (51.3% in 2022) of the adult Hungarian population does not speak any foreign language [5]. With the development of artificial intelligence and Large Language Models, fraudsters are now able to create credible messages in Hungarian [6],[7]. Vishing (voice phishing, usually phone calls) is also becoming very common, especially coupled with phone number spoofing, where the calling number displayed for the target is that of a commercial bank or other trusted party such as the Central Bank of Hungary [8].

2.1. Payments Related Cybercrime in Hungary

The annual Payment Systems Report published by the MNB contains a section on the fraud cases "observed through electronic payments", meaning both electronic payment fraud that is made possible by the electronic channel and other types of fraudulent payments via electronic channels. Card payment related and non-card (credit transfer) data is published separately, as the governing rules and IT systems involved in the transactions are different for card and non-card payments. A sharp rise in both the number and value of non-card fraudulent transactions, but Hungary is still among the less affected countries [9].

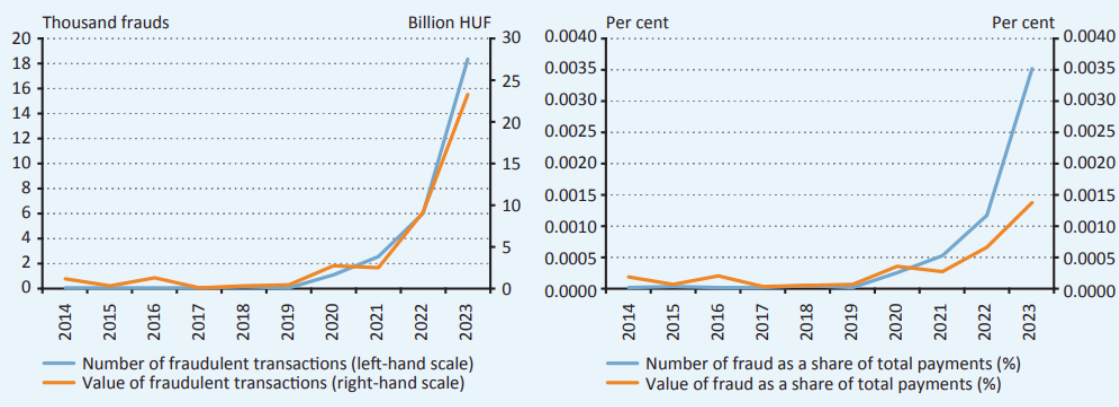

Fig. 1. Volume and value of non-card fraud published by MNB [9]

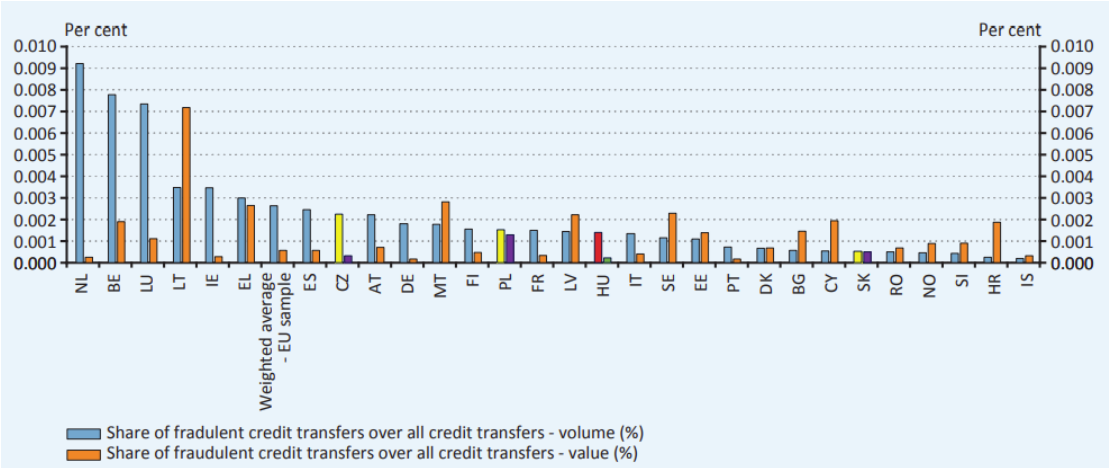

Fig. 2. Volume and value share of successful fraudulent credit transfers over all credit transfers (EBA, 2022) [9]

