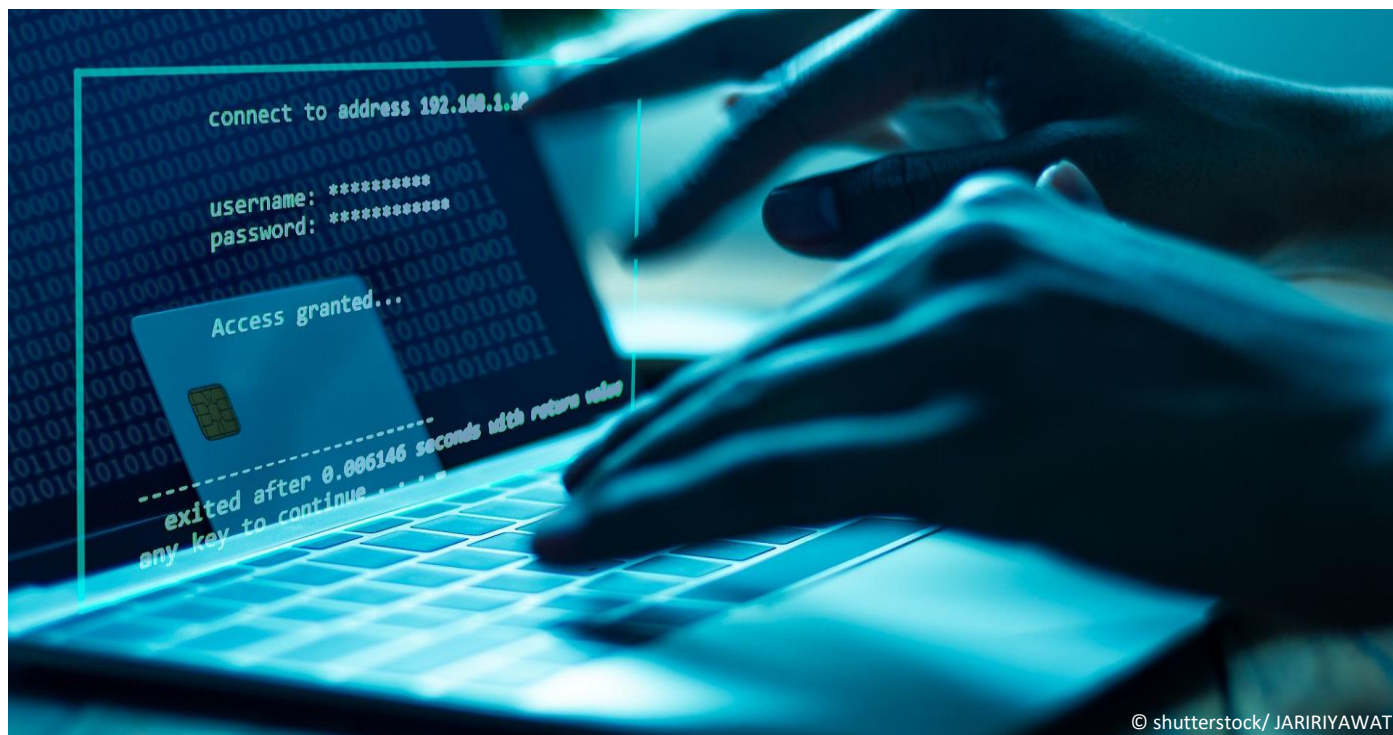


Guarding the Gates

EU Strategy for Safer Payment Market and Fraud Prevention

Anastasia Kotovskaia



© shutterstock/ JARIRIYAWAT

In an era of instant payments and cross-border transactions, the fight against payment fraud remains a pressing challenge for the EU. As fraud techniques evolve and cybersecurity risks continue to undermine payment systems, the limitations of existing regulatory frameworks become increasingly evident. This cepInput examines the primary challenges of financial fraud in the EU and outlines policy priorities to address them.

- ▶ Fragmented approaches to fraud liability and unclear regulatory provisions threaten market order, consumer trust and overall stability of the EU payment market. The vulnerabilities of instant payment systems further exacerbate these risks.
- ▶ To effectively combat financial fraud, the EU should establish a robust regulatory framework that balances market efficiency with adequate protections for consumers. A comprehensive approach to tackling fraud should include three levels of action: I) Collaboration and harmonised standards; II) Technological advancements; and III) Consumer and institutional education.
- ▶ Key policy recommendations include adoption of a harmonised, tiered approach to the liability, strengthening cross-border collaboration, aligning cybersecurity and anti-fraud measures, enhancing transaction monitoring for payment service providers, the integration of advanced technology and artificial intelligence for real-time fraud detection and empowering the AMLA to improve coordination across jurisdictions.
- ▶ By implementing these recommendations, the EU can foster a secure, unified payment environment that bolsters consumer trust and supports the objectives of the EU Capital Markets Union.

