Adapting the Liability of Payment Service Providers to the New Types of Fraud

Ștefania STANCU[1]
Alexandru-Constantin MIU[2]

I. Introductory Aspects

1. Novelty of the Topic

The present work will primarily address the field of „financial law, where the end usually marks a new beginning, as will be seen when highlighting the evolution of any legislation related to the banking and financial field in general, and the EU legislative framework that regulates banking activity, credit institutions and financial markets"[3], do not make the discordant note.

In the context of rapid technological development and innovation over recent years, new legislative gaps have emerged in practice, which could infringe upon the fundamental rights of those involved in various economic processes. The expansion of new technologies raises increasing challenges in judicial practice due to insufficient or even ineffective regulations that fail to fully cover new ways of circumventing provisions, thus triggering legal liability issues through these loopholes.

Furthermore, the technological advancement in banking, coupled with dependency on new technologies and their integration into banking and interbank processes, alongside the emergence of new types of online transactions and an increase in such operations, has brought new threats to the stability of financial institutions, state economies, and the global economy, as well as to the interests of private economic actors (consumers). These threats have highlighted the need to define operational risks as a distinct category, prompting a reconsideration of prudential risk policies, now a fundamental aspect of the financial-banking field.

2. General Aspects Regarding Key Issues in Adapting the Liability of Payment Service Providers to New Types of Fraud

An overarching look at the challenges arising in adapting PSPs' liability to new types of fraud raises many essential questions: "How should, or rather, how must the liability of payment service providers be adapted in light of a continuously evolving economic and digital sector?" "What are the real issues within the current

[1] Student, Faculty of Law, Bucharest University of Economic Studies, stancustefania24 @stud.ase.ro
[2] Student, Faculty of Law, Bucharest University of Economic Studies, miualexandru18 @stud.ase.ro
[3] M. Haentjens, & P. de Gioia Carabellese, (2015). European Banking and Financial Law (1st ed.). Routledge. https://doi.org/10.4324/9781315708515 , p. 4

legislative system regarding provider liability?" and "What are the current types of fraud?" This paper aims to address these questions. We intend to analyze the challenges presented here and propose new solutions by drawing on existing legislation at both the national and European levels. Our objective is to bring forth the latest developments in the economic-legal field to offer a comprehensive perspective; in this regard, we will also reference the recent opinion issued by the European Banking Authority (EBA), an independent EU authority dedicated to ensuring a consistent and efficient level of regulatory and prudential supervision in the EU's banking sector.

II. Main Body

1. Legal Framework of Payment Service Providers' Liability: Legislative Innovations and Practical Possibilities. Challenges and Future Prospects

The main purpose of the European Banking Authority (EBA) [4] s to create an efficient and transparent single market in the area of banking financial products. The EBA contributes to the establishment of a unified rulebook in the financial-banking field (Single Rulebook)[5] thus ensuring convergence of banking supervision practices.

We decide to begin our legal analysis of providers' liability by briefly presenting this European institution, as it plays a key role within financial-banking activities through its regulatory and supervisory role.

In its most recent opinion, the European Banking Authority addresses the issue of new types of fraud related to payment services and potential measures to prevent and combat these phenomena. EBA's competence to issue this opinion is founded on Articles 1(5) and 16a(1) of EU Regulation No. 1093/2010 [6] which pertain to EBA's objectives to enhance consumer protection and create a harmonized regulatory framework that ensures common procedures across the European Union.

Through its actions, the EBA emphasizes the need to update the current norms in the field of payment services to meet the current demands arising from the technological boom of recent years, the intensification of digital processes, and the emergence of more complex types of fraud.

Additionally, EBA's opinion[7] responds to the European Commission's proposals on June 28, 2023, regarding the revision of existing payment services

[4] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-banking-authority-eba_roviewed 02.11.2024

[5] https://www.eba.europa.eu/single-rulebook viewed 02.11.2024

[6] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32010R1093 viewed 02.11.2024

[7] https://www.eba.europa.eu/publications-and-media/press-releases/eba-has-identified-new-types-payment-fraud-and-proposes-measures-mitigate-underlying-risks-and viewed 02.11.2024

regulations within the Payment Services Directive (PSD2)[8] by developing a new regulation under the Payment Services Directive (PSD3) and a new Payment Services Regulation (PSR)[9].

The Commission views the 2023 package[10] as an improvement and evolution of the existing regulations. The proposals aim to promote consumer interests, enhance competition, and increase security in operations. The package is primarily aimed at standardizing the EU's single market in payment services.

The Commission's innovation with this legislative package involves splitting the provisions established by PSD2 into two parts, introducing separate regulations for Financial Data Access (FIDA)[11] aimed at transitioning from open banking to open finance.[12]

For the new legislative package, the Commission has proposed segmentation into:

- The PSR,[13] applicable within the Internal Market, which aims to standardize financial payment services (involving direct application of regulations in EU member states, given its legal nature).
- The PSD3 Directive, which represents an evolution in payment systems and brings necessary updates for the effective functioning of electronic currency services within the EU market. These updates include incorporating electronic money institutions within the framework of payment institutions, thus creating a unified structure under PSD3, whereby previous directives on payment services and electronic money-issuing institutions will benefit from a single, more practical regulation suited to the current context.

