Secure fintech for economic resilience: strengthening digital payments and sustainability under the EU regulatory framework

Ionuț Horătău[1]

To cite this article:
Horătău, I. (2026). Secure fintech for economic resilience: strengthening digital payments and sustainability under the EU regulatory framework. Romanian Journal of Economics, 63(2), 203-221.

Abstract. Objective*: This study proposes to examine how the EU legal framework on payments, by enhancing the security of digital payment services and supporting economic sustainability and fintech ecosystems, might contribute to economic resilience in the European Union (EU). As digital payments become embedded in the EU's transactional backbone, safeguarding electronic payments is essential not only for maintaining payment services user trust and market stability, but also for ensuring the long-term viability and responsible evolution of payment services. The EU is currently redefining its regulatory legal framework through the transition from the revised Payment Services Directive (PSD2) to the Third Payment Services Directive (PSD3) and the Payment Services Regulation (PSR). In this context, the research proposes to investigate how emerging legal framework, together with the approach of the Digital Operational Resilience Act (DORA) and the increasing integration of innovation monitoring tools in supervision, can reinforce secure and sustainable electronic payment ecosystems. The research is also analyzing the complementary impact of the technological progress driven by fintech actors as definitory factors to support economic resilience and sustainability.* ***Method****: The study employs a combined methodological approach. Firstly, it uses a systematic review of the current EU legislation, regulatory proposals, guidelines of the European Banking Authority (EBA) to assess how legal and supervisory mechanisms interact to mitigate ICT and cyber risks without constraining innovation or imposing a disproportionate burden on market participants. Secondly, to complement this regulatory analysis, semi-structured interviews were conducted with fintech practitioners and experts involved in authorization and oversight processes. These interviews offered more practical insights into operational challenges and on emerging security enhancements, that payment service providers are mandated to strengthen operational resilience and contribute to the security of digital payment transactions.* ***Results****: The analysis preliminary indicates that strengthened security requirements, such as strong customer authentication (SCA), advanced transaction monitoring mechanisms and risk-based transaction analysis, tokenization of card data, real-time fraud detection, cross-border incident reporting and coordination, and reinforced oversight of non-bank payment service providers, are key elements in ensuring accessible and safe payment services. On another perspective, the results concluded that an additional prerequisite of supporting economic sustainability is that the legal framework should include the proportionality principle. Mechanisms such as innovation hubs, regulatory testing environments, and structured market dialogue might help supervisory authorities anticipate technological developments and adapt the regulatory expectations, taking into consideration the proportionality and reducing the risk of regulatory misalignment. While the full impact of PSD3/PSR and DORA remains uncertain until implementation, preliminary findings suggest that integrating resilience testing, harmonized oversight, and updated security measures might reduce fraud and could foster security, innovative, and environmentally and operationally sustainable payment services across*

[1] Romanian Academy, School of Advanced Studies of the Romanian Academy, Doctoral School of Economic Sciences, National Institute for Economic Research "Costin C. Kirițescu", "Victor Slăvescu" Centre for Financial and Monetary Research, Bucharest, Romania; e-mail address: ionut.horatau@bnro.ro.

the EU. Policy Recommendations: The study proposes incorporating security and resilience assessments into authorization processes, enhancing EU-level coordination in the oversight of critical payment functions, and regularly updating technical standards in line with PSD3/PSR and DORA requirements. Strengthening safeguards for ICT risk management and cyber resilience might be crucial for supporting reliable and sustainable digital payment services. ***Originality****: This research contributes to a novel EU focused assessment that integrates regulatory analysis with practitioner perspectives, connecting legal insights with operational realities. Unlike existing literature, it emphasizes how well-calibrated security measures and oversight practices can reinforce trust, market confidence, and the sustainable development of payment services. By outlining actionable strategies for regulators and industry stakeholders, the study adds to ongoing discussions on the need for a proportional approach to support an innovation friendly environment in order to foster a sustainable fintech-enabled payment ecosystem in the European Union.*

Keywords*: Fintech regulation; Digital payments; Operational resilience; Economic and social sustainability; PSD3/PSR.*
JEL classification*: G21, G28, K23, O33, E42*

1. Introduction

Digital payments increasingly form the backbone of the European Union's (EU) financial ecosystem, driving financial inclusion, economic resilience, and sustainable growth (European Central Bank, 2024; Korus, 2024). The expansion of fintech has introduced transformative technologies that it seems to enhance efficiency and accessibility of payment services, yet it also raises concerns about cybersecurity, operational resilience, and environmental and social sustainability (Gounari et al., 2024; Vashishta, 2025). Also, from the perspective of digital payment services it seems that it faces additional challenges such as fraud risks, regulatory compliance, and financial inclusion gaps. As digital finance becomes deeply embedded in Europe's economic development, ensuring secure, sustainable, and trusted payment infrastructures and services emerges as a cornerstone for long-term economic resilience and social sustainability (Polasik et al., 2024). Fintech ecosystems obviously are dynamic networks of innovative payment service providers (PSPs), technology platforms, and regulatory sandboxes undoubtedly play a pivotal role in this evolution. From this perspective, they enable operational efficiency, bust competition, and financial inclusion, yet also raise new operational and cyber-risks (Preziuso et al., 2023; Sethupathy, 2025).

The importance of this topic is particularly acute now because the EU is at a regulatory inflection point. The current retail payments regime under the PSD2 is being replaced by a new "payment services package" comprising the PSD3 and PSR (Grabowski, 2025; Tsymbaliuk, 2024). At the same time, DORA introduces binding requirements for ICT risk management, incident reporting, testing, and oversight of third-party ICT service providers in the financial sector (Buttigieg & Zimmermann, 2024; Lichosik, 2023). This regulatory matrix invites the question: how can fintech-enabled payment services strengthen economic resilience and sustainability within the European Union by securing digital payments while preserving innovation and digital inclusion?

This study aims to examine how evolving EU legal instruments and supervisory tools can contribute to securing digital payment services and simultaneously promote innovation through technological advancement, financial integration, and environmental and social sustainability within Europe's digital financial architecture. The contribution lies in an EU-centric evaluation: combining regulatory analysis with practitioner insights (via own expertise as regulator and other expert interviews in the fintech payments sector), thereby intending to bridge the gap between high-level legal frameworks and operational realities (Anwar et al., 2025; Tarasenko et al., 2025).

The paper is structured as follows: Section 2 summarizes existing research on fintech, payments security, and regulatory frameworks through a comprehensive literature review; Section 3 explains the regulatory mapping and interview approach employed in this study; Section 4 presents the main findings on evolving requirements and fintech practices; Section 5 discusses the economic sustainability and social impact dimensions; and Section 6 concludes with implications, limitations, and future research directions.

2. Literature review

The literature on payments and fintech regulation has evolved along three main dimensions: technological innovation, security and resilience, and sustainable economic transformation.

2.1 Technological innovation and financial inclusion

Fintech has expanded access to financial services, reducing transaction costs and bridging the gap between consumers, merchants, and financial institutions as payment services providers (Preziuso et al., 2023). Digitalization facilitates cross-border remittances, real-time transfers, and micro-payments that enhance participation in the digital economy (Korus, 2024). Starting with the mandate under PSD2, open banking systems, allows third-party providers to initiate payments or access payment account data securely, supporting financial integration and competition (Polasik et al., 2024; Zunzunegui, 2018).

Research demonstrates that open banking strengthens the infrastructure needed for inclusive finance, though it was not originally designed specifically for underserved groups (Preziuso et al., 2023). EU standardization through open banking and SEPA interoperability has stimulated new payment services and more efficient intra-EU flows, reinforcing innovation cycles that can enhance the perspective of economic sustainability and material well-being (Korus, 2024). However, payment services users adoption, especially on the consumers side, remains limited by lack of awareness, data privacy and security concerns, and unclear value propositions from the payment services providers side, despite PSD2 increasing competition and innovation (Heins & Rigopoulos, 2024).

Digital payments, including fintech platforms, can improve access to payment services, financial integration and reduce transaction costs, but sustained gains depend on effective regulation and public-private collaboration (Imaningati et al., 2024; Sahu, 2023). Regional disparities matter significantly: EU fintech adoption is uneven, with regions possessing stronger digital infrastructure and supportive regulation showing larger gains in fintech use and related welfare effects (Orăștean et al., 2024).