Table of Contents

1	Introduction	3
2	Current challenges in combating payment fraud	3
	2.1 Evolution of payment fraud techniques and tactics	4
	2.2 Cybersecurity risks in payments and their impact on fraud	6
	2.3 Lack of unified approach to the fraud loss liability.....	7
3	Implications of payment fraud on the EU payments market	8
	3.1 Cross-border financial fraud and fraud risks in instant payments.....	8
	3.2 Impact of combating payment fraud on the EU Single Market and Capital Markets Union ...	11
4	Policy recommendations	12
5	Conclusions	16

List of Figures

Fig. 1:	Timeline for EU financial institutions for receiving and sending instant payments in the EU. ...	10
Fig. 2:	Annual fraud losses in instant payments in the EU	10
Fig. 3:	Three levels of action to combat payment fraud in the EU.....	16

1 Introduction

The accelerated digitalization of the financial sector gave a rise of innovation in payment solutions, fostering more seamless and efficient transactions across the European Union (EU). While advanced digital technologies offer new opportunities for both payment services providers (PSPs) and their customers, they are increasingly exploited by criminals for financial fraud. The interconnected nature of financial systems, coupled with a reliance on third-party service providers, creates systemic vulnerabilities in the payments sector. Such financial fraud conducted through a cybersecurity breach is especially dangerous, as localised cyber incidents have the potential to spread rapidly across countries, thereby posing risks to financial stability within the EU. The increasing prevalence of cyber threats and recent geopolitical tensions have further highlighted the necessity for a robust regulatory framework to ensure the security and resilience of the financial sector.¹

Despite the financial industry's proactive efforts in advanced security systems and the enhancement of information-sharing networks in the last years, a unified regulatory approach at the EU level is essential to effectively address these growing threats. This cepInput outlines the key challenges in combating payment fraud and provides policy recommendations to foster a more secure and resilient payments market across the EU.

2 Current challenges in combating payment fraud

Payment fraud presents a considerable challenge to financial market participants and regulators. The emergence of new payment technologies, such as instant payments, has introduced additional risks for exploitation by fraudsters. The involvement of multiple parties in digital payment systems creates potential points of vulnerability for fraudsters if adequate security measures are not consistently implemented across the payment chain.² Moreover, disparate approaches to fraud prevention and liability across the EU create an uneven regulatory playing field and incentivise regulatory arbitrage by market participants. Hence, this inconsistency undermines the legal certainty and predictability that are essential for a well-functioning market.

The financial losses resulting from payment fraud within the European Economic Area (EEA) exceed an alarming €4 billion annually,³ indicating the substantial financial and operational impact of security breaches on both individual financial institutions and the broader EU financial market. While fraud rates for credit transfers, direct debits and cash withdrawals remain relatively low and stable, fraud rates for card payments and e-money transactions are on the rise.⁴ This underscores the need for the financial sector to adapt its approach to combating and mitigating digital payment fraud. The ongoing

¹ Kotovskaia, A. (2025). Financial Technology in Global Context: Risks and Opportunities. In: Katsikas, D., Del Tedesco Lins, M.A., Ribeiro Hoffmann, A. (eds). Finance, Growth and Democracy: Connections and Challenges in Europe and Latin America in the Era of Permacrisis. United Nations University Series on Regionalism, vol 33. Springer, Cham. https://doi.org/10.1007/978-3-031-68475-3_16.

² Kantar Public (2022). Study on new digital payments methods.

³ EBA and ECB (2024). Report on Payment Fraud, p. 5.

⁴ EBA and ECB (2024). Report on Payment Fraud, p. 10-11.

advancement of technology, the emergence of more sophisticated fraud techniques, the growing cybersecurity threat and the lack of harmonised regulatory frameworks are the factors that make payment fraud more challenging to prevent.

2.1 Evolution of payment fraud techniques and tactics

The constantly evolving complexity and variety of payment fraud techniques present a significant challenge for financial institutions in detecting and preventing fraud. Traditional payment fraud generally involves unauthorised transactions, where fraudsters gained access to victims' bank credentials or credit card details through methods such as skimming⁵ or phishing⁶. However, modern payment fraud has become far more intricate. The payments market within the EU now faces a surge of sophisticated threats, notably from social engineering⁷ and advanced persistent threats (APT).

Social engineering attacks have far-reaching consequences. In the payments sector, these attacks cause fraudulent transactions, disrupt operations, compromise data, and erode customer confidence. In recent years, authorised push payment (APP) fraud, largely driven by social engineering, has become the most challenging type of payment fraud to combat. Losses due to APP fraud across Europe reach approximately €2.4 billion, increasing by 20 to 25 percent annually.⁸ In APP fraud, fraudsters employ social engineering tactics to manipulate victims into authorizing fraudulent payments. This often involves impersonating a trusted entity or a family member in urgent need of funds. Emerging technologies like deepfakes further enhance these schemes by enabling fraudsters to create highly convincing video or audio impersonations, which are used to prompt unauthorised payments or gain access to sensitive financial data.

Unlike social engineering, which exploits human behavior, APTs involve prolonged intrusions that sometimes lasting years⁹ and are aimed at deeply infiltrating systems for espionage or theft. The APT strategies exploit sophisticated cyber tactics to compromise security in ways that traditional systems often struggle to detect.¹⁰ These attacks seek to exploit the inner workings of an organisation's deci-

⁵ Skimming is a technique of theft of sensitive financial information, mainly credit or debit card details, by using a hidden device called a skimmer to capture card data. A skimmer is typically installed on ATMs, gas station pumps, or point-of-sale (POS) terminals.

⁶ Phishing is a type of fraud where cybercriminals attempt to obtain victims' financial data (such as password, credit card number, etc.) with fake emails or websites by pretending to be a trustworthy entity.

⁷ The term "social engineering" is used to describe the manipulation of human behaviour for the purpose of gaining unauthorised access to sensitive information, assets or systems.

⁸ Numbers are estimated by the Edgar, Dunn & Company (2024). <https://thepayers.com/expert-opinion/the-app-fraud-problem-and-its-impact-on-the-payments-industry--1269224#:~:text=How-ever%2C%20EDC%20believes%20that%20APP,%25%20to%2025%25%20since%202022>.