[8] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32015L2366 viewed 02.11.2024

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0366 viewed 03.11.2024

[10] https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en viewed 03.11.2024

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0360 viewed 04.11.2024

[12] Although there is a high degree of similarity between the two concepts, the differences between them are essential. In the case of open banking, the focus is on payment accounts and transaction information, so we can say that it is limited to the date. In contrast, the concept of open finance has a much more comprehensive character, including a much wider range of financial services and products. We can say that open finance offers a holistic view of the user's personal finances, giving him the opportunity to manage his finances through a single interface or through a service. The open finance method is much closer to reaching the interests of consumers by referring to their needs. https://truelayer.com/blog/product/what-is-open-finance-and-how-does-it-differ-from-open-banking/ viewed 04.11.2024

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0367 viewed 04.11.2024

This package aims to create a unified regulatory framework in member states, set enhanced standards for the efficient functioning of open banking services, and foster a more accessible environment for non-bank providers in the EU payment systems market (providers gain the right to a bank account to counteract the trend of risk-offloading[14]). Lastly, from our analytical perspective, the most significant goal is fraud prevention and control achieved through regulations that facilitate efficient information-sharing among PSPs, strengthen client authentication rules, broaden the legal framework for consumers' reimbursement rights in cases of fraud, and enforce verification protocols (covering IBAN codes and account names for payment beneficiaries).[15]

According to the objectives pursued by the legislative package, the measures to prevent and combat fraud are[16]:

- Imposing an obligation on PSPs to offer free verification services to confirm the identity match between the Unique Tax Identification Code (IBAN) and the name of the payment recipient in all transfer operations, regardless of their nature.
- Establishing a legal framework aligned with GDPR standards that enables PSPs to exchange information to prevent and combat digital fraud.
- Strengthening transaction monitoring frameworks.
- Implementing regular awareness campaigns and programs on fraud risks and trends for PSP employees and consumers (organized by PSPs).
- Granting consumers the right to reimbursement in strictly regulated cases.
- Streamlining user authentication rules for payment services.

Some experts describe the connection between the current payment services regulatory framework (PSD2) and data protection (GDPR) as lacking coordination, with legal gaps or even as a "Gordian legal knot."[17] However, this situation is

[14] Risk offloading is as defined in the Guidance on the characteristics of a risk-based approach to supervisory action in the fight against money laundering and terrorist financing, as well as the steps to be followed when performing risk-based supervision under of article 48 paragraph (10) of Directive (EU) 2015/849 (amending the Common Guideline ESAs/2016/72)- refusal to engage in business relations or a decision to terminate business relations with individual customers or categories of customers associated with a higher money laundering or terrorist financing risk or refusal to carry out transactions involving a risk money laundering or larger terrorist financing.

[15] G. Anton, Colocviile juridice ale BNR, Influența dreptului bancar european și comparat în România, Noile reglementări europene în materia serviciilor de plată: PSD3 și PSR, https://www.bnro.ro/Colocviile-juridice-ale-BNR-27593.aspx viewed 04.11.2024

[16] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543 viewed 04.11.2024

[17] F. Ferretti, Open Banking: Gordian Legal Knots in the Uncomfortable Cohabitation between the PSD2 and the GDPR. European Review of Private Law, 2022, 30(Issue 1), 73-102, ISSN 0928-9801. Available from: doi:10.54648/erpl2022004, viewed at 07.11.2024

addressed in the proposed framework, where the PSR resolves these data protection challenges to ensure the security of client data.

The PSR proposal not only supports Third-Party Payment Providers (TPPs) but also expands the existing requirement to offer users permission dashboards, allowing them to easily monitor and manage their data-sharing preferences. To streamline the process for clients, any changes to data-sharing settings will need to be managed by PSPs in collaboration with TPPs (Art. 43 of PSR)[18].

Despite the notable changes outlined, the European Commission has described the published Financial Data Access and Payments Package as an evolution rather than a revolution[19]. While it does aim to address key challenges within the current payment services regulatory framework, there remain certain unresolved issues under the forthcoming PSD3 and PSR frameworks.

First of all, as demonstrated by the delayed publication of the Regulatory Technical Standards (RTS) under PSD2, this delay resulted in a temporary reduction in security, as Payment Service Providers (PSPs) were only required to comply with strict security measures on strong customer authentication after the RTS was published (Art. 115 of PSD2)[20]. Therefore, timely publication of regulatory technical standards by the European Banking Authority (EBA) will be crucial for the new framework as well (e.g., Art. 30 of PSD3 or Art. 89 of PSR).

Second of all, the preparation required from all relevant stakeholders, particularly financial institutions, to implement the new regulatory framework will involve significant costs, especially due to necessary changes in IT systems and processes. Furthermore, the proposed regulations could impose an unnecessary administrative burden and additional reporting obligations on certain market participants, such as limited networks or foreign exchange services.

Thirdly, although the recital in PSD3 states that "buy now, pay later" (BNPL) services are not considered payment services, the legislative text does not include this exception explicitly. The author suggests that a more narrowly defined exception should be included in PSD3's legislative text, specifically for one-time BNPL services that do not provide users with payment accounts or payment cards.

Finally, PSR aims to significantly limit the risk of fraud by improving the current transaction monitoring by mandatory fraud data exchanges between PSPs

---

[18] J. Škrabka, Modernising payment services and enhancing open banking: a comparison of recent EU proposals of payment services directive 3 (PSD3) and payment services regulation (PSR) with current PSD2, in Horizons of Law in Business and Finance, 2023, Available from: https://www.ceeol.com/search/viewpdf?id=1294316 , viewed at 07.11.2024, p. 221

[19] V. Dombrovskis, Remarks by Executive Vice-President Dombrovskis and Commissioner McGuinness on financial data access and payments. European Commission (online) 2023, https://ec.europa.eu/commission/presscorner/detail/en/speech_23_3575 viewed 07.11.2024.