2.2 Security and regulatory oversight

Studies emphasize the vulnerabilities of open banking APIs and the need for robust authentication and encryption mechanisms (Gounari et al., 2024). Comparative analysis reveals a lack of clarity in preexisting technical security specifications across frameworks such as NIS2, the Cybersecurity Act- Regulation (EU) 2019/881, GDPR, ISO 27001, and PCI-DSS, which undermined consistent PSD2 implementation and raises privacy and security risks for banks and third-party providers (Gounari et al., 2024). This was a preexisting baseline further complemented by the framework envisaged under DORA.

Regulatory responses, notably SCA, transaction monitoring mechanism and transaction risk analysis provisions, aim to reduce fraud without hindering user experience (Grabowski, 2025; Polasik et al., 2024). Securing fintech ecosystems, especially on the payments side, seems to require secure coding, encryption, payment service user identity management, real-time threat detection as transaction monitoring mechanism, and Zero Trust Architecture to manage expanding attack surfaces from APIs, cloud services, and third parties (Vashishta, 2025). Tokenization, biometrics, encryption, and AI-driven anomaly payment transaction detection create layered defences that reduce fraud and build consumer trust in digital payments (Sethupathy, 2025).

Meanwhile, DORA extends ICT resilience obligations to fintechs, as part of the third-party service providers legal perspective under this regulation, marking a systemic shift toward operational security in the financial sector (Buttigieg & Zimmermann, 2024; Ni Thuama & Costigan, 2024). It seems that fraud and cyber threats associated to card and payments services in general are dynamic; shifting from reactive to proactive transaction monitoring mechanisms, industry cooperation, especially on payment service users' perspective and performance key performance indicators (KPIs) improves resilience and ensure business continuity under stress conditions (Tarasenko et al., 2025).

2.3 Sustainability and financial resilience

Recent policy research links secure, inclusive payment services and infrastructures to broader economic resilience and sustainable development. The European Green Deal and Digital Finance

Strategy both underline the potential of digital finance to channel capital efficiently while reducing resource use and promoting transparency (European Commission, 2020). Frameworks for "liable and sustainable by design" technologies propose regulatory instruments to ensure digital innovations align with social and environmental objectives while preserving trust (Aseeva, 2023).

Security technologies such as tokenization, encryption, biometrics, and AI might be considered also as important instruments for reducing the fraud phenomenon in payments, lowering enforcement costs, and fostering consumer trust that enables wider assimilation of payment services and social inclusion benefits (Sethupathy, 2025). Digital payments can enhance financial inclusion and system stability if adequate risk mitigation frameworks, supervision, and cooperative public-private measures mitigate fraud and privacy risks (Sahu, 2023). Analyses over the digital euro project emphasize its complementary role to cash, privacy and offline considerations, and the need for cybersecurity and inclusive design to support social policy goals (Dukhnevych, 2025).

2.4 Research gaps

Despite growing interest, empirical research rarely integrates sustainability, resilience, and regulatory frameworks into a unified analytical perspective. Academic research in this field remains limited, particularly in connecting payment security and fintech innovation with social welfare and environmental sustainability. This study fills that gap by examining how the security of digital payments supports long-term economic and social goals under EU regulation, combining regulatory analysis with operational insights from fintech practitioners.

This study contributes to the existing literature by offering an integrated EU-focused assessment that links regulatory evolution (PSD3/PSR and DORA) with operational realities observed in fintech ecosystems. Unlike prior research, which typically examines security, innovation, or sustainability in a separate approach, or in different combinations, this paper combines regulatory analysis with practitioner insights to show how secure digital payments can reinforce economic resilience and sustainability. The study also advances the literature by mapping security obligations to economic and social outcomes and by identifying proportionality-based supervisory approaches that support innovation without compromising resilience.

3. Methodology and data

3.1 Research design and hypothesis framework

The study employs a mixed-method qualitative research design, integrating regulatory analysis with semi-structured expert interviews to examine how EU payment services regulation influences security, resilience, innovation, and sustainability. The methodological framework is explicitly structured around four hypotheses (H1–H4), which define the analytical logic of the study and guide both data selection and interpretation.

The regulatory analysis maps PSD2, PSD3, PSR, and DORA provisions to operational practices, focusing on cybersecurity, strong customer authentication, adequate transaction monitoring mechanisms, incident reporting, and ICT resilience. Given that PSD3 and PSR remain under legislative negotiation and that DORA has only recently entered into application, the study does not aim to estimate causal effects quantitatively. Instead, it evaluates regulatory impact mechanisms, focusing on how regulatory requirements are expected to translate into operational practices and economic outcomes.

From this perspective, expert interviews provide qualitative insights into how payment service providers (PSPs) and fintechs translate regulatory expectations into practical innovations that enhance both system reliability and sustainable development outcomes.

3.2 Regulatory analysis

The regulatory analysis addresses different hypotheses: H1 (Security and operational resilience) and H4 (Regulatory harmonization), through a systematic qualitative examination of EU legal instruments and supervisory guidance. A central focus of the review was the PSD2, alongside its formal evaluation by EU institutions and recent academic assessments (European Parliament, 2023; Polasik et al., 2024). For H1, the analysis maps strengthened security and resilience requirements to operational

risk-mitigation mechanisms. This includes SCA, transaction monitoring and fraud prevention tools, incident classification and reporting obligations, and ICT risk management frameworks. The analysis assesses whether these measures plausibly reduce fraud exposure, operational disruptions, and systemic vulnerabilities, thereby supporting economic resilience and trust in digital payments.

In response to these challenges, it was the European Commission's June 2023 legislative package proposing a new directive (PSD3) and a directly applicable regulation (PSR). These proposals signal a structural shift in the oversight perspective of the payment services by clarifying supervisory powers, strengthening consumer protection, and tightening the regulatory perimeter around non-bank payment service providers (Grabowski, 2025; Tsymbaliuk, 2024). For H4, the analysis focuses on regulatory structure and scope, comparing the directive-based approach of PSD2 with the proposed shift toward a regulation (PSR) and the cross-sectoral harmonization introduced by DORA. Attention is given to uniformity of application across Member States, supervisory convergence, and reduced compliance uncertainty in cross-border payment activities.

They also aim to reduce fragmentation by transitioning core rules from a directive to a regulation, thereby advancing cross-border harmonization. This perspective is also for opening the usage of new category of funds as digital euro under proposal for a Regulation on the establishment of the digital euro (European Parliament & Council of the European Union, 2023) and for using the electronic money tokens under MiCA Regulation for payments services purpose PSR.

A second pillar of the regulatory review was DORA, which introduces a comprehensive regime for managing ICT risk across the financial sector. DORA represents a paradigm shift by consolidating operational resilience requirements that had previously been dispersed across multiple guidelines. The regulation addresses ICT risk management governance, incident classification and reporting, digital-operations resilience testing, and oversight of critical third-party providers such as cloud service operators (Buttigieg & Zimmermann, 2024; Lichosik, 2023; Ni Thuama & Costigan, 2024). Its emphasis on harmonized technical standards seeks to ensure that financial entities, including credit institutions, payment institutions and electronic money institutions, can withstand, respond to, and recover from cyber threats and operational and security incidents in an increasingly interconnected digital ecosystem.

The chapter's analysis also incorporated supervisory technical standards and guidelines issued by the European Banking Authority (EBA) and national competent authorities. These instruments provide operational detail on the implementation of SCA, common and secure communication interfaces, tokenization practices, and advanced transaction monitoring systems incorporating transaction risk analysis (Gounari et al., 2024; Grabowski, 2025). The supervisory guidance plays a critical role in shaping market practices, particularly by interpreting regulatory obligations in light of evolving fraud typologies and technological advancements.

Overall, it seems that the regulatory trajectory suggests a maturing digital finance ecosystem in which technological evolution is closely accompanied by enhanced governance and resilience requirements. The interplay between PSD2, the proposed PSD3/PSR framework, DORA, and EBA supervisory standards illustrate the EU's commitment to securing digital payments while fostering competitive, innovative, and resilient financial services across the Single Market.