⁹ Kumar R. et al. (2022). APT attacks on industrial control systems: a tale of three incidents. *Int J Crit Infrastruct Prot.* 2022;37:100521.

¹⁰ Hussain S., Bin Ahmad M., Uddin Ghouri S. (2021). Advance persistent threat—a systematic review of literature and meta-analysis of threat vectors. *Adv Intell Syst Comput.* 2021;1158:161–78.

sion-making and financial processes. For payment institutions, consequences extend beyond mere financial loss¹¹ and reputational harm, since such fraudulent activities pose a risk also to their operational continuity and regulatory compliance.¹²

The increasing sophistication of fraud tactics gives rise to a regulatory debate about the sufficiency of current legislation and practical challenges in the implementation of the existing EU legal framework to the newest types of payment fraud like APP fraud.¹³ The current regulatory framework for combating payment fraud proves unable to adequately keep pace with the rapid advancements of emerging fraud techniques financial sector. Even the most recent review of the EU Payment Services Directive (PSD3¹⁴) has been deemed insufficient for addressing the increasing risks associated with sophisticated fraud tactics.

In general, the recent adoption of PSD3 and the Payment Services Regulation (PSR¹⁵) can be, nevertheless, evaluated as a right step towards strengthening the EU approach to mitigate fraud risks within the EU financial sector.^{16,17} It is welcomed that one of the central measures of the recent reform relates to the provisions regarding Confirmation of Payee (CoP) services,¹⁸ which has been already introduced in the Instant Payments Regulation¹⁹ (see cep [PolicyBrief](#)). CoP requires banks to verify that the recipient's name matches the associated account number before authorizing a transaction, adding an essential layer of security to prevent APP fraud and accidental payments. By standardizing CoP services across member states, PSD3 aims to reduce cases of misdirected funds and boost consumer confidence in digital payments. The clarifications of some liability issues for PSPs provided in the PSR and expanding the responsibilities of electronic communications service providers (ECSPs) and online platforms in fraud prevention, may indeed incentivise market participants to improve their fraud policies and to promote more cooperation between institutions.

Despite these advancements, PSD3 and PSR leave several critical challenges unaddressed, particularly regarding the liability provisions issues in case of sophisticated social engineering fraud and other

¹¹ Johnson A.L. (2016). Cybersecurity for Financial Institutions: the Integral Role of Information Sharing in Cyber-Attack Mitigation, vol. 20, North Carolina Banking Inst (2016), pp. 277-310.

¹² Pawlak, P. (2017). Cyber security woes: WannaCry? EUISS.

¹³ Werner S. (2024). Social Engineering im Zahlungsverkehr: mehr Kontrollpflichten zulasten der Zahlungsdienstleister. RdZ 2024, 145.

¹⁴ Proposal for a directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, COM/2023/366 final.

¹⁵ Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010, COM/2023/367 final.

¹⁶ Conreder C., Hausemann F. (2024). Der Kommissionsentwurf zur 3. Zahlungsdienste-RL und Zahlungsdienste-VO. BKR 2023, 729.

¹⁷ Zahrte K. (2023). Das Financial Data Access and Payments Package. Teil I: PSD 3 und PSR. Zeitschrift für Wirtschaftsrecht, 44 (2023), 49, S. 2555 – 2563.

¹⁸ Articles 50 and 57 PSR.

¹⁹ Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro.

emerging fraud techniques (see [Section 2.3](#)). While PSD3's enhanced monitoring and CoP requirements may mitigate some risks, without adaptive fraud prevention approach to identification of complex fraudulent tactics, the payments market remains vulnerable to fraud.

2.2 Cybersecurity risks in payments and their impact on fraud

Since the COVID-19 pandemic catalysed digital payments, the cyber risks that are associated with digital payments are continuously growing. Financial institutions face intense competitive pressure, leading them to introduce innovative solutions to meet customer demands. However, the adoption of cutting-edge but less-proven technologies increases cyber risks in the financial sector. Moreover, PSPs often use third-party software which can create security bottleneck. While recent legislative efforts such as the Cyber Resilience Act²⁰ (see [cepPolicyBrief](#)) and the DORA Regulation²¹ (see [cepPolicyBrief](#)) and NIS 2 Directive²² (see [cepAdhoc](#)), have strengthened cybersecurity foundations across the financial sector, APP fraud and deepfake-related scams reveal limitations in the current framework. Indeed, criminals still exploit system weaknesses to access sensitive information and use it for financial fraud and data theft. Since more and more software systems and data are stored in the cloud, it results in an increase in cloud-based attacks. As a response, financial institutions must ensure that their technical infrastructures are securely configured to withstand fraudulent activities. From fraud to sophisticated data breaches, cyber risks are threatening not only the security of payment methods but also the trust of customers in modern payment solutions.²³ However, trust in the integrity of payment systems is essential for fostering a well-functioning digital economy.

Against this background, payment security and cybersecurity are inherently interconnected. Both aim to protect sensitive information, prevent unauthorised transactions, and ensure a seamless and secure user experience. Cybersecurity strategies are essential to the infrastructure of payment systems, as they guard against fraud. Cyber-attacks on payment systems can lead to leakage of highly sensitive information, such as credit card numbers, bank account details, and personal data.