2.2. The Effects of Digitalization on Electronic Payments

In addition to the language factor, another major contributor to the rising fraud trends may be the rapid digitalization of the payment service providers and the COVID-19 induced transfer of consumers/clients to the digital channels (as opposed to visiting the brick-and-mortar bank branches). Some of these clients are not comfortable with the use of electronic channels and their lack of computer literacy makes them vulnerable to online fraud. On the other hand, now all Hungarian banks offer online current account opening and personal loan applications [10], thus serving their increasingly digitalized clients, but also providing a bigger attack surface for fraudsters.

2.3. Regulatory Background

The legal framework for cybercrimes in Hungary is in line with the Budapest Convention on Cybercrime [11], covering basically all cases of electronic payment fraud that are not covered by the fraud related article (§ 373, "csalás") of the Hungarian Criminal Code [12], which is favoured by judicial practice. However, the Budapest Convention is considered by some to be outdated and in need of a review [13].

Hungary has implemented the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2, [14]) in its payment regulations, therefore the regulatory environment is very similar to all other EU countries. The PSD2 basically mandates the use of strong authentication (two-factor authentication) for online transactions [15]. The original purpose of the regulation was to increase the security of the payment systems and protect the consumers by defining strict liability rules for fraudulent transactions. According to the European Central Bank, "observed fraud rates for credit transfers remained consistently at 0.002% or below across all categories analysed" in 2022 and 2023 [3]. However, the unexpected result of the PSD2 implementation was that criminals found new ways to target consumers and trick them into handing over their e-banking credentials, resulting in increasingly large losses on the client side with 98.3% of the financial liabilities falling to consumers [9]. This resulted in a strong perception that banks do not do enough to protect their customers and has begun to undermine the trust in the banking system, spurring MNB to take action.

3. The KiberPajzs Initiative

The founding members of the KiberPajzs initiative were the Central Bank of Hungary (MNB) both in its capacities of financial supervisor and consumer protection authority, the Hungarian Banking Association, the National Media and Infocommunications Authority (NMHH), the National Cyber Security Center of Hungary (NBSZ-NKI) and the Hungarian Police. The five original founding organizations signed a cooperation agreement on 7th November 2022 and the website https://www.kiberpajzs.hu was launched at the same time. The founders were later joined by the Hungarian Financial Arbitration Board, the Ministry of Justice (also including the network of victim support centres), the Hungarian State Treasury, the Supervisory Authority for Regulated Activities (SZTFH), the Ministry of Economics and the National Protective Service (NVSZ) [1]. These powerful participants launched a comprehensive educational programme to improve customers' digital financial awareness through a unified, ongoing communication campaign and to help consumers to detect and prevent fraud at an early stage. In addition to the communication campaign, another very important benefit of the initiative is the sharing of knowledge between experts on fraud scenarios, analysis of fraud scripts, modus operandi, characteristics and trends, and more efficient prevention and protection processes.

The outcomes of the initiative have been manyfold:

- the awareness campaign is ongoing, with various platforms and messages to a wide variety of target audiences from billboards to television spots, TikTok videos and paper handout at pensioners' club events by local police officers;
- smoother and more efficient interaction between law enforcement agencies, banks and other authorities, resulting in faster interventions and successful cases of asset recovery;
- streamlined journey for fraud victims, with guidance for banks on how to communicate sympathetically to fraud victims [1], improved police reporting, unified messages for consumer protection and redressal procedures and easier access to victim support;
- improved legal framework for cooperation, information sharing and fraud prevention thanks to the participation of major regulators.

4. Other Initiatives Related to KiberPajzs

Some participants of the KiberPajzs initiative also added their own spinoffs to the project and enhanced the actions of KiberPajzs. Particularly the MNB, the Hungarian Banking Association (together with MédiaUnió) and the Hungarian Police launched successful actions.