3.3 Expert and fintech interviews

This study incorporates a qualitative methodology grounded in semi-structured interviews that provided the primary empirical basis for examining H2 (Proportionality and innovation) and H3 (Sustainability and inclusion). Interviews were conducted with practitioners from the European payment ecosystem, complemented by the author's long-standing professional expertise in EU regulatory processes.

The methodological design is also informed by the author's direct participation in EU legislative and supervisory processes, including involvement in working groups responsible for the development of PSD1, PSD2 and the current PSD3/PSR proposals, as well as in national transposition activities. This experience extends to contributions within several working groups within European Supervisory Authorities, focused on security measures, ICT and operational resilience, authorization processes, innovation monitoring, and oversight cooperation.

Participation in the elaboration of measures under the DORA Regulation, the MiCA Regulation and related guidelines offer an additional analytical lens for interpreting regulatory intentions, supervisory expectations and implementation challenges.

For H2, interviews explore how proportionality mechanisms such as innovation hubs, regulatory sandboxes, simplified reporting, and risk-based supervision influence compliance costs, market entry, and innovation capacity, particularly for smaller PSPs and fintechs. The analysis examines whether these mechanisms mitigate regulatory burdens without undermining security objectives.

For H3, interviews focus on the perceived links between secure digital payments and broader sustainability outcomes. Topics include reductions in transaction costs, efficiency gains from interoperability, trust-driven adoption of digital payments, and implications for financial inclusion and environmentally efficient payment infrastructures.

This background is incorporated through a structured, transparent use of expert judgment, enhancing the interpretative depth of the empirical material without substituting or predetermining the insights generated from the interviews.

The empirical component consisted of semi-structured interviews with representatives of eight organizations active across different EU jurisdictions, including payment service providers, technology-driven fintech firms and regulatory consultants. Sampling followed a purposeful logic, targeting entities directly involved in payment security, authentication processes, transaction monitoring, API design, incident reporting, and ICT risk management. This ensured that the collected perspectives reflected the operational realities of firms for which compliance with security requirements is central to their business model and to their contribution to a resilient and sustainable payments environment.

Interviews explored the practical challenges encountered in implementing regulatory obligations, the technological and organizational innovations adopted to strengthen security, and the perceptions of how evolving regulatory frameworks support or constrain innovation and market competitiveness. Discussions covered themes such as the integration of new authentication procedures, the use of advanced data analytics and criteria for fraud detection, the governance of third-party ICT providers, the adaptation to supervisory expectations, and the broader implications of these measures for payment service users' trust, operational continuity and long-term economic performance.

The interviews were conducted remotely, recorded with the explicit consent of the persons involved, transcribed verbatim, anonymized, and also coded thematically. The coding framework combines deductive categories derived from the four hypotheses with inductively generated themes emerging from practitioner experience.

The integration of the experts and practitioners' interviews provided a robust methodological foundation for examining the implications of the adequate security measures for the payment services as determinants of economic sustainability. The approach captures how regulatory requirements translate into everyday operational processes, how security investments support market trust and resilience, and how legislative and supervisory developments shape innovation trajectories in the payments sector. The combined qualitative and expert informed methodology therefore offers a comprehensive, context sensitive understanding of the dynamics linking payment security, regulatory evolution and sustainable digital finance.

Preliminary findings from regulatory analysis and interviews perspectives were integrated through analytical triangulation, systematically comparing regulatory objectives, supervisory guidance, and operational practice. Each hypothesis (H1–H4) served as an adequate way of evidence across sources, reducing repetition and ensuring coherence between theory, methodology, and results.

3.4 Data limitations

It seems that the qualitative nature of the empirical material might introduce several limitations that shape the scope and extensibility of the findings. The interviews were based on a dedicated sample selected based on the direct involvement in payment security processes and regulatory compliance. While this approach ensures a relevant balance between the legal perspective and the operational facts, it does not provide a statistically representative picture of the entire fintech payments landscape in the European Union. The perspectives only captured a more general view of possible national payment landscapes or reflected the experiences of specific fintechs with advanced operational exposure to secure payment requirements, and their views may differ from those of smaller market actors. There is also an

additional constraint because fintech entities might develop different business models or might operate in less regulated segments of the payment services ecosystem or different oversight practices.

Another limitation arrives from the evolving nature of the legal framework. Several of the legislative texts examined, particularly the PSD3/PSR package, remain under negotiation at the time of analysis. This means that some elements of the assessment concern not an enforced legal framework but rather the perspective of a regulatory proposal. From this point of view, although the proposals offered a clear perspective on enforced security measures, a degree of uncertainty still remains regarding the final scope and supervisory approaches that will ultimately reshape the payment services providers and different stakeholders' practices. Although the analysis draws on the author's extensive involvement in EU and EBA working groups, which provides a preliminary insight into the direction and rationale of regulatory developments, the final legislative outcomes may differ substantially from the initial versions examined for this research.

Despite existing limitations, integrating regulatory assessments with practitioner insights may yield significant contributions, as methodological triangulation encompassing legal scrutiny, practical experience, and expert interpretation fosters a more nuanced understanding of secure payment services in practical contexts, thereby facilitating a comprehensive analysis of the interplay between security mandates, operational resilience, and economic viability beyond what singular documentary analysis or interviews could achieve.

4. Research results and comments

To achieve an adequate perspective on the findings, these are presented along inter-related dimensions comprising the following: regulatory developments, fintech operational and security responses, and interactions between regulation and innovation in payment ecosystems, as a balanced approach between ensuring the need for a secure payment services environment and an innovation supportive perspective.

4.1 Regulatory developments strengthening payment security and resilience

4.1.1 Enhanced authentication and fraud-prevention requirements

The proposed PSD3/PSR framework for sure will strengthen authentication and fraud-prevention obligations to address persistent vulnerabilities persistent under PSD2. The PSR introduces stricter requirements concerning strong customer authentication procedure, tokenization and real-time transaction monitoring (Grabowski, 2025). Notably, the PSR maintains the principle that SCA must rely on two independent elements from different categories, thereby rejecting the use of two factors from the same category and reinforcing the layered security model. The proposal further expands liability for payment service providers in cases of complex fraud scenarios involving spoofing fraud and imposes more detailed expectations regarding behavioural analytics, dynamic risk scoring and enhanced monitoring capacities (Polasik et al., 2024).

Research increasingly demonstrates that tokenization, biometric authentication, encryption frameworks and AI-driven anomaly detection reinforce multilayered defences capable of reducing fraud rates and improving user confidence in digital payment channels (Sethupathy, 2025). Systems employing machine learning for fraud detection tend to achieve higher accuracy and adaptiveness, though they require strong governance and oversight to mitigate risks related to bias, transparency, operational complexity and customer-experience friction (Anwar et al., 2025). Together, these developments show a regulatory and technological shift toward more sophisticated and inclusive authentication frameworks that support the broader objective of securing digital payment infrastructures.

4.1.2 Frameworks for market structure and competitiveness

Central driver of the PSD3/PSR reform is the need to address structural shortcomings that emerged under PSD2, including partial differences in national implementation, although it is a maximum harmonisation directive, the main focus was represented by the uneven supervisory practices and disparities in the treatment of bank and non-bank PSPs (European Parliament, 2023; Polasik et al., 2024). The main transition from a directive to a regulation for core conduct provisions, especially the perspective on transparency in conditions and the rights and obligations of the parties aims to create

more uniform obligations across the EU, reducing fragmentation and uncertainty for payments services providers operating cross-border. This regulatory shift is expected to give fintech PSPs a more predictable environment for scaling operations and reducing the compliance asymmetries that previously disadvantaged especially small payment service providers as non-bank actors (Korus, 2024; Tsymbaliuk, 2024).

Although it seems clear that empirical evidence indicates that PSD2 contributed to market entry through open banking services, innovation and fraud reduction, due to the inconsistent national transpositions and divergent supervisory approaches that was an important limitation factor that reduced the effectiveness of some PSD2 provisions (Polasik et al., 2024). The PSR's directly applicable framework is intended to overcome these challenges by creating more coherent market conditions, strengthening competitive neutrality and supporting a payments market in which secure, innovative and resilient services can develop sustainably.