Many third-party applications, such as payment platforms, facilitate financial services. These apps often require customers to provide consent for accessing their bank accounts or other financial data through Application Programming Interfaces (APIs). In practice, however, market participants are facing difficulties in distinguishing the unauthorised access from the authorised access where the customer gave consent via third-party applications.²⁴ Since different third-party applications use different security standards or consent verification protocols, this inconsistency makes it harder for financial institutions to verify whether access requests genuinely stem from authorised sources. At the same

²⁰ Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019C1020, COM/2022/454 final.

²¹ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, PE/41/2022/INIT, OJ L 333, 27.12.2022, p. 1–79.

²² Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ L 333 27.12.2022, p. 80.

²³ OECD (2020), Personal data use in financial services and the role of financial education: a consumer-centric analysis.

²⁴ Impact Assessment Report for a Proposal for PSD3, Annex 11.

time, cybersecurity practices can help to protect this information from unauthorised access. For example, using advanced encryption protocols in payment systems ensures that data remains secure throughout the transaction process. Also advanced authentication mechanisms play an essential role for both cybersecurity and payment security. PSPs and third parties implement procedures as multi-factor authentication (MFA) and strong customer authentication (SCA) that require users to verify their identity through multiple factors enhance security measures. Preventing unauthorised access to accounts and ensuring that only verified users can initiate transactions increases an overall security level, limiting risks for both cybersecurity breaches and payment fraud. Cybersecurity tools are furthermore helpful in identifying patterns of fraud or unauthorised access. In payment security, these tools analyse transaction data in real time, flagging irregularities or suspicious behaviour. For instance, sudden changes in purchasing patterns may indicate fraud attempts. By leveraging these cybersecurity tools, payment systems can better identify and mitigate fraud before it affects users.

Payment security and cybersecurity are, therefore, two sides of the same coin in the digital economy. Effective payment security relies on strong cybersecurity foundations to protect users, transactions, and sensitive data from a growing array of digital threats. In turn, a resilient payment infrastructure supported by strong cybersecurity is vital for sustaining customer confidence in payment solutions and promoting a stable and fair market environment. In this interdependent relationship, a harmonised and comprehensive approach to cybersecurity is not just a technical necessity but a cornerstone for the sustainable growth of the digital economy in the EU.

2.3 Lack of unified approach to the fraud loss liability

To date, EU countries have adopted varying approaches for fraud loss liability. For instance, in the Netherlands, approximately 89% of the losses from the most types of financial fraud are reimbursed to affected consumers through a voluntary leniency program established by four major Dutch banks.²⁵ This program allows banks to cover fraud losses beyond standard liability thresholds, helping to alleviate the financial burden on consumers and demonstrating high standard of duty of care. This approach contrasts with practices in other EU countries, where customer liability caps for different types of fraud are more rigidly applied or refunds for fraud involving social engineering are mostly refused. It highlights the differences in how fraud liability is handled across the EU.

The primary reason for these discrepancies is the lack of a unified definition of "gross negligence" under PSD2²⁶. Under PSD2, PSPs are liable for unauthorised payment transactions unless the victim has acted with "gross negligence". While the liability provisions under PSD3 and the PSR represent an improvement, the absence of a standardised definition of "gross negligence" creates difficulties in the application of these legal provisions in the area of liability, resulting in inconsistent handling of fraud cases, particularly in APP fraud disputes. Member states interpret "gross negligence" differently, with national courts given broad discretion to determine criteria for assessment. This inconsistency has led

²⁵ European Commission (2023). Impact Assessment Report of 28.6.2023 SWD(2023) 231 final.

²⁶ Directive (EU) 2015/2366 on payment services in the internal market. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366>.

to consumer uncertainty, uneven application of liability provisions and increased litigation across jurisdictions.

The evolving nature of fraud techniques adds further ambiguity to liability standards, especially in cases involving APP fraud. The current PSD framework lacks clear rules specific to APP fraud, frequently leaving consumers to bear the financial consequences. Victims are unlikely to succeed in court²⁷ unless they can demonstrate that the PSP failed in its duty of care, such as by not flagging a suspicious transaction. Europe-wide, the liability borne by payment service users (PSUs) is much higher than compared to PSPs. The European Banking Authority (EBA) reported that, in 2022, PSUs incurred 79% of fraud losses in credit transfers, amounting to approximately €1.2 billion.²⁸ This disproportionate burden can be partially explained by the growing prevalence of APP fraud and the absence of a clear distinction in PSD between authorised and unauthorised transactions. A standardised definition of “gross negligence” could help PSPs to design fraud prevention measures more consistently across the EU. This harmonised approach should also reflect the complexities of social engineering fraud, enabling fairer fraud case assessments and ensuring a balanced approach to consumer protection and PSP liability across the EU which could help build a fairer, more resilient financial system.

Moreover, PSD3 does not fully address liability for so-called “mule” accounts, which facilitate money laundering and fraud by quickly moving stolen funds across borders. While PSD3 encourages PSPs to share information to track fraud patterns, it lacks a specific liability framework for cases involving mule accounts between payer and payee banks. Addressing this issue would require greater coordination among member states and clearer guidelines to prevent fraudsters from exploiting regulatory gaps.

The lack of an EU-wide approach to fraud liability in the payments market poses a risk for the European payment market. Clear and consistent rules are necessary to ensure a level playing field across the EU member states. Without harmonised regulations across member states, disparities in fraud liability frameworks can lead to an uneven competitive landscape, disadvantages for consumers in less-protective jurisdictions, and undermine trust in digital payments. A unified approach on fraud liability would ensure that liability is allocated transparently and equitably, supporting the broader goals of a stable and competitive European payments market.