4.1. MNB action

MNB issued a comprehensive Fraud Recommendation in 2023 for supervised payment service providers (mainly banks) that covers the prevention, detection and management of fraud observed through payment services and comes into force in three stages: 1st January 2024 for "quick wins", 1st September 2024 for requirements that need a larger implementation effort, 1st March 2025 for real-time fraud monitoring systems [16]. The Fraud Recommendation introduced new requirements on contracting, on the delivery of new payment instrument to the customers (such as new payment cards or mobile banking activation), on the lines of defence preventing external and internal fraud, the design and operation of the IT environment and process controls, analysis and lessons learnt of fraud cases, improving customers' security awareness, transaction limits and restrictions, strong customer authentication by third party service providers, mitigation of the risks attached to the multifunctional instrument providing any element of strong customer authentication, transaction monitoring mechanisms related to fraud, and the requests for rectification related to unauthorised payment transactions. It is worth noting that though the recommendations of MNB are not legally binding, MNB evaluates the compliance to the recommendations during its supervisory activities, meaning that noncompliance can result in supervisory actions.

In addition to the Fraud Recommendation, the MNB has also issued several circulars detailing expectations about the use of KiberPajzs communication materials by banks of drawing the attention of banks to specific modus operandi for electronic payment fraud [17]. Some of these circulars are not public, so they are not published but only shared with the intended recipients.

The most resource intensive action by MNB is the initiation of a central fraud monitoring and prevention solution that will be developed and operated by GIRO, the MNB owned Hungarian clearing house that processes all domestic transactions [18]. The development is expected to go live in 2025, so it is not relevant for the current payment trends.

4.2. The Mátrix Project

The Hungarian Police announced the Mátrix project in October 2023 with the intent to tackle online fraud [19]. They established a new strategic unit specialized in cybercrime, with a provisional headcount of 300 officers and a mandate to cooperate across the law enforcement organization countrywide. They have ever since encountered some serious success stories such as dismantling a complete call centre of 41 individuals specialized in Hungarian language vishing and AnyDesk fraud

in cooperation with the Ukrainian police [20], [21]. These actions have resulted in a perceivable drop of criminal activity.

The new unit is also very active in communicating both the fraud prevention messages and the success stories and organizing online and offline educational event for various target audiences.

4.3. The MédiaUnió Campaign

MédiaUn[22]association of media content providers, who donate their free spots for social purposes and select a topic each year. In 2023 and 2024 they decided to address online fraud and cooperated with the Hungarian Banking Association and the KiberPajzs subject matter experts to create messages that are consistent with the KiberPajzs campaign but have a distinct design. The MédiaUnió campaign significantly amplified the fraud prevention and security awareness messages and provided new channels of communication.

4.4. Pénz7

Pénz7 [22] is the Hungarian equivalent of the European Money Week organized by the European Banking Federation in order to provide financial education and raise awareness about money and personal finances. Throughout one week in March, many financial education events are organized across Europe by national banking associations and the European Banking Federation. [23]. In Hungary, the main targets of the educational campaign are schools, with different materials for all ages of children. In 2023, the special focus of the campaign was the security of digital finance, with professional volunteers touring the country and delivering lectures and classes and various educational institutions [24].

5. Fraud Data Published by the Central Bank of Hungary

In accordance with Article 96(6) of PSD2 [14], payment service providers (mostly banks) are required to report statistical data on fraud relating to different means of payment to their competent authorities, that is the MNB in case of Hungary. These data are collected for every quarter of the year and published by the MNB regularly. The changes in reporting methodology sometimes make comparisons difficult, but the reporting regime under PSD2 is consistent enough for 2020-2024 to allow for analysis. Major changes are expected in the reporting framework for 2025 due to regulatory changes.

The data reported to MNB is collected through the official reporting platform of MNB and payment service providers failing to submit reports are subject to supervisory actions such as fines, but the different reporting practices of the payment service providers (mainly banks) make the data somewhat less reliable, even though MNB publishes a detailed guidance on how and what to report [25]. Payment fraud related data is reported currently in form P12. This data is more relevant and timely than other data sources such as the complaints handled at the financial consumer protection authority, the Financial Arbitrage Board of police data, because the fraudulent transactions are reported for the time period when they took place (as opposed to when the client decides to complain or file a police report, which may be typically weeks later in case of complaints) and the latency (not reporting) is much smaller than in case of the police or other sources.