4.1.3 Digital operational resilience via DORA

The DORA, on the other hand, introduces binding requirements in ICT risk management, incident reporting, resilience testing and the oversight of critical ICT third-party service providers (Buttigieg & Zimmermann, 2024; Lichosik, 2023). Although some European Banking Authority guidelines issued under PSD2 mandate, previously dealt with a similar approach for addressing ICT risks and incident reporting, the DORA legal framework establishes a unified governance framework requiring financial entities to ensure board-level accountability, implement comprehensive ICT risk controls, maintain capabilities for incident detection and recovery and report significant incidents to supervisors under standardised timelines (Ni Thuama & Costigan, 2024), more or less under similar criteria and timeframes, but with an extended approach for third party providers risks and a robust framework for testing the overall security measures. Within the payment's domain, the regulatory analysis shows that incident-reporting obligations previously established under PSD2 are also integrated into the DORA regime to minimise duplication, strengthen consistency with the previous approach and reduce the administrative burden on PSPs for ensuring compliance with current DORA perspective (Buttigieg & Zimmermann, 2024).

While DORA provides a unified baseline for digital resilience across the financial sector, challenges remain in achieving supervisory convergence and avoiding fragmentation in national implementation approaches (Lichosik, 2023). Ensuring consistent application of DORA's requirements, especially regarding oversight of ICT third-party providers, it seems will be of a high importance for sustaining secure and resilient payment ecosystems, especially in case of cross border business activity, that ultimately will broader economic stability.

4.1.4 Innovation-friendly supervision and market monitoring

At the level of European supervisory authorities, different national competent authorities increasingly are using innovation hubs, regulatory sandboxes and structured engagement mechanisms to monitor technological developments and support proportionate regulatory adaptation to address also the specific need to support the fintech companies, that tend to be more agile in developing innovative solutions (Polasik et al., 2024; Pulatov, 2025). These instruments are designed to facilitate dialogue between regulators and fintechs, enhance supervisory awareness of emerging technologies and also, the most important aspect, to enable controlled experimentation with innovative payment solutions. Policy analyses and innovation monitoring practitioners argue that such mechanisms support more inclusive financial markets and strengthen the capacity of microfinance institutions and fintech actors to collaborate in delivering secure, innovative and accessible services (Preziuso et al., 2023).

Although empirical research on the long-term effects of these supervisory tools remains relatively limited, practitioner insights suggest that regulators increasingly aim to anticipate technological transformations and calibrate security, operational resilience and consumer-protection requirements in ways that do not impede innovation (Negrea et al., 2025). This trend reflects a broader shift toward a regulatory posture that balances robust security safeguards, necessary for economic sustainability and fraud mitigation, with flexibility to foster experimentation and responsible market development.

4.1.5 Engagement with regulatory innovation frameworks

In general, the fintech entities intending to participate in regulatory sandboxes and innovation hubs to interact and accommodate with national competent authorities, enabling them to pilot new authentication flows, API services, or payment-initiation models under supervision (Polasik et al., 2024; Preziuso et al., 2023). On the other perspective, based on the interviews with different payment market stakeholders, this was also seen as a pre-validation of the viability of the business model. This engagement might also mitigate regulatory uncertainty and accelerate innovation while maintaining clear regulatory oversight and ensuring consumer protection.

It is important to note that fully implementing the PSR and DORA might bring additional costs for the PSPs. From this perspective the costs mainly arise from developing adequate strong customer authentication solutions, improving transaction-monitoring systems, reinforcing ICT security, and also from ensuring the compliance with the new reporting and resilience-testing obligations arising from DORA. In the short to medium term, such requirements increase operational expenses.

The impact of these costs is not uniform across the market. From the perspective of large payment services providers as banks and well-established fintech firms, they generally have the financial capacity, technical infrastructure, and specialized staff needed to absorb compliance investments without major disruption. On the side of smaller and medium-sized payment services providers they might face greater difficulties from the perspective of cost for ensuring regulatory conformity. As such, the interview insights indicated that compliance costs can slow down product and services developments, might limit innovation, and also can increase the reliance on external technology providers, which may reduce, from this perspective, the strategic flexibility.

These differences might also shape the market competitiveness. On one side, while regulatory harmonization across the EU can reduce cross-border barriers and create more consistent competitive conditions, on the other side, higher compliance costs may place smaller providers at a disadvantage. In some cases, this can lead to market exit or increased consolidation. From this perspective it can be appreciated that there is a stringent need for a proportional approach, through balanced measures, including simplified requirements for low-risk providers, innovation hubs, and regulatory sandboxes. Therefore, in my opinion these instruments might play a key role in ensuring that stronger security and resilience standards do not undermine competition or market diversity.

4.2 Interaction between regulation, innovation, and economic resilience

The interplay between regulatory evolution and fintech ecosystem dynamics reveals several key insights:

4.2.1 Trust and market stability

It seems that enhanced security requirements (SCA, tokenization, real-time transaction monitoring mechanisms) reinforce consumer trust in electronic payments, which underpins usage growth and hence economic resilience (Sethupathy, 2025). But, without robust security, payment outages, and especially fraud, or large-scale disruptions could undermine the payment services users trust and reduce digital payments adoption, harming the broader fintech ecosystem and economy (Tarasenko et al., 2025).

4.2.2 Proportional regulation fosters innovation

Fintech actors emphasize that the regulatory framework must remain proportionate: overly prescriptive rules and difficult to interpret in practice might reduce the fintech agility and innovation, while too-light oversight may increase systemic risk (Polasik et al., 2024). The emerging use of fintech innovation hubs and regulatory sandboxes appears to offer a more adequate mechanism to balance resilience with innovation, while allowing for controlled experimentation, better informing competent oversight authorities, and maintaining consumer protection (Preziuso et al., 2023; Pulatov, 2025).

4.2.3 Harmonization and level playing field

The move from national implementations of PSD2, with different national option, to a directly EU applicable regulation (PSR) and uniform resilience standards under the DORA framework, definitely will help reduce fragmentation, regulatory arbitrage, and market imbalances between

traditional payment services providers as banks and small fintech PSPs across jurisdictions (Korus, 2024; Tsymbaliuk, 2024). This enhances the integrity and competitiveness of the internal market for payment services and supports cross-border financial integration (Grabowski, 2025).

4.2.4 Third-party ICT supply chain as a systemic risk vector

Developed fintech ecosystems amplify supply chain dependencies on cloud providers, API platforms, and data analytics firms (Buttigieg & Zimmermann, 2024; Vashishta, 2025). The DORA legal framework is placing this risk in the regulatory perimeter, helping prevent a single-point provider failure from cascading across multiple payment service providers, and different EU jurisdictions. This strengthens the resilience of the payments market as a whole and addresses a critical systemic vulnerability.

4.2.5 Remaining gaps and challenges

Despite the regulatory advances reflected in the PSD3/PSR proposals and the introduction of DORA, several challenges continue to shape the environment in which payment service providers operate. The ongoing negotiation of the PSD3/PSR package generates a degree of regulatory uncertainty for firms planning medium-term investments in authentication technology, since it is still not clear the full perspective of the fraud-monitoring infrastructure and ICT resilience. It seems that uncertainty regarding the final scope limits the ability of PSPs to commit to long-term implementation strategies and may delay the alignment of internal security frameworks with future requirements (Grabowski, 2025; Tsymbaliuk, 2024). A complementary guiding role should be assumed by the different national competent authorities

Resource constraints, either they are human or financial, remain a structural concern for smaller fintech PSPs, particularly those operating at an early stage in payments markets, as that tend to become one of the most heavily regulated segments of the financial sector. Implementing the full suite of resilience measures envisaged by the new legal framework under DORA, including advanced penetration testing, comprehensive ICT third-party oversight or robust exit strategies, may exceed the technical or financial capacity of smaller entities. In my opinion such disparities raise questions regarding proportionality, supervisory expectations and the risk that compliance obligations could reinforce competitive asymmetries between large incumbents and smaller innovators (Polasik et al., 2024). These issues remain central to discussions on whether harmonized rules can be applied in a way that supports both security and an open, competitive payments market.