3 Implications of payment fraud on the EU payments market

3.1 Cross-border financial fraud and fraud risks in instant payments

In recent years, rising trends in cross-border financial fraud and fraud in instant payments within the EEA pose complex challenges for both regulatory bodies and financial institutions. Fraud rates for cross-border transactions, particularly for credit transfers and card payments, are nearly nine times higher than for domestic transactions.²⁹ One of the main reasons for that is insufficient cross-border cooperation among PSPs and regulatory bodies across jurisdictions, which hinders effectively detecting

²⁷ Kai Zahrte (2024). Aktuelle Entwicklungen im Zahlungsdiensterecht (2022–2023). BKR 2024, 135.

²⁸ EBA and ECB. 2024 report on payment fraud.

²⁹ EBA (2024). Opinion on new types of payment fraud and possible mitigants.

and preventing fraud. In general, the lack of standardization in cross-border payments leads to significantly varying rules for their execution in different countries.^{30,31} A non-transparent and intricately landscape makes them a target for financial fraud. Apart from that, divergent application of SCA requirements, especially in cross-border transactions with non-EEA countries, lowers the overall security level. These inconsistencies create exploitable gaps for fraudsters to bypass security protocols. Inconsistent enforcement of SCA across member states may also make certain jurisdictions more attractive targets for fraud. Fraud rates vary considerably across member states, with some countries experiencing fraud rates up to 10 times the EEA average.³² These disparities can be attributed to several factors, including the differing implementation of security requirements by PSPs and variations in regulatory oversight. Low level of financial and digital literacy among citizens also plays a role (see [cepInput](#)), as users in certain regions may be more susceptible to social engineering fraud tactics. The disparities across the EU underscore the need for a harmonised regulatory approach that strengthens cross-border fraud detection and prevention mechanisms.

Instant payments, or real-time credit transfers, are increasingly becoming popular due to their efficiency and convenience. However, they have also presented new vulnerabilities due to the rapid nature of transactions. In 2022, fraud rates in instant payments were observed to be approximately 10 times higher than in traditional credit transfers.³³ Now, after the recent adoption of the Instant Payments Regulation requiring PSPs, electronic money institutions (EMI) and payment institutions (PI) to send and receive instant payments, it is expected that instant payments will become a new normal in the EU and therefore replace the standard SEPA payments that take one business day.

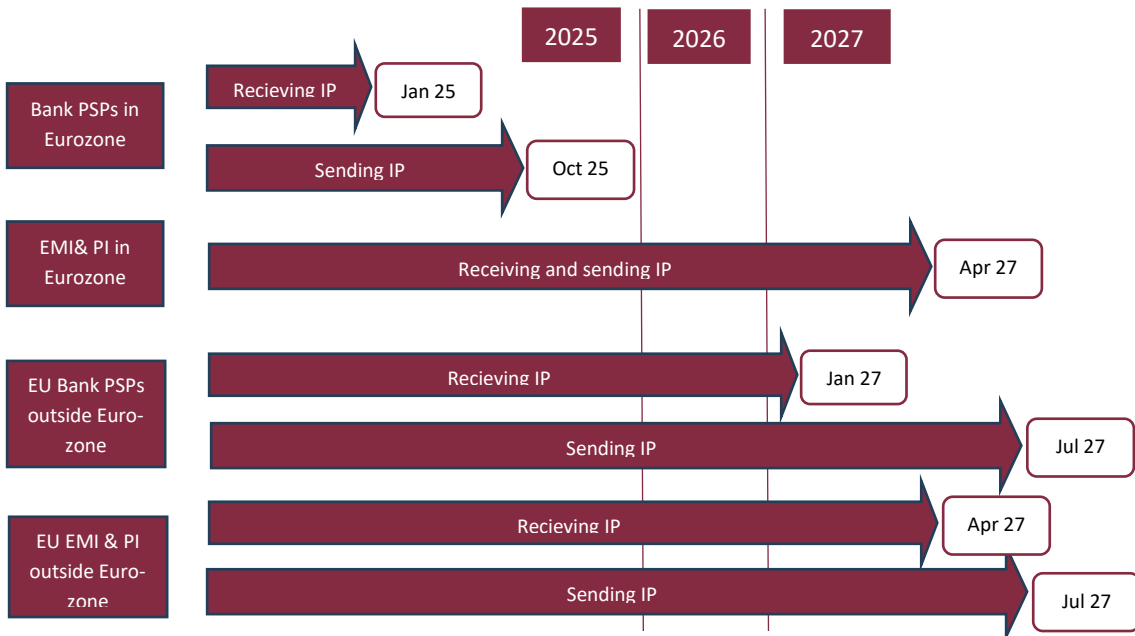
³⁰ Financial Stability Board (2020). Enhancing cross-border payments. Stage 1 report to the G20: Technical background report.

³¹ CPMI (2020). Enhancing cross-border payments: building blocks of a global roadmap. Stage 2 report to the G20 – technical background report. Bank of International Settlements, Basel.

³² EBA and ECB. 2024 report on payment fraud.

³³ EBA and ECB. 2024 report on payment fraud.