[20] P. T. J . Wolters and B. P. F. Jacobs. The security of access to accounts under the PSD2. Computer Law & Security Review. 2019, 35(1), 29-41. ISSN 0267-3649. Available from: doi:10.1016/j.clsr.2018.10.005. viewed 07.11.2024

(Art. 83 of PSR). Statistical data on frauds will have to be reported to national regulators, and PSPs will have to inform their users of new trends in fraud, fraud prevention and appropriate countermeasures (Art. 84 of PSR)[21].

In terms of the implementation schedule, it is estimated that the legislative package introducing PSD3 and PSR will take effect in 2025. As for the mandatory transposition of PSD3, member states will be required to adopt it within 18 months of publication in the Official Journal of the European Union (OJ). For ongoing operations, authorized institutions will need to comply with PSD3's requirements as stipulated.

In addition to European regulations, national legislation includes a comprehensive set of provisions in the field of payment services and payment service providers, set out in Law No. 209/2019, which regulates the obligations of payment service providers and users as outlined in the first article of this law[22].

2. Legal and Practical Perspectives on Fraud: Types of Payment Service Frauds

In the continuously evolving landscape of financial technologies (FinTech), payment service providers (PSPs) face growing challenges related to fraud. As digital payment systems become more common, the types of fraud encountered diversify, demanding a reassessment of liability frameworks.

The primary measures targeted by the PSR focus on "social engineering"[23] cases, where well-intentioned consumers are tricked into authorizing payments to fraudsters. PSR specifically addresses "spoofing" cases in which fraudsters abuse PSP information (e.g., name, email address, or phone numbers), posing as the provider to deceive consumers into taking actions that result in financial harm (for instance, misleading users into installing applications that allow fraudsters remote access to their devices, authorizing unauthorized transactions on behalf of the consumer). Initially, under PSD2, the main question was whether these transactions were considered authorized or unauthorized, as the directive limited reimbursements to unauthorized transactions only. Another obstacle was the directive's lack of tools

[21] J. Škrabka, Modernising payment services and enhancing open banking: a comparison of recent EU proposals of payment services directive 3 (PSD3) and payment services regulation (PSR) with current PSD2, in Horizons of Law in Business and Finance, 2023, Available from: https://www.ceeol.com/search/viewpdf?id=1294316, viewed at 07.11.2024, p. 222

[22] Law 209/2019, art. 1: "This law regulates the conditions of access to the activity of providing payment services, the prudential supervision of payment institutions and providers specialized in information services regarding accounts, the transparency regime for information conditions and requirements regarding payment services , as well as the corresponding rights and obligations of payment service users and payment service providers in the context of providing payment services on a professional basis."

[23] https://www.consilium.europa.eu/ro/policies/cybersecurity/cybersecurity-social-engineering/ viewed 04.11.2024

to counterbalance the effects of this new type of fraud; for example, strong customer authentication measures were insufficient to prevent such frauds.

Understanding payment system threats and adapting legal regulations to them is essential. For this, we need at least an overview of both traditional financial fraud types and the new types of digital fraud.

A. Traditional Types of Financial Fraud

In this study, we will provide an exhaustive view of traditional financial fraud types identified. Traditional financial fraud typically involves deceptive practices aimed at illegally obtaining money or assets. Common forms include:

1. Ponzi Schemes[24]: This type of fraud creates the illusion of high returns for investors, but in reality, profits come from funds invested by new investors rather than actual business earnings. Eventually, the scheme collapses as new investments slow down.

2. Embezzlement[25]: This occurs when someone in a trusted position, such as an employee or director, illegally uses, appropriates, or traffics money or assets under their management for personal gain. For accurate categorization, this form of crime falls under the special offense of embezzlement as stipulated in Article 272(1), letters b) and c) of Law 31/1990, which applies secondarily to the Criminal Code provisions for offenses by a company's founders, administrators, directors, supervisory board members, or legal representatives in cases covered by this specific law.

3. Insurance Fraud[26]: This involves falsifying or exaggerating claims to receive insurance payments, such as repeated accidents or inflated damages for higher payouts.

4. Bank Fraud[27]: This includes deceitful activities like check fraud, identity theft, or falsification of financial information to gain unauthorized access to funds or bank credit.

5. Securities Fraud:[28]: This occurs when individuals or companies manipulate or falsify stock or securities information to deceive investors, often through misleading financial statements, insider trading, or market manipulation.

[24] https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme viewed 05.11.2024

[25] https://sfc.ec.europa.eu/sites/default/files/RO-TRA-General%20Guidelines%20on%20National%20Anti-Fraud%20Strategies.pdf viewed 05.11.2024

[26] Insurance Europe, https://www.insuranceeurope.eu/priorities/23/fraud-prevention viewed 06.11.2024

[27] https://www.fraud.com/post/bank-fraud viewed 06.11.2024

[28] https://kkc.com/frequently-asked-questions/what-is-securities-fraud/ viewed 06.11.2024

6. Tax Evasion[29]: The deliberate act of avoiding taxes by underreporting income, inflating deductions, or hiding money in offshore accounts.

7. Mortgage Fraud[30]: This involves providing false information on a mortgage loan application to qualify for a loan or misrepresenting the value or condition of a property to deceive lenders or buyers.

8. Pyramid Schemes[31]: Similar to Ponzi schemes, these frauds rely on new recruits to generate profits for previous participants, often with promises of high financial rewards. The scheme ultimately collapses as recruitment slows.