Another challenge concerns the limited empirical evidence on the broader macro-financial implications of forthcoming regulatory changes. While the frameworks aim to strengthen resilience, there is still insufficient research on how the forthcoming PSD3/PSR legal framework with harmonized authentication rules, enhanced fraud prevention obligations and ICT resilience requirements will influence systemic risk, cross-border payment services development or the management of major ICT incidents or cyber threats across EU jurisdictions. Current analyses within the DORA framework highlight the need for more systematic evaluation of how resilience measures interact across EU jurisdictions and sectors, indicating that understanding their aggregate effects on market stability requires further assessment (Buttigieg & Zimmermann, 2024).

These gaps suggest that, although regulatory reforms mark a substantial step forward, continued analytical work, supervisory coordination and empirical monitoring will be necessary to evaluate the effectiveness of the evolving framework and its impact on the long-term resilience of the European payment ecosystem.

4.2.6 Quantified economic effects of secure digital payments

Although there is an ongoing conceptual debate on the economic benefits of secure digital payments, it should also be emphasized that preliminary evidence shows measurable effects on fraud reduction, transaction costs, and market efficiency. From this perspective the industry assessments indicate that enhanced authentication and real-time transaction monitoring mechanisms might reduce fraud losses by 20–40%, depending on the payment channel. ECB data shows in 2024, the payment fraud rate in the European Economic Area remained stable at 0.002% of total transaction value, but the total fraud value rose from €3.5 billion in 2023 to €4.2 billion. Strong customer authentication

procedures continue to be effective against traditional fraud types targeted under PSD2, particularly in card payments. However, emerging fraud methods, especially those involving manipulation of payers, are increasing and will require new mitigation strategies (European Banking Authority, 2025); applying stronger SCA and tokenization could therefore reduce annual losses by hundreds of millions of euros across Member States (Fritscher & Kump, 2000). From this perspective, it is expected that these measures enhance the security at the level of payment services and also further consolidate the consumer trust in using those services, which is in my opinion essential for an extended adoption of digital payment systems in Europe.

Cross-border efficiency gains are also expected under PSD3/PSR, as harmonised rules and improved interoperability reduce administrative and compliance costs for PSPs operating in multiple Member States (Junius et al., 2022).

These preliminary figures illustrate how strengthened security and harmonised regulation can translate into tangible economic benefits, supporting the broader argument that secure digital payments contribute to economic resilience and market efficiency in the EU (Yawe & Mukisa, 2020). Moreover, it is to be appreciated that the integration of efficient and adequate security measures at the level of the payment services, will consolidate the digitalisation process for payments and converge with the European Union's broader goals of enhancing market efficiency and fostering economic resilience, particularly in light of the evolving consumer preferences and technological advancements.

4.2.7 Sustainability and resilience linkage

The research identifies that secure and efficient digital payments not only reinforce economic resilience but also advance sustainability by enhancing access to financial services, supporting financial integration, and contributing to social inclusion and environmental efficiency through dematerialized payment services that reduce paper, energy, and logistical resource use (Aseeva, 2023; Sethupathy, 2025).

Table 1. PSD3/PSR/DORA measures to the economic, social and environmental impact

Regulation	Key measures	Economic impact	Social impact	Environmental impact
PSD3	Stronger SCA, liability rules, fraud refunds	Lower fraud costs; increased trust; reduced disputes	Higher consumer protection; improved inclusion	Indirect—supports digital-by-default processes
PSR	Harmonized rules, real-time transaction monitoring, open banking improvements	Lower transaction costs; cross-border efficiency	Better access to services; transparency	Reduced paper-based processes
DORA	ICT risk management, resilience testing, third-party oversight	Fewer disruptions; lower operational losses	More reliable services; continuity	Reduced need for redundant physical infrastructure

Source: Data based consolidated on the author's own research results.

5. Economic sustainability and social impact of secure digital payments

The security of retail payments continues to evolve in response to increasing digitalisation, changing consumer expectations, and expanding technological dependencies across the financial sector. Although PSD2 laid the foundation for strong customer authentication, data access rules and enhanced fraud mitigation, emerging risks linked to cyber-threats, cross-border interoperability and technological complexity demonstrate that the security landscape remains fluid and far from stable. As proposed, PSD3 and the Payment Services Regulation (PSR) aim to modernise and harmonise security requirements; however, their eventual impact on consumer protection remains uncertain, as the

proposals have yet to be negotiated, implemented and tested across diverse market environments (European Commission, 2023; Tsymbaliuk, 2024).

It seems that the increasing digitalisation of payment services simultaneously broadens inclusion opportunities but, on the other side it amplifies systemic vulnerabilities. Fintech innovation can strengthen financial participation and convenience but also introduces novel operational and cybersecurity challenges (Imaningati et al., 2024; Sahu, 2023). The growth of online payments, instant transfers and integrated financial platforms requires more sophisticated safeguards, including resilient authentication mechanisms, enhanced fraud-detection models and robust governance of third-party providers (Tarasenko et al., 2025). It seems that under current perspective under PSD2 the regulatory frameworks remain fragmented and, in some cases of traditional payment services providers, technologically outdated, leading to inconsistencies in implementation and uneven supervisory expectations across member states (European Parliament, 2023; Korus, 2024).

5.1 Enhancing the security of payment services for consumers

The ongoing transition toward secure, digital, and inclusive payment systems within the European Union carries significant but still partly uncertain implications for economic sustainability, social well-being, and environmental protection. As PSD3 and the PSR seek to reinforce the security and integrity of payment services through enhanced authentication procedures, strengthened monitoring, and more harmonized oversight, the resulting framework interacts with broader technological developments, notably artificial intelligence (AI) and FinTech innovation. Although the long-term effects of these regulatory and technological shifts remain to be fully assessed, existing research highlights the potential for meaningful transformation in how households, businesses, and institutions engage with the financial system and participate in sustainable economic development (Manta et al., 2025; Vasile & Manta, 2025).

PSD3/PSR aim to consolidate and clarify security obligations, especially by reinforcing authentication rules, improving access to account infrastructures for third-party providers and redefining liability frameworks. However, the practical consequences for fraud reduction, consumer trust and market efficiency will depend on future supervisory guidance, industry alignment and the ability of payment service providers to absorb compliance costs. Studies on open banking implementation already show uneven adoption patterns, with consumers' willingness to use data-sharing services influenced by perceived security, trust in providers and clarity of obligations (Heins & Rigopoulos, 2024; Polasik et al., 2024; Preziuso et al., 2023). The degree to which PSD3/PSR will resolve these issues remains difficult to anticipate.

Another layer of complexity is to be assessed from the sustainability point of view and also considering the ethical governance of digital payment services. As emphasised in sustainability-by-design perspectives, financial technologies must embed responsible data management, energy-efficient infrastructures and transparent accountability mechanisms from inception (Aseeva, 2023). While PSD3/PSR do not explicitly address environmental objectives, their reinforcement of governance, data-quality controls and operational standards indirectly contributes to a more responsible digital ecosystem. On the other side DORA integrates a sustainable perspective that embeds environmental factors into digital resilience, aligning with EU sustainability goals. DORA includes specific rules that require energy efficient data centers, renewable energy use, and disaster recovery plans for environmental risks for building a greener, stronger financial sector. Still, the extent to which the new framework will enhance long-term sustainability or merely increase compliance burdens remains to be assessed once implementation begins.

It is also to be taken into consideration that the integration of new payment instruments, including instant payments and the potential deployment of a digital euro, may further reshape security expectations. Instant payments, while offering convenience and competitiveness, require stronger fraud-mitigation measures and precise liability rules, which the proposed framework attempts to address, although uncertainties remain regarding market adoption and harmonised enforcement (Grabowski, 2025; European Central Bank, 2024). The potential introduction of a digital euro could amplify the demand for integrated cybersecurity strategies, privacy-preserving mechanisms and operational safeguards across centralised and decentralised architectures (Dukhnevych, 2025; European Parliament

& Council, 2023). The interaction between these initiatives and PSD3/PSR will need to be continuously monitored, as their parallel development increases regulatory complexity and testing requirements.