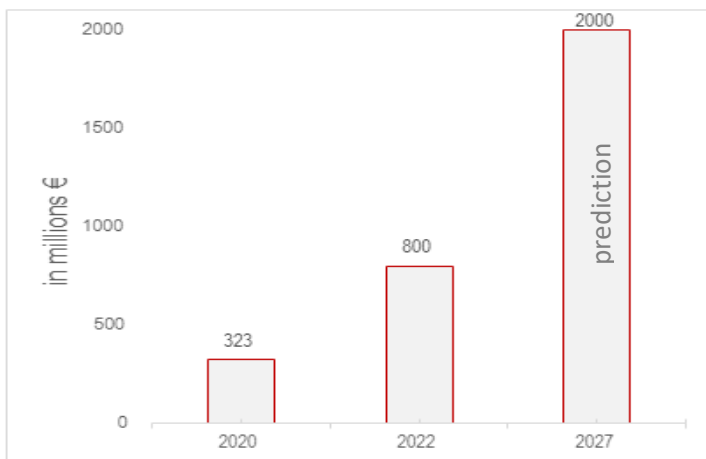
Fig. 1: Timeline for EU financial institutions for receiving and sending instant payments in the EU.



Source: EU Instant Payments Regulation.

The first phase of the transitional period requiring all banking services provides in the Eurozone at least receiving instant transfers already expired on 9 January 2025 Regulation. That means that instant transfers are becoming a default option for SEPA transfers for most of the users. Furthermore, the European Central Bank (ECB) plans in the next step to introduce the possibility of cross-currency transactions in real time.³⁴ Simultaneously, it significantly increases the risks of financial fraud. Whereas the fraud-related financial loss in instant payments in the EU was estimated at €800 million in 2022, it is expected to rise to €2 billion by 2027.^{35,36}

Fig. 2: Annual fraud losses in instant payments in the EU



Sources: ECB (2020), EBA Clearing (2024).

³⁴ ECB (2020). MIP news. <https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews201006.en.html>.

³⁵ EBA (2024). Opinion on new types of payment fraud and possible mitigants.

³⁶ EBA Clearing 2024.

Instant payment fraud can be particularly problematic for several reasons. Fraudulent instant payments are in most cases irrevocable because they are executed within seconds. In practice, it makes it nearly impossible to intervene and withdraw a fraudulent transaction after it has been initiated. At the same time, there are no legal obligations for PSPs to deploy any measures allowing to revoke fraudulent transactions and refund stolen money to their customers. Only a few financial institutions voluntarily provide refunds in cases of fraud, but this can leave PSPs to absorb the financial losses while fraudsters retain the stolen funds. This lack of protections makes instant payments an attractive target for fraudsters who can quickly move stolen funds across multiple accounts. The technical infrastructure of PSPs may further lack the real-time monitoring capabilities needed to identify suspicious instant transactions, particularly in cases of social engineering and APP fraud. These vulnerabilities highlight the need for robust safeguards specific to instant payments, including enhanced fraud detection and monitoring systems capable of analysing transactions in real time.

To date, PSD3 has not addressed the absence of reversal mechanisms for instant payments, which remain highly susceptible to fraud. While the introduction of CoP obligations³⁷ provides an additional verification step, consumers still lack options to retract large transactions shortly after they are made. Implementing a “cooling-off” period or similar safeguard for high-value transfers could help mitigate these risks.

Aligning regulatory practices and technological standards for cross-border payments has proven to be a challenging objective. The widespread adoption of instant payments in the EU introduces additional security challenges due to its relative rapid implementation. Without cohesive collaboration and standardised approaches, gaps in security frameworks will persist, leaving the EU payment market increasingly vulnerable to financial crime.

3.2 Impact of combating payment fraud on the EU Single Market and Capital Markets Union

The effectiveness of payment fraud prevention has direct implications for the EU Single Market and the Capital Markets Union (CMU), both of which rely on a secure financial environment. Secure and stable payment transactions are an inevitable foundation of the market economy. Financial fraud, especially cross-border fraud, not only undermines the integrity of markets but also reduces consumer confidence. Its negative impact can lead to market distortions that in long term, jeopardising the stability of the entire payment market.

Creating a secure financial environment is essential for making EU capital markets more accessible, efficient, and transparent. Strong and uniform fraud prevention measures are necessary for achieving the EU’s objectives of a truly integrated financial market and a resilient capital market across member states. It therefore indirectly contributes to the stability and resilience of the EU single market, ensuring fair competition and reducing financial crimes’ negative impacts on cross-border economic activities.

³⁷ Articles 50 and 57 PSR.

Combating fraud and any other illegal activities affecting the financial interests of the EU is in a shared responsibility of both the EU and its member states.³⁸ However, significant differences in fraud prevention regulations across member states can hinder the effectiveness of the single market and CMU. Establishing a coherent regulatory environment is essential for reducing compliance burdens and fostering cross-border financial activities, thus enabling the single market and CMU to thrive.

4 Policy recommendations

The financial sector can be described as an intensively regulated industry. Some security-related provisions can be found in various EU policies and legislations (e.g. PSD2 or MIFID2³⁹). In response to the increasing cyber and information security threats, the EU has recently introduced a legislative framework⁴⁰ to enhance overall cybersecurity in the EU and operational resilience particularly in the financial sector that provides a structure for managing ICT risk, protecting sensitive information, and ensuring digital products and services are secure. Yet, the constant evolution of payment fraud tactics demands continuous refinement of regulatory approaches to maintain effective defences. From this point of view, introduction of new obligations and technical standards for financial institutions in order to guarantee the security of payment transactions and minimise security risks can be justified by objective of protecting the functioning of the payment market.