9. Investment Scams[32]: These include deceptive high-yield investment offers (like "too good to be true" real estate deals or commodity investments) where promoters hide risks or misrepresent returns.

The common feature of these fraud types typically involves deception, misrepresentation, or concealing facts to gain illegitimate access to money or assets, often exploiting the good faith of the victims.

B. New Types of Digital Fraud

This subchapter begins with a concise definition of digital fraud: any form of deceptive or illegal activity using digital technologies (such as the internet, digital platforms, or electronic devices) to gain unauthorized access to personal, financial, or organizational assets.

Through our research for this paper, we identified multiple types of digital fraud:

1. Identity Theft[33]:

Occurs when fraudsters obtain personal information (e.g., identification documents, bank details, or credit card data) to impersonate someone and commit fraudulent activities in their name, typically through phishing or hacking.

2. Phishing[34]:

A type of digital fraud where attackers impersonate legitimate institutions (e.g., banks, online stores) to deceive individuals into sharing personal information, such as passwords or credit card numbers, through fraudulent emails, websites, or messages. Phishing has gained momentum in recent years, evidenced by numerous prevention announcements on the official website of the National Cybersecurity

[29] European Comission https://taxation-customs.ec.europa.eu/este-timpul-sa-recuperam-partea-lipsa_en viewed 06.11.2024

[30] https://www.investopedia.com/articles/mortgages-real-estate/10/how-mortgage-fraud-affects-markets.asp viewed 06.11.2024

[31] https://ag.ny.gov/pyramid-schemes viewed 06.11.2024

[32] https://www.tn.gov/attorneygeneral/working-for-tennessee/consumer/resources/materials/investment-scams.html viewed 06.11.2024

[33] https://netacea.com/blog/5-common-types-of-digital-fraud-and-how-to-stop-them/ viewed 06.11.2024

[34] Ibidem

Directorate (DNSC), such as the recent alert from September 6, 2024, regarding "spoofing/phishing/vishing attacks on Romanian users."[35]

3. Credit Card Fraud[36]:

Fraudsters obtain or steal credit card information (through hacking, phishing, or skimming) and use it to make unauthorized purchases or withdraw cash, which may also involve counterfeit card creation.

4. P2P Payment Fraud[37]:

Currently, around one billion people worldwide use platforms like PayPal, Venmo, Zelle, Apple Pay, and similar digital payment apps for peer-to-peer (P2P) transactions. These platforms have become prime targets for fraudsters, as companies often lack sufficient data and insights to recognize emerging fraud patterns specific to these apps.

Scams are prevalent; for example, fraudsters may sell products on online marketplaces, requiring payment via PayPal or Zelle, and then fail to deliver. Additionally, criminals can set up P2P accounts with stolen credit card information to buy goods or services. Since 2016, the incidence of fraud targeting P2P payment users has skyrocketed by an alarming 733%. Unfortunately, most P2P payment apps lack policies to protect users from fraud losses related to scams. Even more concerning, P2P fraud can open the door to account takeovers and other types of cybercrime.

5. Account Takeover[38]:

Here, fraudsters gain access to a person's or company's online account (e.g., banking or social media accounts) by obtaining credentials, often through phishing, brute-force attacks, or data breaches. Once they gain access, attackers can conduct unauthorized transactions or steal sensitive information.

6. Ransomware[39]:

This form of malware locks users out of their systems or encrypts files, demanding ransom (usually in cryptocurrency) in exchange for restoring access.

7. Business Email Compromise (BEC)[40]:

BEC is a cyber fraud tactic where attackers gain access to a business email account, impersonate directors or employees, and instruct employees to transfer funds or provide sensitive data, often causing significant financial losses.

8. Synthetic Identity Theft[41]:

In this type of fraud, perpetrators create a false identity by combining real information with fabricated data, using it to open various accounts or apply for credit.

---

[35] https://dnsc.ro/citeste/alerta-atacuri-de-tip-spoofing-phishing-vishing-asupra-utilizatorilor-din-romania viewed 07.11.2024

[36] https://netacea.com/blog/5-common-types-of-digital-fraud-and-how-to-stop-them/ viewed 07.11.2024

[37] https://www.datavisor.com/wiki/types-of-bank-frauds/ viewed 07.11.2024

[38] Ibidem

[39] Ibidem

[40] https://www.ibm.com/topics/business-email-compromise viewed 07.11.2024

[41] https://www.fraud.com/post/top-10-fraud-identity-theft-trends viewed 07.11.2024

9. Social Media Fraud[42]:

Fraudsters use social media platforms to deceive people through various techniques, such as fake lottery wins, charitable organizations, or investment opportunities.

10. Investment Fraud[43]:

This fraud occurs when perpetrators promote false investment opportunities, often through digital platforms or social media, to convince people to invest in non-existent or worthless assets like cryptocurrencies, stocks, or real estate.

11. Advertising Fraud[44]:

Fraudsters install malware on websites or apps to monitor user browsing activities, including schemes like click fraud, where fake clicks on digital ads generate revenue for cybercriminals.

12. Cryptocurrency Fraud[45]:

This includes scams and fraudulent schemes related to cryptocurrency transactions, such as Ponzi schemes, fake exchanges, and fraudulent Initial Coin Offerings (ICOs), as well as stealing cryptocurrency from wallets through hacking or phishing.

Given these different types of digital fraud, it's evident that digital fraud has evolved as a dynamic category of financial crime that leverages technological advancements. It ranges from simple scams to highly sophisticated schemes that often involve social engineering and advanced technical skills.