It seems that the developments and enhancements of the security measures through PSD3/PSR and DORA will strongly address existing vulnerabilities in the security of the payment services and payment services users' protection, complex fraud scenarios and technological governance from the third services providers. On the other hand, given the early drafting stage of the proposals (PSD3/PSR), the absence of preliminary application of DORA, and the multiple dependencies on broader regulatory initiatives under instant payment regulation and digital euro, their impact will require further assessement and remains uncertain at this stage. The effectiveness of the new framework will depend on future supervisory convergence, the capacity of providers to operationalise robust controls, and the evolving threat landscape within the EU's increasingly interconnected payment ecosystem.

The extend of digitalization process among payment services providers and the preparedness of regulatory frameworks, may show considerable variation across Member States. While, for example, the Nordic member states demonstrate an extensive integration of digital payment solutions and possess sophisticated fraud-monitoring systems, whereas certain regions in Southern and Eastern Europe encounter obstacles pertaining to digital literacy, infrastructural development, and supervisory capabilities. These disparities have implications for the pace and expense associated with the implementation of PSD3/PSR and DORA, potentially engendering transitional discrepancies in compliance obligations and market competitiveness.

5.2. DORA and payments security risks in a sustainable approach for economy

The DORA introduces a unified framework for managing ICT risks across the EU financial sector, aiming to ensure that institutions can withstand, respond to and recover from operational disruptions. As financial services become deeply embedded in complex digital supply chains and rely increasingly on external ICT providers, operational resilience has become a core element of payment-security governance. Existing literature underscores that financial stability is now closely tied to the robustness of digital infrastructures, third-party services, and cross-platform interoperability (Buttigieg & Zimmermann, 2024; Lichosik, 2023; Ni Thuama & Costigan, 2024). Nevertheless, the real impact of DORA on market practices and payments security outcomes remains uncertain, as implementation has only recently begun and firms are still adapting their governance frameworks.

DORA sets out more stringent requirements on ICT risk management, incident reporting, digital-operational resilience testing, and oversight of critical third-party service providers. From this perspective, the new obligations reflect the increasingly interconnected nature of the payment ecosystem with different other financial services and also technological developments, where different major ICT and cyber incidents or different vulnerabilities in a single component might impact and propagate across different EU jurisdictions or institutions. The growing reliance on cloud infrastructures, API-based connectivity, and AI-enabled services further intensifies these dependencies. Studies confirm that digitalisation enhances efficiency and innovation but simultaneously increases the range and scale of vulnerabilities, requiring continuous monitoring and adaptive supervisory approaches (Orăștean et al., 2024; Vashishta, 2025).

Despite its complex and integrated perspective for addressing operational resilience, it seems that DORA' effectiveness will still depend on supervisory coordination and the ability of regulated entities to implement the required recommendations and enforced measures. From this point of view, it seems that smaller fintech firms, payment institutions and emerging providers may face resource constraints when deploying advanced resilience testing, continuous monitoring systems or complex incident-reporting procedures. Earlier analyses of regulatory transitions in payment services suggest that disproportionate compliance costs can hinder smaller market participants and limit innovation uptake (Polasik et al., 2024; Korus, 2024). Whether DORA will strike the right balance between resilience and proportionality remains an open discussion.

There is also uncertainty regarding the interaction between DORA and parallel regulatory initiatives, including PSD3/PSR, the digital access to financial data through FIDA regulation, AI governance frameworks and potential developments around central bank digital currencies, such as digital euro, for example. These interconnected regimes may generate both synergies and some

redundancies or sometimes overlapped legal frameworks that should be further assessed. On the one hand, DORA's emphasis on ICT governance, testing and third-party oversight may complement PSD3/PSR's security objectives, providing a more coherent foundation for managing cross-cutting risks in payments. On the other hand, simultaneous compliance with multiple regulatory layers may increase complexity, especially when guidance and supervisory expectations differ across authorities or jurisdictions (European Commission, 2020; European Central Bank, 2024).

Academic and policy research also notes that operational-resilience frameworks must evolve alongside emerging technologies and geopolitical risks. AI based instruments may also assist the journey in threat detection and complex fraud scenario analysis, but concerns persist regarding transparency, model drift, and the risk of over reliance on automated decision-making tools. Similarly, dependence on non-EU cloud infrastructures raises strategic vulnerabilities that DORA seeks to mitigate through enhanced oversight of critical third-party providers. This objective is aligned with broader European initiatives promoting digital sovereignty and a more sustainable technological architecture (Aseeva, 2023; Dukhnevych, 2025).

Given the complexity and novelty of the framework, it remains difficult to determine whether DORA will meaningfully reduce systemic vulnerabilities or primarily increase regulatory obligations without delivering proportional benefits. The regulation represents an important step toward harmonised operational resilience, but its long-term effectiveness will only become clear once it is fully implemented, tested in real-world conditions and adjusted through supervisory practice. So, from this point of view continuous evaluation, market feedback and cross-institutional cooperation seems to add a clearer perspective on the essential role of DORA to a safer, more stable, and more sustainable financial ecosystem.

5.3 Social sustainability and financial inclusion

Fintech innovation continues to play an important role in advancing social sustainability by expanding access to essential financial services. Secure digital payments for sure will offer new entry points for individuals previously excluded from traditional banking payment infrastructures, allowing them to be further integrated from the financial point of view, make transfers, and engage in digital commerce with greater confidence (Preziuso et al., 2023; Sahu, 2023). The EU's Retail Payments Strategy, together with the evolving PSD3/PSR rules, prioritizes broad access to safe instant payments and affordable cross-border transactions, contributing to a more cohesive and inclusive digital society (European Commission, 2020; Grabowski, 2025).

Artificial intelligence might decisively impact these inclusion dynamics by enabling new forms of payment methods, remote credit assessment grounded on alternative data sources, ranging from mobile phone usage and utility payments to behavioural payment transaction patterns. Such models can provide credit access to individuals lacking conventional credit histories, potentially narrowing long-standing financial access gaps (Vasile & Manta, 2025). AI-enabled microloan automation and efficiency gains in digital payment infrastructures can further reduce service costs, making financial inclusion economically feasible for low-income groups (Manta et al., 2025). Nevertheless, the long-term perspective on the accuracy and fairness of AI based tools remains subjects of ongoing evaluation.

It seems that ensuring the security of payment services remains a central prerequisite for social sustainability and consumers' trust. The DORA institutes strict provisions for ICT risk management, incident reporting, and third-party oversight, all of which are critical for protecting vulnerable users from digital fraud and exploitation (Buttigieg & Zimmermann, 2024). AI-powered fraud detection strengthens these efforts through real-time transaction monitoring mechanisms that can identify the dynamic pattern recognition, reinforcing the integrity of payment flows and mitigating the risk of financial harm (Manta et al., 2025). These tools also reduce manual processing vulnerabilities and align with the cloud-native architectures increasingly adopted by PSPs. While the DORA perspective remains promising, their real-world effectiveness will depend on the capacity of different payment service providers and other obligated institutions to maintain efficient measures for obtaining operational resilience.

Secure digital payment can also contribute to gender equality and youth empowerment by lowering barriers to entrepreneurship, particularly where digital channels substitute for costly or

inaccessible traditional financial services (Orăștean et al., 2024). Trust in these payment services supported by PSD3/PSR security measures and AI-driven safeguards, is essential for enabling broad participation across socio-economic groups (Gounari et al., 2024; Sethupathy, 2025). However, the persistence of gaps in the adoption of digital solutions, which also stem from the uneven adoption of artificial intelligence in Europe, may limit these benefits, unless complemented by specific policies and capacity-building initiatives.

5.4 Fintech, digitalization, and financial integration

Digitalization contributes to deeper financial integration by linking consumers, merchants, banks, and non-bank PSPs through interoperable infrastructures supported by secure APIs, standardized authentication, and harmonized regulatory requirements. PSD3/PSR reinforce this integration by clarifying licensing obligations, aligning supervisory practices, and facilitating safer cross-border payments in line with the EU's ambition for a Digital Single Market (Korus, 2024; Grabowski, 2025; Tsymbaliuk, 2024).