To confront these emerging challenges and adapt to evolving threat landscapes, the EU must consider targeted measures aimed at improving collaboration, advancing payment fraud detection capabilities, and enhancing consumer protection. Keeping in mind growing increasing fraud risks for the payment industry, it is necessary to introduce preventive measures that will have a stabilising effect in the long term. This ceplInput suggests the following key policy recommendations to address specific vulnerabilities in the financial sector and foster a more resilient regulatory environment:

1. Enhancing cross-border collaboration and information sharing

Fraudsters often exploit regulatory inconsistencies across EU member states, making stronger cross-border collaboration essential to mitigating fraud risks. To address this, the EU should establish harmonised protocols for fraud reporting, investigation, and data sharing among PSPs and competent authorities. This would facilitate timely information sharing and improved fraud detection in cross-border transactions.

Currently, some EU member states have developed voluntary information-sharing initiatives among financial institutions to address payment fraud. For instance, the Transaction Monitoring project in the Netherlands⁴¹ uses machine learning to improve individual financial institutions' fraud detection.

³⁸ Article 325 of the Treaty on the Functioning of the European Union (TFEU).

³⁹ Directive 2014/65/EU on markets in financial instruments. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065>.

⁴⁰ Including the Digital Operational Resilience Act (DORA), Network and Information Security Directive 2 (NIS2), and Cyber Resilience Act (CRA).

⁴¹ Transaction Monitoring Netherlands (2024). Transaction Monitoring Netherlands adapts its working method to new European legislation - TMNL.

Within this network, participating banks share transaction data which helps to detect suspicious patterns in the transactions and to identify financial fraud or money laundering. This project uses advanced analytics and machine learning to enhance detection capabilities. However, this level of collaboration exists only in select countries, which contributes to uneven financial security standards across the EU and leaves jurisdictions without similar initiatives more vulnerable to fraud and cybersecurity threats. Aligning cybersecurity and anti-fraud practices within financial institutions is therefore crucial for the EU to strengthen the resilience of its financial sector, as cyber threats and fraud often intersect. Harmonised protocols for fraud reporting and investigation as well as cybersecurity standards for financial institutions across all member states would reduce opportunities for fraudsters to exploit these jurisdictional inconsistencies, ensuring that financial institutions across all member states uphold the highest levels of security. These standards should particularly address requirements for SCA, cross-border monitoring, and a risk management framework to promote consistency across the EU. By creating uniform compliance requirements, the EU would not only enhance the overall security of its payment systems but also foster a more integrated market.

A practical solution would be to create an EU-wide platform for sharing fraud-related information among PSPs and competent authorities. To comply with the data protection provisions and to guarantee privacy, personal data should be anonymised and could be only disclosed to the law enforcement authorities in case of an opened investigation. Such a platform would streamline communication between PSPs and support faster responses to suspected fraud. Furthermore, this solution would enhance the EU's ability to combat cross-border fraud, which is challenging to address effectively due to jurisdictional differences.

2. Mitigating irrevocability of instant payments through security enhancements

As elaborated above, the irreversibility of instant payments makes them an attractive target for fraudsters. To minimise fraud risks and protect consumers, PSPs should implement additional security mechanisms to intercept fraudulent transactions before they are completed.

One effective measure could be the introduction of "cooling-off periods" for high-value transactions exceeding a specific threshold. During this period, which could last up to one hour, a payer could alert their bank of a suspected fraudulent transaction. The payee's bank would then be required to initiate a prompt reimbursement. While not mandatory for all PSPs, this option could be recommended as an added service that consumers can choose to enable if they wish.

Another useful tool could be the implementation of "kill switches" - account-freezing mechanisms available through online banking platforms and mobile apps. A kill switch would allow customers to instantly freeze all accounts and cards, stopping both outgoing and incoming transactions in cases of suspected fraud. This feature provides consumers with immediate control over their accounts, allowing them time to seek assistance and prevent funds from leaving their accounts.

3. Introducing clear liability standards for APP fraud

To establish a fair and predictable framework for fraud refunds across the EU, the European Commission should introduce clear liability standards for APP fraud in the next PSD review. A standardised, EU-wide definition of "gross negligence" would offer customers clarity on their rights and responsibil-

ities, eliminating the inconsistencies caused by varying national interpretations. Additionally, harmonising liability standards could motivate banks to adopt a high duty of care and to improve their anti-fraud strategies to better investigate specific types of fraud. Such protections would help customers feel secure in digital payments, especially instant and cross-border transactions, contributing to the European Commission's goal of an integrated digital market.

The current version of the PSD does not clearly differentiate the liability of PSPs and customers for losses incurred from authorised and unauthorised transactions. A tiered liability framework, tailored to different types of payment fraud, would best serve to create a safer and more reliable payment ecosystem, ensuring that both consumers and PSPs are adequately safeguarded against fraud risks. For low-risk transactions, minimal bank liability could apply where there is clear evidence of customer involvement or gross negligence, such as intentionally sharing sensitive information with fraudsters. Moderate-risk transactions would entail shared liability between banks and customers in cases of social engineering fraud, encouraging banks to educate consumers on security practices. High-risk fraud types, such as sophisticated impersonation scams, would place full liability on banks, as these rely on explicit abuse of the bank's name and reputation by fraudsters. By establishing a tiered liability framework tailored to the specific characteristics of each fraud type, the EU can foster a safer, more reliable payment ecosystem that aligns with consumer protection priorities and sustains the operational viability of the banking sector.

Furthermore, it should be better clarified if the payer's or payee's PSPs should be liable in case of fraudulent transaction. A revised approach should introduce a shared liability model, where responsibility for losses is balanced between the payer's and payee's PSPs. By sharing liability, both PSPs would be incentivised to invest in preventive measures. This approach was recently introduced in the UK, where the cost of reimbursing victims for APP fraud is shared between sending and receiving PSPs on the 50/50 basis.⁴² Such a shared liability model would address the role of "mule" accounts by holding both payer and payee banks accountable.