C. Impact of New Fraud Methods on Consumer Security and Trust

The emergence of new fraud methods has a substantial impact on consumer security and trust, affecting their perception of data and financial transaction security in today's digital landscape. Technological advancements exploited by fraudsters increase the complexity of attacks, making detection and prevention more challenging. Such methods include sophisticated phishing attacks, social engineering, advanced malware programs, and unauthorized access through highly complex hacking techniques.

Impact on Financial Transaction Security

These new fraud methods expose vulnerabilities in security systems, particularly in the digital environment where most financial transactions occur. For example, phishing attacks and malware targeting sensitive information, such as credit card details or bank passwords, pose significant financial risks to consumers. Additionally, attacks exploiting contactless technology, such as contactless

[42] https://www.scamwatch.gov.au/types-of-scams/social-media-scams viewed 08.11.2024
[43] https://www.secatty.com/legal-blog/what-is-investment-fraud/ viewed 08.11.2024
[44] https://www.cloudflare.com/learning/bots/what-is-ad-fraud/ viewed 08.11.2024
[45] Europol: Crypto investment scams – how do they work? https://www.europol.europa.eu/sites/default/files/documents/EP_Scenario%20Crypto%20Scams%20infographic_ENa.pdf viewed 08.11.2024

skimming, raise security concerns, putting consumers at risk even when their cards are not actively used.

Erosion of Consumer Trust in Financial Systems

The frequency of fraud incidents contributes to a decrease in consumer trust in financial and digital systems, with consumers becoming hesitant to use online services and electronic payments. Studies suggest that when consumers are aware of the risks associated with digital transactions, they become less willing to adopt financial innovations. This trend manifests in reduced usage of digital payment methods or even a reversion to cash transactions, to the detriment of electronic transactions.

3. Theoretical and Practical Aspects of Payment Service Providers' Liability and Adapting Liability to New Types of Fraud

Adapting liability for PSPs is essential for ensuring adequate investments in anti-fraud measures while maintaining consumer trust and regulatory compliance. This essay explores the current state of fraud in payment systems, the implications of liability frameworks, and the necessary adaptations to effectively address new types of fraud.

The growth of digital payment systems has been accompanied by a corresponding increase in fraudulent activities. Credit card fraud, as previously discussed, remains a significant concern characterized by unauthorized access to payment information for illicit purchases. Despite the implementation of advanced detection tools, the sophistication of fraudulent strategies continues to evolve, leading to considerable financial losses for both consumers and service providers. The challenge lies not only in detecting fraud but also in understanding the liability implications when fraud occurs. As perpetrators develop increasingly sophisticated techniques, existing liability frameworks may become inadequate, necessitating a comprehensive review and adaptation. This fact has also happened currently as we can see in the opinion of the EBA issued in the spring of this year.[46]

[46] "6. The EBA welcomes that the proposals incorporate many of the 200+ recommendations that the EBA had addressed to the EU Commission in its Opinion of June 20221. This was particular so for those recommendations that were aimed at further reducing payment fraud and enhancing the security of retail payments, which were themselves a result of the EBA's and NCAs' observations of how payment service providers (PSPs) had complied with the requirements set out in PSD2.

7. Since the publication of the EBA's Opinion of June 2022, the EBA has carried out further work to assess new fraud trends and types of payment fraud, leveraging on the new fraud data that became available to the EBA and the European Central Bank (ECB) at the end of 2023. This analysis was further informed by additional data collection conducted with NCAs in 2023 on particular data points that are not requested under the EBA Guidelines (GL) on fraud reporting under the PSD22, such as data on fraud for instant credit transfers and fraud related to the so-called mail orders or telephone orders (MOTOs). Moreover, the assessment of new fraud types draws on input provided by authorities

Liability frameworks play a crucial role in shaping PSP behavior regarding their investments in fraud prevention measures. Various authors highlight that, depending on liability regulations, PSPs invest differently, resulting in notable differences in their responses to fraud prevention.

For example, when liability rests with the integrated payment service provider (IPP), there is a greater tendency to invest in fraud prevention technologies, as the IPP knows that its position is vulnerable. Due to liability regulation, its financial exposure is directly linked to the effectiveness of its fraud detection systems. Conversely, if liability is shared or transferred to consumers, PSPs may feel less compelled to invest in meaningful anti-fraud measures, potentially increasing consumer vulnerability to fraud. In our view, this dynamic underscores the importance of establishing a liability framework that encourages proactive investments in fraud prevention.

The introduction of new payment services, such as Payment Initiation Services (PIS)[47] and Accounting Information Services (AIS),[48] under the second Payment Services Directive (PSD2) in the European Union, leads to a complication of the landscape of the presumed liability legal regime. Along with the benefits brought by these services by increasing consumer convenience and financial inclusion, new risks and opportunities for fraud also arise. The legal interpretation of liability in relation to these services is still evolving and regulations need to adapt to technological advances in payment systems. As new payment instruments emerge, the legal frameworks governing them must also evolve to meet the unique challenges they present, ensuring liability is properly assigned to minimize risks.

Furthermore, the digital transformation of financial services has led to the automation of numerous processes, including fraud detection. This should, in theory, increase the responsibility of all parties involved: both payment service providers, whose commitment is essential (especially in areas like fraud prevention systems), and consumers, who need better knowledge about new technologies and the risks they entail to recognize less complex forms of fraud.

Automated systems can analyze vast amounts of transactional data in real-time, identifying patterns indicative of fraudulent activity. However, reliance on automated systems raises questions about responsibility and liability when these systems fail to detect fraud. While automation can enhance efficiency, it requires a clear delineation of responsibility in cases where automated fraud detection systems

responsible for the supervision of PSPs as well as those responsible for the oversight of payment systems and instruments, including the ECB."