Strategic partnerships between traditional financial institutions as banks and emerging FinTech providers further advance this process. Through modular APIs, cloud services, and AI-driven capabilities, developed by agile fintech entities, banks can adopt advanced payment innovations without full system overhauls (Manta et al., 2025). This co-evolution supports secure, scalable services and allows institutions to meet PSD3/PSR requirements more effectively, especially those concerning authentication procedures for payment service users, transaction monitoring mechanisms, and fraud detection. The result is an increasingly interconnected payment landscape that may enhance macroeconomic stability, although the degree to which such stability will materialize depends on real-world implementation quality and resilience to systemic shocks.

AI powered automation and predictive tools used for complex analytics might strengthen this resilience by enabling institutions to anticipate operational disruptions, optimize capacity allocation, and react swiftly to different threats, due to major ICT incidents and cyber-attacks. These capabilities align with DORA's expectations for continual ICT risk management and could help mitigate contagion effects across the financial system (Buttigieg & Zimmermann, 2024). However, these benefits may vary across jurisdictions and depend heavily on the maturity of technological infrastructures, fintech environment development and not the least supervisory capacity.

5.5 Payments as drivers of sustainable development

Secure and inclusive payment systems hold the potential to contribute to broader sustainable development objectives. By expanding access to affordable financial services through AI-supported alternative scoring and efficient payment channels, digital payments may help reduce inequality and foster social mobility (Preziuso et al., 2023; Sahu, 2023; Manta et al., 2025). The transparency of digital transactions, enhanced by regulatory clarity under PSD3/PSR, can support investment in green and social enterprises by improving ESG analytics and enabling more informed capital allocation (Orăștean et al., 2024; Vasile & Manta, 2025). Digital public finance mechanisms, including AI-enabled fraud detection, may also strengthen fiscal efficiency and help governments allocate resources more effectively (Dukhnevych, 2025; Manta et al., 2025). While these possibilities are well-founded by the literature, the actual extent of their impact remains uncertain and will require further ongoing evaluation.

Effective governance under the current and envisaged legal framework perspective seems essential for realizing these sustainability benefits. PSD3, PSR, and DORA provide a solid foundation for secure and resilient digital payments, but the integration of AI necessitates additional considerations such as AI model transparency, bias mitigation, and clear accountability for automated decisions (Manta et al., 2025; Vasile & Manta, 2025). Regulatory sandboxes and innovation hubs offer promising environments for testing emerging AI-FinTech models under supervised conditions, though the long-term outcomes of such initiatives remain to be validated.

Aligning FinTech innovation with ESG and inclusion goals will require continued policy attention, including clearer sustainability metrics, transparent AI scoring for green projects, and incentives for responsible digital finance. Hybrid AI models combining diverse data sources with human

oversight may help balance performance with explainability and fairness (Manta et al., 2025). Overall, while the direction of change is promising, the evidence base regarding long-term sustainability impacts remains incomplete.

6. Conclusion

This study examined how secure digital payment ecosystems in the European Union, shaped by the evolving regulatory landscape and enhanced by artificial intelligence, can contribute to economic resilience and sustainable development, while acknowledging that many of the expected impacts remain subject to uncertainty. The analysis integrated insights from PSD3, the PSR, and DORA with operational and technological developments in the FinTech sector, highlighting both the potential and the limitations of current frameworks.

6.1 Major findings

A key finding concerns the consolidation and strengthening of EU regulatory requirements governing payment services. PSD3, the PSR, and DORA collectively introduce more stringent authentication obligations, clearer rules for third-party risk management, improved reporting requirements for ICT incidents, and stronger governance expectations (Buttigieg & Zimmermann, 2024; Grabowski, 2025; Lichosik, 2023). These measures aim to further enhance payment security measures and operational resilience of payment services providers, yet their final impact will depend on the consistency and effectiveness of implementation across member states.

A second major insight includes the huge transformative potential of AI in payment services. FinTech providers are increasingly adopting operational strategies, such as tokenization, AI based tools used for fraud detection, vendor management tools, and automated decision systems, that align with the regulatory trajectory and can strengthen payment services user trust (Anwar et al., 2025; Sethupathy, 2025; Tarasenko et al., 2025; Vashishta, 2025). Predictive analytics, anomaly detection, and personalized financial services may fundamentally reshape financial intermediation (Manta et al., 2025; Vasile & Manta, 2025), though uncertainties remain regarding long-term outcomes and the governance of increasingly complex AI systems.

A third finding consists in the importance of an integrated relation between regulation, innovation, and market structure. Harmonized EU-wide rules reduce fragmentation, while innovation-friendly supervision facilitates agile development (Korus, 2024; Tsymbaliuk, 2024; Polasik et al., 2024; Preziuso et al., 2023). Strategic bank–FinTech partnerships may accelerate digital transformation, but their success will depend on proportional regulation and the ability of smaller PSPs to meet evolving compliance expectations. The resilience benefits anticipated from DORA's supply-chain requirements remain plausible but unproven.

Finally, secure and innovative payment systems appear capable of supporting sustainable development objectives by promoting financial inclusion, facilitating green finance, and reducing transaction frictions (Aseeva, 2023; Dukhnevych, 2025; Orăștean et al., 2024). These contributions, while theoretically seems to be compelling, require further empirical validation.

6.2 Policy implications

For policymakers, the analysis underscores the need for ongoing integration of AI governance into payment regulations, or at least to introduce the perspective for using efficient AI based tools, with attention to model validation, transparency, bias mitigation, and explainability (Manta et al., 2025; Vasile & Manta, 2025). Coordination between EU and national authorities remains essential to ensure consistent implementation of PSD3, the PSR, and DORA, particularly in areas relating to operational resilience and sustainability reporting (Buttigieg & Zimmermann, 2024; Grabowski, 2025). Proportionality will need to be carefully balanced to ensure smaller PSPs can meet security requirements without stifling competition (Preziuso et al., 2023). As emerging technologies evolve, technical standards should be continually updated, and innovation hubs and regulatory sandboxes should play a strategic role, both for policy learning and to support experimentation in green and inclusive digital finance. From this perspective, a mandatory and uniform approach at the EU level for launching a

regulatory sandbox and innovation hub should be taken into consideration, not only from the AI perspective but for including specific financial services under the real-life testing.

For industry stakeholders, the findings point to the importance of treating resilience and AI governance not as a compliance obligation but as strategic innovation enablers that might enhance trust and competitive performance. So, it seems that investments in secure architectures, reliable third-party providers, AI based tools used for fraudulent transaction detection, and scalable cloud infrastructures might strengthen the potential impact on secure and sustainable payment services (Manta et al., 2025; Sethupathy, 2025; Vashishta, 2025). Active engagement with innovation hubs and regulatory sandboxes may help regulators and supervisors to understand additional risks and fintech companies to manage regulatory uncertainty during the transition to PSD3/PSR. Partnerships between banks and fintech firms can also accelerate digital transformation, since agile fintech companies might become a technological driver for traditional payment service providers to adopt innovative payment solutions. Aligning product design with ESG and inclusion goals will be increasingly important as regulators and consumers place greater emphasis on responsible finance.

6.3 Limitations and future research

The study is limited by the evolving status of the PSD3 and PSR proposals, the small number of available empirical evaluations, and the emergent nature of AI integration in payments. Future research should, in my opinion, focus on quantifying the effects of the new regulatory framework on fraud rates, payment services KPIs, payment services users trust, and macro-financial stability (Buttigieg & Zimmermann, 2024; Manta et al., 2025). A complementary important factor might be represented by the comparative analyses across EU member states that could help identify best practices in regulatory implementation and AI adoption (Grabowski, 2025; Vasile & Manta, 2025). Additional work is needed to examine how emerging technologies, such as quantum computing, advanced machine learning, and blockchain interact with PSD3/PSR and DORA (Manta et al., 2025; Polasik et al., 2024). Environmental life-cycle assessments will be essential for evaluating digital payments' net ecological impact (Aseeva, 2023; Vasile & Manta, 2025). Also, the effectiveness of regulatory sandboxes and innovation hubs might depend on a uniform approach at the EU level and depends on a systematic study (Preziuso et al., 2023), as do questions of AI fairness, bias mitigation, and governance (Manta et al., 2025; Vasile & Manta, 2025).