4. Promoting transaction monitoring enhancements for PSPs

For instant payments, where transactions are completed in seconds, it is desirable to encourage PSPs to implement real-time transaction monitoring to detect potential fraud patterns prior to execution. This monitoring should cover all payment channels, including ATMs and POS systems, enabling a comprehensive view of transaction patterns and quick detection of inconsistencies. Such measures would ensure better enforcement of rules and safeguards essential for maintaining market stability.

5. Integrating advanced technology and AI for fraud detection

Advanced machine learning and artificial intelligence technologies that can analyse transaction patterns in real-time should be implemented across the industry to detect unusual activities quickly.⁴³

⁴² UK Payment Systems Regulator (2023). PS23/3: Fighting authorised push payment fraud: a new reimbursement requirement. <https://www.psr.org.uk/publications/policy-statements/ps233-fighting-authorised-push-payment-fraud-a-new-reimbursement-requirement/>

⁴³ The opportunities of the usage of advanced technology in fraud prevention are far-reaching, s. Hernandez Aros L., Bustamante Molano L.X. et al (2024). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanit Soc Sci Commun* 11, 1130; Polak P., Nelischer C. et al (2020). Intelligent finance and treasury management: what we can expect. *AI Soc* 35(3):715–726.

Standardizing these technologies will enhance fraud detection capabilities for APT and APP fraud, providing faster responses to emerging payment fraud techniques. More competition through an orderly and security-regulated market access would further enhance innovation and consumer choice while ensuring a high level of trust and safety in digital transactions.

6. Enhancing consumer education on fraud prevention

While PSD3 emphasises consumer education, it lacks specific provisions to ensure that fraud prevention and security measures are accessible to vulnerable users, such as the elderly or non-tech-savvy individuals. SCA requirements are intended to be accessible, but without dedicated consumer education programs, these groups may remain susceptible to sophisticated payment fraud tactics. Financial institutions should be required to proactively inform their customers about current fraud risks and trends by publishing educational materials on their websites and regularly encouraging customers to increase their fraud awareness. This will foster more secure digital behaviour among consumers, contributing to overall financial security across the EU.

7. Empowering the Anti-Money Laundering Authority (AMLA)

The establishment of the Anti-Money Laundering Authority (AMLA) represents a significant opportunity for more centralised and coordinated antifraud efforts within the EU. AMLA should be equipped with a clear mandate to set consistent standards across member states and facilitate information sharing in cooperation with the European Anti-fraud Office (OLAF), national competent authorities, Euro-pol, and the European Public Prosecutor's Office (EPPO). It is recommended that AMLA be required to publish an annual fraud and AML report, assessing data from member states to help identify fraud patterns and expose complex fraud schemes spanning multiple jurisdictions.

The recommendations listed above can be divided into three levels of action, each addressing distinct aspects of combating financial fraud: I) Collaboration and standards; II) Technological advancements; and III) Consumer and institutional education (see Fig. 3). As fraud tactics evolve, a unified, proactive approach will enable the EU to protect the payment services users and to safeguard the integrity of the payment market, maintaining a fair and competitive financial environment.

Fig. 3: Three levels of action to combat payment fraud in the EU

Source: own illustration.

5 Conclusions

Digital innovation is reshaping the financial sector, but it also brings increasingly sophisticated payment fraud schemes. The growing vulnerabilities in interconnected payment systems, exacerbated by fragmented fraud liability frameworks and the evolution of financial fraud techniques and cyber risks present the central challenges in combating payment fraud in the EU. Despite incremental progress through regulatory advancements like PSD3 and PSR, critical regulatory gaps still persist. Emerging payment trends, such as the rise of instant payments, add new dimensions to fraud risks. The EU regulatory framework has to adapt in a timely manner to these evolving challenges. Addressing these vulnerabilities now will not only safeguard current payment systems but also lay the groundwork for a more secure digital financial ecosystem in a long term. Safeguarding the financial sector from fraud is furthermore essential to maintaining the integrity and stability of the EU's single market and CMU.

Combating payment fraud requires a multifaceted strategy that combines three levels of action: collaboration and harmonised standards, technological innovation, and education. To mitigate the increasing risks, EU regulators should prioritise a harmonised approach in dealing with payment fraud and cybersecurity risks. A unified, tiered framework to fraud liability is essential to eliminate disparities across member states, ensuring a level playing field that supports fair competition and fosters trust in payments, especially in cross-border and instant transactions. A robust antifraud strategy should fur-

thermore include strengthened cross-border collaboration to share intelligence and best practices, enhanced transaction monitoring systems based on advanced technologies for real-time fraud detection, aligning cybersecurity and fraud prevention practices, and greater consumer and institutional education to improve awareness of emerging threats. Empowering entities like the AMLA to coordinate antifraud efforts across jurisdictions is crucial for a cohesive response. By implementing these measures, the EU can bolster the resilience of its financial sector and enhance consumer confidence, particularly in the context of digital and instant payments.

**Author:**

Dr. Anastasia Kotovskaia, LL.M., Head of Department Financial Markets & Information Technologies
kotovskaia@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN

Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin
Phone + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN, the **Centre de Politique Européenne** PARIS, and the **Centro Politiche Europee** ROMA form the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

The cep institutes are specialised in the analysis and evaluation of European Integration Policy. They publish their scientific work independently of any vested interest, in favour of a European Union that respects the Rule of Law and the principles of the social market economy.