[47] It is a modern service through which bank transactions are initiated directly bank-to-bank through the consent of the consumer.

[48] Accounting services involve the systematic measurement, processing and communication of data provided in financial statements. These services have had an upward evolutionary path so that more recently attempts are being made to develop software systems based on AI technology to make accounting activities more efficient. The services I have referred to are part of a wider set of ways to push beyond the limits assumed by basic accounting to increase business performance.

do not perform as expected. This highlights the need for PSPs not only to invest in technology but also to establish clear protocols for accountability when systemic failures occur. Thus, a comprehensive regulatory framework is essential to address any potential obstacles in current practice.

As fraud continues to evolve, so must the strategies used by PSPs to combat it. We emphasize that the absence of a robust security culture within organizations (a comprehensive cybersecurity regulatory framework) can lead to significant financial losses from potential cyber fraud. To address this issue, PSPs need to cultivate a culture of security that prioritizes fraud prevention at all organizational levels. This involves not only investing in technology but also training employees to recognize and respond to fraudulent threats, setting clear measures for detecting and preventing cyberattacks, and combating them if they occur or cannot be avoided.

In practice, the PSP liability regime shows that consumers can dispute any contactless transaction under Article 74 of PSD2, though the process remains complicated. The situation has not improved following the European Court of Justice (ECJ) ruling in the Denizbank case, which has increased legal uncertainty, as explained below.

If a contactless card is used fraudulently, three potential articles of PSD2 could apply to determine the consumer's responsibility:

- **Article 74, Paragraph 1, First Sentence**: Generally, when a card is stolen and used, consumer liability is limited to €50 for transactions made before reporting the loss.
- **Article 74, Paragraph 2**: If a contactless card is used without Strong Customer Authentication (SCA), the consumer is not liable and will be fully reimbursed. This was the European Commission's position according to the Retail Payments Strategy. However, since the ECJ's Denizbank ruling, a different conclusion has been reached.
- **Article 63, Paragraph 1**: This applies to anonymous transactions, where consumer liability is limited to €30 for a single transaction and €150 for multiple transactions, according to PSD2.

The ECJ ruling concludes that contactless transactions are considered anonymous, meaning Article 63 applies.[49]

Following the Court's ruling on contactless cards, there are significant doubts about its interpretation.

In our view, the ECJ erred in its classification of the technology, concluding that contactless transactions fall under Article 63. Proximity communication (near-field communication) is a communication technique, not a payment instrument. Moreover, it is not explicitly mentioned in the Court's decision that consumers are no longer protected under Article 74, Paragraph 2, in the absence of SCA.

[49] C-287/19, Judgment of the Court (First Chamber) of 11 November 2020 DenizBank AG v Verein für Konsumenteninformation https://curia.europa.eu/juris/liste.jsf?num=C-287/19 viewed 8.11.2024

4. Fraud Prevention Measures and Liability of Providers

Determining PSP liability for new types of fraud may appear unfair given the uncontrollable nature of fraudulent activities. However, we believe that establishing PSP liability is justified by the position of power they hold over consumers and the resources they possess to remedy damages. Moreover, this responsibility ensures that PSPs remain committed to technological advancement for fraud prevention. Another argument supporting PSP liability in the face of new fraud types is their duty of care to consumers, as stipulated in current regulations.

Considering these arguments, we propose that PSPs' liability framework should also cover new forms of fraud to ensure effective functioning and development within the payment services domain.

5. Case Study

To provide a realistic dimension to our topic and gain a comprehensive view of the economic and social implications of fraud, as well as the necessity for a comprehensive legal framework that leaves no room for interpretation and provides adequate protection, we will use data provided by authorized entities focused on analyzing and raising consumer awareness about the socio-economic impact of this phenomenon.

First, data from the Global Anti-Scam Alliance (GASA), in collaboration with Feedzai, provides a report on global fraud trends in 2024[50], based on responses from people from diverse regions.

The GASA study revealed the economic and social impact of fraudulent tools on consumers. The study involved 58,329 respondents. The results show that over $1.03 trillion in assets were lost globally in the past year alone, a sum comparable to the GDP of certain countries. However, the report also offers hope, revealing growing fraud awareness and resilience among consumers.

Despite extensive global efforts to prevent and combat fraud through legislative updates and preventive measures (e.g., PSD3 and PSR for EU member states) and numerous awareness campaigns highlighting consumer risks, fraud continues to pose significant, unpredictable threats. According to the report, nearly half of global consumers encounter at least one attempted fraud weekly. In certain countries, this exposure is even more frequent, affecting consumers daily, with Brazil, Hong Kong, and South Korea experiencing the highest rates. Conversely, some countries, including Vietnam, Saudi Arabia, and China, report significant reductions in consumer fraud exposure, reflecting sustained prevention efforts.

On the positive side, the study found that 67% of global respondents feel confident in their ability to detect scams, demonstrating the positive impact of global awareness campaigns. This also suggests that people are adapting to new technologies. Countries with high confidence in fraud detection include China (84%)

[50] https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai viewed 8.11.2024

and Australia (72%), while Japan lags, indicating a need for additional educational efforts tailored to specific regions and even specific criteria.

Nonetheless, to understand fraud's full impact, we must consider the global financial toll. The results show that countries like the United States, Denmark, and Switzerland report the highest per-victim losses. U.S. citizens lose an average of $3,520 per affected consumer, while in Denmark, the average loss is $3,067 per victim, and in Switzerland, $2,980.