It is also to be emphasized that future research should quantify the economic effects of PSD3/PSR and DORA on fraud reduction, transaction costs, and market structure. Comparative studies across Member States could also assess how differences in digital maturity influence the distribution of benefits. Further work is also needed to evaluate environmental impacts of digital payments, particularly regarding energy consumption of ICT infrastructures and the sustainability of cloud-based payment systems. Finally, long-term socioeconomic evaluations will be needed to assess the broader impact of AI-enabled financial services on income distribution, entrepreneurship, and sustainability outcomes.

Acknowledgement: *This article is grounded in a methodology that combines practitioner expertise with interviews conducted with industry professionals. I extend my appreciation to the Romanian FinTech community for their openness and valuable contributions, as well as to colleagues from the National Bank of Romania for their support in clarifying technical and regulatory aspects. The views expressed are solely those of the author and are offered with the aim of contributing to a deeper understanding of the subject.*

Funding*: not applicable;*

References

1. Anwar, S., Sayedahmed, N., & Pradeep, S. (2025). AI-driven risk management in online financial transactions: Enhancing cybersecurity in the fintech ERA. International Journal of Innovative Research and Scientific Studies, 8(4), 328–335. https://doi.org/10.53894/ijirss.v8i4.7784.

2. Aseeva, A. (2023). Liable and sustainable by design: A toolbox for a regulatory compliant and sustainable tech. Sustainability, 16(1), Article 228. https://doi.org/10.3390/su1601022.
3. Buttigieg, C. P., & Zimmermann, B. B. (2024). The digital operational resilience act: Challenges and some reflections on the adequacy of Europe's architecture for financial supervision. ERA Forum, 25, 143–160. https://doi.org/10.1007/s12027-024-00793-w.
4. Dukhnevych, O. (2025). Strategic and technological aspects of the digital euro: Between regulatory challenges and academic reflection. Aspekti Publìčnogo Upravlìnnâ, 13(2), 40–50. https://doi.org/10.15421/152519.
5. European Central Bank. (2024). Digital payments and financial integration in the European Union. ECB Publications.
6. European Banking Authority. (2025). 2025 Report on payment fraud (EBA/REP/2025/40). https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf.
7. European Commission. (2020). Digital finance strategy for the EU. https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.
8. European Commission. (2023). Proposal for a Directive on payment services (PSD3) and Regulation on payment services (PSR). COM(2023) 366 final.
9. European Parliament & Council of the European Union. (2023). Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro (COM (2023) 369 final). Publications Office of the European Union.
10. European Parliament. (2023). Payment Services Directive 2 (PSD2): European implementation assessment. European Parliamentary Research Service.
11. Fritscher, M., & Kump, O. (2000). Security and Productivity Improvements - Sufficient for the Success of Secure Electronic Transaction? 909–916.
12. Gounari, M., Stergiopoulos, G., Pipyros, K., & Gritzalis, D. (2024). Harmonizing open banking in the European Union: An analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. International Cybersecurity Law Review, 5, 143–178. https://doi.org/10.1365/s43439-023-00108-8.
13. Grabowski, M. (2025). The EU instant payments regulation and payment packages – interpretation and best practices. Financial Law Review, 37(1), 33–48. https://doi.org/10.4467/22996834flr.25.003.22192.
14. Heins, M., & Rigopoulos, G. (2024). An empirical exploration of key factors and barriers to consumer's adoption of open banking applications. IIARD International Journal of Economics and Business Management, 9(5), 1–12. https://doi.org/10.56201/ijebm.v9.no5.2023.pg1.12
15. Imaningati, S., Mayndarto, E. C., Huda, M., & Bakri, A. A. (2024). The role of fintech technology in improving financial inclusion and financial system stability. Nomico, 5(2), 145–159.
16. Junius, K., Devigne, L., Honkkila, J., Jonker, N., Kajdi, L., Reijerink, J., Rocco, G. L., & Rusu, C. (2022). Costs of Retail Payments – an Overview of Recent National Studies in Europe. Social Science Research Network. https://doi.org/10.2139/ssrn.4115174.
17. Korus, K. (2024). Impact of the EU regulations on the payment services. Ekonomia i Prawo, 23(4), 637–654. https://doi.org/10.12775/eip.2024.32.
18. Lichosik, A. (2023). DORA jako prawny instrument ochrony cyfrowego bezpieczeństwa rynku finansowego [DORA as a legal instrument for protecting the digital security of the financial market]. Studia Prawnoustrojowe, 62, 217–231. https://doi.org/10.31648/sp.9581.
19. Manta, O., Vasile, V., & Rusu, E. (2025). Banking Transformation Through FinTech and the Integration of Artificial Intelligence in Payments. *FinTech*, *4*(2), 13. https://doi.org/10.3390/fintech4020013.

20. Negrea, C. I., Scarlat, E. M., Horățău, I., & Manta, O. (2025). Governing financial innovation through institutional learning: Lessons from Romania's fintech innovation hub. *FinTech*, *4*(4), Article 67. https://doi.org/10.3390/fintech4040067.
21. Ni Thuama, R., & Costigan, S. S. (2024). DORA - Understanding the new regulatory framework on digital operational resilience. Social Science Research Network. https://doi.org/10.2139/ssrn.4549564.
22. Orăștean, R., Mărginean, S., & Cristian, M. G. (2024). Fintech evolution in the European Union: Trends, drivers and challenges. Revista Economică, 76(2), 82–90. https://doi.org/10.56043/reveco-2024-0018.
23. Polasik, M., Butor-Keler, A., Widawski, P., & Keler, G. (2024). Evaluating the regulatory approach to open banking in Europe: An empirical study. Financial Law Review, 34(2), 59–90. https://doi.org/10.4467/22996834flr.24.007.20612.
24. Preziuso, M., Koefer, F., & Ehrenhard, M. L. (2023). Open banking and inclusive finance in the European Union: Perspectives from the Dutch stakeholder ecosystem. Financial Innovation, 9, Article 1. https://doi.org/10.1186/s40854-023-00522-1.
25. Pulatov, T. (2025). Concepts of digital financial technologies and their legal nature. International Journal of Law and Policy, 3(1), 15–28. https://doi.org/10.59022/ijlp.260.
26. Sahu, J. K. (2023). The development of digital payment solutions: Impact on financial inclusion and approaches to risk management. National Journal of Arts, Commerce & Scientific Research Review, 10(2), 12–24. https://doi.org/10.52458/23944870.2023.v10.iss2.kp.a2.
27. Sethupathy, U. K. A. (2025). Evolving frameworks in digital payment security: Technological innovations, economic impact, and consumer trust dynamics. International Journal of Computational and Experimental Science and Engineering, 11(1), 1–12. https://doi.org/10.22399/ijcesen.3893.
28. Tarasenko, A., Zhavoronok, A., & Suhovetskyy, V. (2025). Payment security in the digital economy: Challenges for the banking card business. Naukovij Vìsnik Polìssâ, 1(30), 233–247. https://doi.org/10.25140/2410-9576-2025-1(30)-233-247.
29. Tsymbaliuk, K. (2024). Porivnialno-pravovyi analiz PSD2 ta proiekta novoi platizhnoi dyrektyvy PSD3 i rehlamentiv [Comparative legal analysis of PSD2 and the draft new payment directive PSD3 and regulations]. De Iure, 1, 15–28. https://doi.org/10.36074/deiure.issue1.002
30. Vashishta, R. S. (2025). Securing fintech in a connected economy. In: Advances in Fintech Security (pp. 45–68). https://doi.org/10.48001/978-81-980647-2-1-3.
31. Vasile, V., & Manta, O. (2025). FinTech and AI as Opportunities for a Sustainable Economy. *FinTech*, *4*(2), 10. https://doi.org/10.3390/fintech4020010.
32. Yawe, B. L., & Mukisa, I. (2020). The impact of the Revised Payment Services Directive on the market for payment initiation services. https://doi.org/10.69554/leve5702.
33. Zunzunegui, F. (2018). La digitalización de los servicios de pago (Open Banking) [The digitalization of payment services (Open Banking)]. Social Science Research Network. https://doi.org/10.2139/SSRN.3264759.

© 2026 The Institute of National Economy - Romanian Academy. All Rights Reserved.
Disclaimer: The views expressed in this document are solely those of the author.