Figure 3. demonstrates the rise of the number and value of fraudulent transactions, as described in the MNB Payment Report for 2023 [9], but we see a significant drop in both the amount and the number of successful fraud in the fourth quarter of 2023, when we would expect to see a rise because of the increase in online shopping (and related fraud) due to the Christmas holidays. In 2023 Q4 the KiberPajzs initiative already took momentum, while the MNB Fraud Recommendations were not yet in force and the Mátrix project had just been announced, so the most likely explanation is that the communication campaign and other KiberPajzs efforts were successful.

In 2024 Q1 we see a spike in the numbers, but the increase in value was caused by a one-off event, a large retail store loosing 6 billion Forints (€15.5 million) to fraud [26]. In 2024 Q2 the trend is declining again.

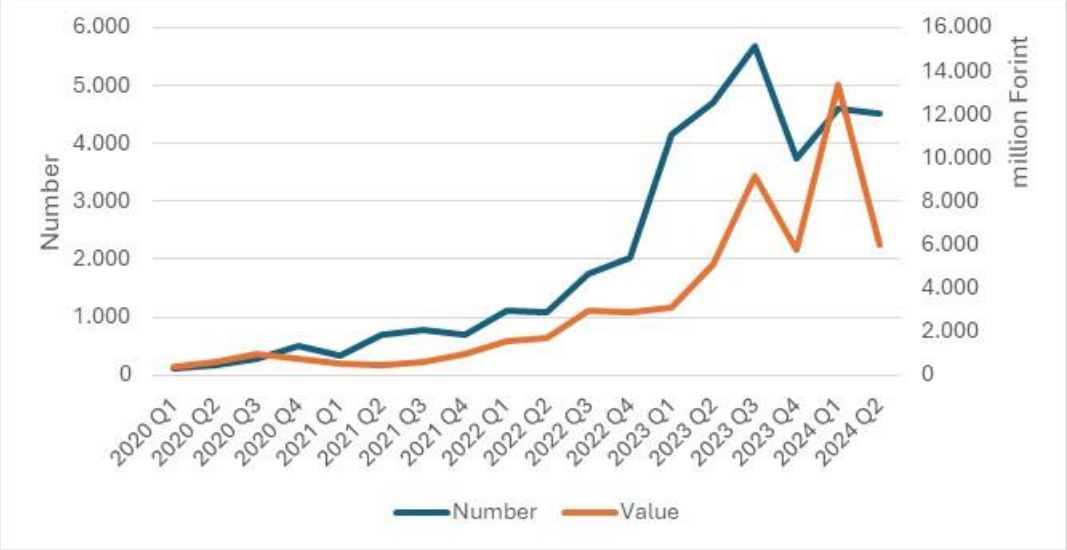

Fig. 3. The number and value of fraudulent transactions in electronic payments (edited by the author based on the dataset published by MNB [2])

Figure 4. shows the number and value of unsuccessful fraudulent transaction attempts, as reported by payment service providers to MNB. The criteria for reporting are the following: "*[…]any case in which the loss incurred by the payment service provider or the customer does not occur (typically the payment order is not executed or the fraudulent customer's claim for reimbursement is rejected by the reporting party). These include cases where the payer's payment service provider intervenes before the payment order is approved, typically as a result of the fraud filtering mechanisms in place, regardless of the origin or main motive of the fraud."*[25] In case the value of the attempted fraud is not known, the case if reported with a value of 0, so the increase the value seen in 2023-2024 means that more exact data is available, rather than an increase in actual fraud attempts. The drop in the number of attempts can also indicate that fewer frauds attempts are blocked by the banks, because clients are more likely to recognize fraud attempts at an earlier stage.