In relation to GDP, we highlight the losses suffered by Italy, the Netherlands, and France, with GASA data showing that these three countries estimate fraud losses at approximately 0.2% of GDP.

Looking at developing countries, the economic impact of fraud in Pakistan is much higher, with financial losses equivalent to 4.2% of the country's GDP. Kenya and South Africa are also heavily impacted, with fraud accounting for 3.6% and 3.4% of their GDP, respectively.

The study also reveals that around 70% of victims choose not to report fraud incidents. This underreporting is disadvantageous, as these reports could raise awareness of the phenomenon and drive development of new protective measures both legally, socially, and technically, such as advanced detection systems, smart software, and modern cybersecurity technologies.

Another factor influencing fraud rates is the development of artificial intelligence (AI). The GASA study highlights that a large portion of global consumers remain unfamiliar with the role and methods by which AI technology can be used in fraud schemes (with awareness levels varying by country). Countries where citizens lack a clear understanding of AI's role in fraud include Japan, Thailand, and Malaysia. The study found that 31% of respondents were uncertain if AI was involved in fraud or fraud attempts they had encountered. This statistic is concerning, reflecting the complexity of modern fraud.

Fraudsters exploit consumer ignorance by utilizing popular platforms and channels. The study indicates that phone calls and text messages remain the primary ways fraudsters initially contact victims, especially in countries like Hong Kong, the Philippines, and Thailand. The most common fraud types involve applications like WhatsApp, Instagram, and Gmail. Certain countries, including the Philippines, South Korea, and Brazil, have higher incidences of fraud via SMS.

The report also provides insights into the most frequent types of fraud by region. In Kenya and Nigeria, for example, shopping fraud is particularly prevalent. A unique factor for Nigeria is the prevalence of investment fraud, which remains widespread in that country. Meanwhile, countries like South Korea and Vietnam report the lowest levels of online shopping fraud. Other countries report high rates of identity theft, with rates reaching 25% in Australia and Mexico.

According to the study, only 4% of fraud victims successfully recover their losses. The highest recovery rates are in the U.S. and the U.K., although these rates remain relatively low in comparison to the total value of losses and the number of people affected.

We consider these data suggest an urgent need for international cooperation to mitigate the economic and social impact of fraudulent activities.

6. Interdisciplinary Nature of the Topic

This paper takes an interdisciplinary approach, linking areas of Civil Law, Financial Law, and European Banking Law.

Additionally, considering the broad scope of this study, its interdisciplinary nature also includes related legal fields such as Technology Law, given the continuous evolution of payment systems and the need for comprehensive regulations in this domain; Criminal Law and Business Criminal Law, especially since most fraud cases involve the offense of conducting fraudulent financial operations, classified as an offense against property in the Criminal Code, Chapter IV – "Frauds Committed through Computer Systems and Electronic Payment Means"; Commercial Law, due to the presence of both natural and professional economic actors, as defined by Article 287/2009 of the Civil Code; European Union Law, given the free movement of capital within the EU; and Consumer Protection Law, as consumers, the main subjects in this context, are among the most vulnerable in the financial-banking operations chain.

III. Conclusions

1. Brief Remarks on the Topics Addressed

In this paper, we have highlighted the impact of fraud on our constantly evolving society, along with key issues, given the novelty of this subject as presented by recent proposals from the EBA and the legislative package set for implementation next year regarding PSR, PSD3, and FIDA.

2. Practical Applicability of Proposed Solutions

We consider the practical solutions proposed in this project to be beneficial and applicable given the economic, human, technical, and practical resources available to payment service providers. Expanding the liability framework to allow consumers to recover their losses is justified due to their generally weaker position in terms of resources. Similarly, establishing PSP liability based on their duty of care is valid to achieve widespread practical utility through the faster and more efficient development of technologies to prevent and combat fraud.

3. Lex Ferenda Proposal

Rationale

In the context of rapid technological evolution and increasingly sophisticated fraud techniques, current regulations on payment service provider (PSP) liability are no longer fully aligned with today's challenges. New fraud methods, including advanced phishing, social engineering attacks, and contactless skimming, expose consumers and financial institutions to significant risks. Therefore, it is necessary to adapt the legal framework to balance user protection in payment services with PSP liability, to increase trust in the financial system and encourage the use of digital services.

The legislative proposal has the following objectives:

1. **Increasing Consumer Protection**: Establishing clear and efficient mechanisms to protect consumers against new types of fraud.
2. **Clarifying PSP Liability in Different Fraud Scenarios**: Adapting the PSP liability regime to respond to cases where fraudsters use sophisticated techniques that make detection and prevention challenging.
3. **Encouraging Collaboration between PSPs and Authorities**: Creating a closer collaboration framework between payment service providers and relevant authorities for information sharing and fraud prevention.
4. **Improving Consumer Education on Digital Fraud Risks**: Promoting awareness campaigns by PSPs to help consumers identify and prevent fraud attempts.

Proposed Regulation

Article 1: Definition of New Types of Fraud

The regulation will include a detailed definition of new types of digital fraud, such as phishing, social engineering, skimming, and other attacks that can compromise transaction security without the user's direct involvement.

Article 2: PSP Liability for Fraudulent Transactions

1. Payment service providers are liable for fraudulent electronic transactions where cyber attackers use advanced techniques that consumers cannot easily detect.
2. For contactless transactions and other technologies that do not require Strong Customer Authentication (SCA), PSPs will be responsible for consumer losses if the attack was carried out using advanced fraud techniques.
3. If the fraudulent transaction results from a phishing attack, PSPs are responsible for fully reimbursing the lost amount, provided the user has not acted with gross negligence.