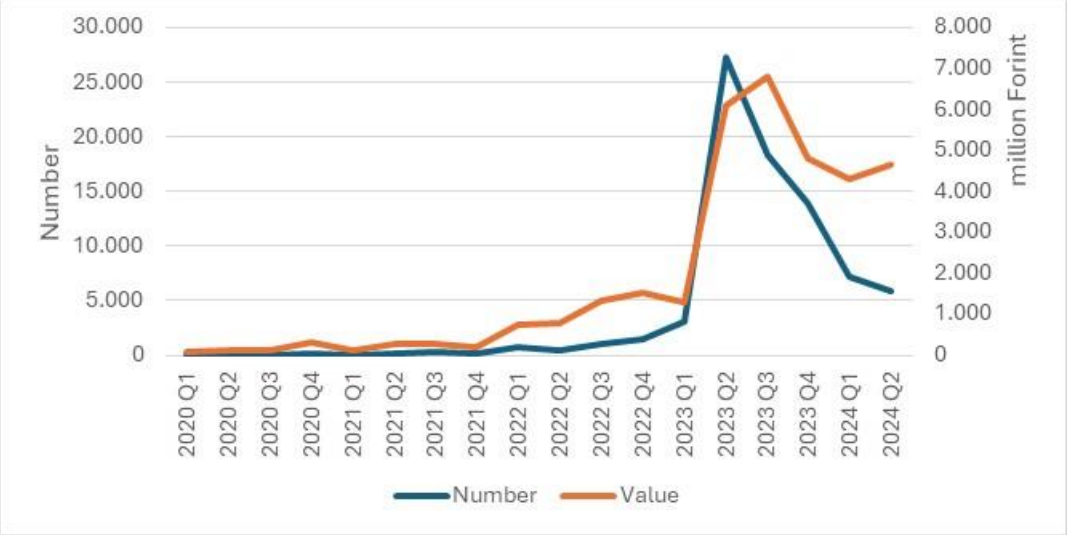

Fig. 4. The number and value of unsuccessful fraudulent transaction attempts in electronic payments (edited by the author based on the dataset published by MNB [2])

6. Conclusion

The data on fraudulent transactions and unsuccessful fraud attempts in electronic payments published by MNB suggests that the KiberPajzs initiative had a positive effect on fraud prevention. Other initiatives that might have had an impact were not mature enough during the reporting period to significantly influence the numbers. MNB itself also made a moderately optimistic announcement about the success of KiberPajzs in 2024, after the release of the 2023 Q3 data [27]. The fight against fraud is never over and we have yet to see what effect the central fraud prevention system will have on payment fraud or is cyber criminals come up with new modus operandi, but for now it seems that KiberPajzs is effective in decreasing electronic payment fraud.

References

[1]. Magyar Nemzeti Bank, 'Kiberpajzs'. Accessed: Oct. 27, 2024. [Online]. Available: https://kiberpajzs.hu/

[2]. Magyar Nemzeti Bank, 'Pénzforgalmi visszaélések'. Sep. 16, 2024. Accessed: Oct. 17, 2024. [Online]. Available: https://statisztika.mnb.hu/idosor-3644

[3]. European Central Bank, 'ECB and EBA publish joint report on payment fraud'. Aug. 01, 2024. Accessed: Oct. 27, 2024. [Online]. Available: https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.en.html

[4]. Magyar Nemzeti Bank, 'Jelentés a Pénzügyi Békéltető Testület éves tevékenységéről 2023.' Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/bekeltetes/bemutatkozas/eves-jelenteseink/jelentes-a-penzugyi-bekelteto-testulet-eves-tevekenysegerol-2023

[5]. Eurostat, 'Number of foreign languages known (self-reported) by sex'. Eurostat, 2022. doi: 10.2908/EDAT_AES_L21.

[6]. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, European Union Agency for Law Enforcement Cooperation. LU: Publications Office, 2024. Accessed: Jul. 28, 2024. [Online]. Available: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

[7]. Europol, Facing reality?: law enforcement and the challenge of deepfakes : an observatory report from the Europol innovation lab. LU: Publications Office, 2024. Accessed: Oct. 17, 2024. [Online]. Available: https://data.europa.eu/doi/10.2813/158794

[8]. 'Ismét csalók próbálnak visszaélni az MNB nevével'. Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2023-evi-sajtokozlemenyek/ismet-csalok-probalnak-visszaelni-az-mnb-nevevel

[9]. Magyar Nemzeti Bank, 'Payment Systems Report'. Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/en/publications/reports/payment-systems-report

[10]. Magyar Nemzeti Bank, 'FinTech and Digitalisation Report, July 2024'. Jul. 2024. Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/en/publications/reports/fintech-and-digitalisation-report/fintech-and-digitalisation-report-july-2024

[11]. Convention on cybercrime | EUR-Lex. Accessed: Oct. 27, 2024. [Online]. Available: https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html

[12]. Btk. (új) - 2012. évi C. törvény a Büntető Törvénykönyvről - Hatályos Jogszabályok Gyűjteménye. Accessed: Oct. 27, 2024. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1200100.tv

[13]. C. Krasznay, 'Húsz év a globális kiberbűnözés elleni küzdelemben : A Budapesti Egyezmény értékelése', Külügyi Szemle, vol. 20, no. Különszám, pp. 191-214, 2021, doi: 10.47707/Kulugyi_Szemle.2021.2.09.

[14]. DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on Payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. Accessed: Oct. 27, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32015L2366

[15]. COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. Accessed: Oct. 27, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32018R0389

[16]. Magyar Nemzeti Bank, Recommendation No 5/2023 (VI.23.) of the Magyar Nemzeti Bank on the prevention, detection and management of abuses observed through payment services.

[17]. Magyar Nemzeti Bank, 'Vezetői körlevelek'. Accessed: Oct. 27, 2024. [Online]. Available: https://www.mnb.hu/felugyelet/szabalyozas/felugyeleti-szabalyozo-eszkozok/vezetoi-korlevelek

[18]. GIRO, 'Összefogással a biztonságos banki tranzakciókért'. 2024. Accessed: Jul. 21, 2024. [Online]. Available: https://www.giro.hu/news/biztonsagos-banki-tranzakciok

[19]. ORFK, 'Mátrix Projekt a kiberbiztonságért', A Rendőrség hivatalos honlapja. Accessed: Oct. 27, 2024. [Online]. Available: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/matrix-projekt-a-kiberbiztonsagert

[20]. 'Mátrix Projekt - közös nemzetközi akcióban számolták fel a rendőrök az eddigi legnagyobb illegális call center hálózatot', A Rendőrség hivatalos honlapja. Accessed: Oct. 27, 2024. [Online]. Available: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/matrix-projekt-kozos-nemzetkozi-akcioban

[21]. 'Поліція Закарпаття ліквідувала масштабну мережу шахрайських кол-центрів - затримано лідера та 18 членів злочинної організації | Національна поліція України'. Accessed: Oct. 27, 2024. [Online]. Available: https://www.npu.gov.ua/news/politsiia-zakarpattia-likviduvala-masshtabnu-merezhu-shakhraiskykh-kol-tsentriv-zatrymano-lidera-ta-18-chleniv-zlochynnoi-orhanizatsii

[22]. 'PÉNZ7 - Pénzügyi és Vállalkozói Témahét', PÉNZ7 - Pénzügyi és Vállalkozói Témahét. Accessed: Oct. 27, 2024. [Online]. Available: https://www.penz7.hu/

[23]. 'EUROPEAN MONEY WEEK', EBF. Accessed: Oct. 27, 2024. [Online]. Available: https://www.ebf.eu/europeanmoneyweek/

[24]. E. Terták and L. Kovács, 'Fókuszban a pénzügyi biztonság kibertérben is - PÉNZ7', G.É.P., vol. 10, no. 1, pp. 5-20, 2023, doi: 10.33926/GP.2023.1.1.

[25]. Magyar Nemzeti Bank, 'Kapcsolódó előírások, technikai segédletek'. Accessed: Oct. 27, 2024. [Online]. Available: https://aszp.mnb.hu//eloirasok-technikai-segedletek

[26]. J. Kwak, 'Pepco Group N.V. - Notice regarding Hungarian business', Pepco Group. Accessed: Oct. 27, 2024. [Online]. Available: https://www.pepcogroup.eu/media-news/pepco-group-n-v-notice-regarding-hungarian-business/

[27]. Magyar Nemzeti Bank, 'Tavaly év végén csökkentek az átutalásos kibercsalások, de továbbra is fokozott figyelem kell'.