Article 3: Establishment of a Compensation Fund for Fraud Victims

A digital fraud compensation fund is established, to which PSPs will contribute proportionally to the volume of transactions they handle. This fund, managed by a financial regulatory authority, will compensate affected consumers in cases where PSP liability is unclear under existing regulations.

Article 4: Reporting and Cooperation Obligation

1. PSPs must promptly report any fraud incidents involving new fraud techniques to supervisory authorities.
2. PSPs will collaborate with law enforcement and regulatory authorities to share information and improve fraud detection and prevention mechanisms.

Article 5: Education and Awareness Campaigns for Users

PSPs will conduct periodic user education campaigns on new types of fraud and preventive measures they can adopt. Campaigns will include accessible digital

and physical materials to raise user awareness of risks associated with digital transactions.

Article 6: Educating New Generations

PSPs, in collaboration with state authorities, will carry out activities to educate future generations on the risks of fraud, providing an overview of payment services and how they function.

This legislative proposal aims to adapt the liability framework for payment service providers to the realities of new digital fraud methods, thereby enhancing consumer protection and restoring trust in electronic payment systems. Implementing these measures is expected to positively impact the security of digital transactions and encourage responsible innovation in the financial sector through increased collaboration and PSP accountability.

Bibliography

Books and Articles

1. Anton G. "Colocviile juridice ale BNR: The Influence of European and Comparative Banking Law in Romania: The New European Regulations in Payment Services: PSD3 and PSR." Available at: BNR Legal Colloquium
2. Dombrovskis V. "Remarks by Executive Vice-President Dombrovskis and Commissioner McGuinness on Financial Data Access and Payments." *European Commission*, 2023. Available at: European Commission
3. Ferretti F. "Open Banking: Gordian Legal Knots in the Uncomfortable Cohabitation between the PSD2 and the GDPR." *European Review of Private Law*, 2022, 30(1), 73-102. ISSN 0928-9801. Available from: doi:10.54648/erpl2022004, viewed 07.11.2024.
4. Haentjens M., & de Gioia Carabellese P. (2015). *European Banking and Financial Law* (1st ed.). Routledge. https://doi.org/10.4324/9781315708515
5. Škrabka J. "Modernising Payment Services and Enhancing Open Banking: A Comparison of Recent EU Proposals of Payment Services Directive 3 (PSD3) and Payment Services Regulation (PSR) with Current PSD2." In *Horizons of Law in Business and Finance*, 2023. Available at: CEEOL, viewed 07.11.2024, pp. 221-222.
6. Wolters P. T. J., & Jacobs B. P. F. "The Security of Access to Accounts under the PSD2." *Computer Law & Security Review*, 2019, 35(1), 29–41. ISSN 0267-3649. Available from: https://doi.org/10.1016/j.clsr.2018.10.005

Websites

1. European Union. "European Banking Authority (EBA)." Available at: European Union
2. European Banking Authority. "Single Rulebook." Available at: EBA Single Rulebook
3. EUR-Lex. "Regulation (EU) No 1093/2010." Available at: EUR-Lex

4. European Banking Authority. "EBA Has Identified New Types of Payment Fraud and Proposes Measures to Mitigate Underlying Risks." Available at: EBA Press Release
5. EUR-Lex. "Directive (EU) 2015/2366 (PSD2)." Available at: EUR-Lex
6. EUR-Lex. "Proposal for PSD3 and PSR." Available at: EUR-Lex
7. European Commission. "Financial Data Access and Payments Package." Available at: EC Finance
8. EUR-Lex. "Commission Proposal for FIDA." Available at: EUR-Lex
9. TrueLayer. "What Is Open Finance and How Does It Differ from Open Banking?" Available at: TrueLayer
10. EUR-Lex. "Commission Proposal for PSD3 (2023)." Available at: EUR-Lex
11. European Commission. "Cybersecurity Social Engineering Policies." Available at: Consilium
12. U.S. Securities and Exchange Commission. "Ponzi Scheme." Available at: Investor.gov
13. European Commission. "Anti-Fraud Strategies Guide." Available at: European Anti-Fraud Office
14. Insurance Europe. "Fraud Prevention." Available at: Insurance Europe
15. Fraud.com. "Bank Fraud Overview." Available at: Fraud.com
16. KKC. "What is Securities Fraud?" Available at: KKC
17. European Commission. "Recover Missing Parts Initiative." Available at: Taxation and Customs
18. Investopedia. "How Mortgage Fraud Affects Markets." Available at: Investopedia
19. New York State Attorney General. "Pyramid Schemes." Available at: NY AG
20. Tennessee Attorney General. "Investment Scams." Available at: TN Attorney General
21. Netacea. "5 Common Types of Digital Fraud and How to Stop Them." Available at: Netacea
22. DNSC. "Spoofing/Phishing/Vishing Attacks Alert in Romania." Available at: DNSC
23. DataVisor. "Types of Bank Fraud." Available at: DataVisor
24. IBM. "Business Email Compromise." Available at: IBM
25. Fraud.com. "Top 10 Fraud and Identity Theft Trends." Available at: Fraud.com
26. ScamWatch. "Social Media Scams." Available at: ScamWatch
27. SEC Attorneys. "What is Investment Fraud?" Available at: SEC Attorneys
28. Cloudflare. "What is Ad Fraud?" Available at: [Cloudflare] (https://www.cloudflare.com/learning/bots/what-is-ad-fraud