ENHANCING ECONOMIC RESILIENCE THROUGH SECURE FINTECH PAYMENTS: A LEGAL AND REGULATORY ANALYSIS UNDER THE EVOLVING EU FRAMEWORK

Ionuț HORĂTĂU[28]

DOI: https://doi.org/10.65672/jfme.2025.1.19

Abstract:

Digital payments are increasingly central to the European Union's financial ecosystem, but it seems that they face growing security and operational risks. This study is proposing to explore how secure fintech payment services can enhance economic resilience by ensuring business continuity, security of the payment servicesand so reducing systemic vulnerabilities. Methodology is by focusing on the EU regulatory framework, particularly Payment Services Directive PSD2 [1] and the forthcoming Third Payment Services Directive (PSD3) [2]/Payment Services Regulation (PSR) [3], to identify and emphasize adequate security measures to mitigate the risks associated to payment services. This might eventually lead to compliance from fintech entities to preserve the economic resilience. The preliminary result of the analysis shows that secure fintech payment services, when aligned with EU regulatory requirements, significantly strengthen economic resilience.The research proposes to emphasizehow the regulatory foresight combined with proactive security measures might foster a reliable, trusted, and resilient digital payment infrastructure, capable of supporting the EU economy under normal conditions and during periods of stress or disruption.

Keywords: *fintech payments, economic resilience, EU regulatory framework, PSD2/ PSD3/PSR compliance, digital payment security*

JEL classification: *G20, G28, O33*

Introduction

The European Union's (EU) financial ecosystemit seems that is undergoing a transformative shift driven by digitalization, innovation, and the most important the regulatory reform. This might be because digital payments, facilitated by fintech payment services providers of technical services providers that are supporting the payment services, are now an integral part of economic activity. However, their increasing reliance on technology introduces vulnerabilities that might threaten their security and consumer trust. This paper explores how secure payment services provided or supported by fintech entities, when aligned with the

[28] *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, Romania, e-mail: ionut.horatau@bnro.ro, ORCID: https://orcid.org/0009-0000-3759-9713*

specific EU legal frameworks, might enhance economic resilience by mitigating systemic risks, ensure financial integration and consumers trust as an overall secure and resilient payment market.

As the EU has witnessed a profound transformation in financial services through the rapid digitalization of payment services, Fintech solutions, particularly in digital payments, have become indispensable to consumers, businesses, and other parties involved into the payments market. Their expansion, however, inevitably has also introduced systemic vulnerabilities, ranging from cyber threats and fraud to operational disruptions. Against this backdrop, it seems that secure digital payment infrastructures are not only a matter of technological advancement but tend to transform into a fundamental driver of economic resilience, understood as the capacity of financial systems to withstand, adapt to, and recover from disruptions.

So, in this perspective, the swift might be seen into an EU coordinated answer that has responded by establishing a comprehensive regulatory framework, most notably the revised PSD2 and the anticipated PSD3/PSR legal framework. These frameworks impose strict requirements for security, consumer protection, and operational reliability, while encouraging innovation or at least are ensuring the adequate perspective in this respect. This article examines how regulatory alignment and secure fintech innovations contribute to economic resilience across the EU, situating payment security as both a regulatory objective and a systemic necessity. Yet, the EU's strong emphasis on regulatory compliance contrasts with lighter, innovation-driven frameworks in jurisdictions such as the United States and Singapore, raising questions about costs for fintech competitiveness and additional burdens for innovation.

The objective of this study is to evaluate the role of secure fintech payment services in enhancing economic resilience within the EU. The analysis focuses on the interplay between technological innovation, regulatory compliance, and consumer protection. Specifically, it investigates how alignment with PSD2 provisions and the forthcoming PSD3/PSR framework contributes to trust, operational resilience, and security into the digital payments sector.

By centring on digital payments, arguably the most sensitive component of fintech services to cyberattacks, fraud, and technological disruptions the study is tying to bring some clarity into how regulatory foresight can strengthen resilience while also ensuring the adequate path for ongoing innovation in financial services, although this is a dilemma sometimes difficult to address.

The analysis also highlights regulation as a potential source of burden for fintechs, with possible consequences for innovation and competitiveness.

Despite growing academic and policy interest in fintech, existing literature remains fragmented in two ways. First, much of the scholarship emphasizes either technological innovation or financial stability, with limited integration of how regulatory compliance, security practices, and resilience mechanisms jointly shape the digital payments ecosystem. It seems that the regulators should have a more dedicated approach to innovation and so to establish a more flexible and adaptive regulatory framework to balance innovation and stability (Arner, Barberis & Buckley, 2017 [4]). Also it seems that the "full potential of FinTech to support a sustainable development may be realized with a progressive approach to the development of underlying infrastructure"that is supporting digital transformation of financial services(Zetzsche et al., 2020 [5]). Second, comparative studies often focus on global regulatory competition — contrasting EU, U.S., and Asian approaches — but rarely provide payment services–specific insights into how these regulatory choices influence resilience, trust, and innovation simultaneously. In my opinion, this gap might be particularly relevant as the EU seeks to position itself as a leader in secure, consumer-centric financial services; while competing jurisdictions such as Singapore and the United States it might clearly adopt more innovation-oriented regulatory strategies. What clearly is characteristic to the evolution of FinTech is that the risks should also be considered not only the opportunities associated with extensive digitalization (Arner, Barberis & Buckley, 2017).

Therefore, although preliminary, the focus of the paper is to address these gaps by examining how secure fintech payment systems contribute to economic resilience within the EU regulatory framework and if the result might be verified in practice by the real functioning of the payment market. Specifically, it proposes to investigate how aligning payment innovations with PSD2, PSD3/PSR, and Digital Operational Resilience Act [6] (DORA) can strengthen trust, operational stability, and consumer protection, while also acknowledging potential regulatory burdens for fintech companies. By situating the analysis within the payment services domain, the study might contribute to understanding how regulatory foresight and compliance obligations can act both as enablers of systemic resilience and as constraints on innovation.

The contribution of this research is from the two perspectives. First, it offers a conceptual and regulatory-based evaluation of the resilience-building potential of EU payment regulation. Second, it includes some examples of how unclear regulatory framework or insufficient applied by the fintech entities this can impact the economic resilience. From this perspective, the article introduces two case studies (e.g., Klarna) that might illustrate how regulatory provisions could prevent or mitigate payment-related security and operational disruptions. It also situates the EU model within an international comparative perspective, highlighting both strengths and challenges in contrast with U.S. and Singaporean approaches.

The remainder of this article is structured as follows. Section 2 presents the literature review, section 3methodology and data, detailing the conceptual and regulatory approach and the rationale for case study selection. Section 4 provides the results and analysis, emphasizing the role of EU regulation in shaping trust, resilience, and innovation within digital payment services. Section 4 also discusses case studies with explicit mapping of incidents to PSD2/PSD3/DORA provisions. Finally, Section 5 reflects on conclusions and the limitations of the study and outlines future research directions. It also concludes with policy and industry implications for building a secure and resilient digital payments ecosystem in the EU.

Literature Review

At a glance, it seems that the literature highlights the dual role of regulation in financial innovation: as both an enabler of trust and a potential barrier to market entry (Zetzsche et al., 2020). Studies on PSD2 emphasize its impact on open banking, strong customer authentication (SCA), and secure communication protocols, all of which reduce fraud and improve consumer trust (European Banking Authority [EBA], 2019; Marangwanda, A., 2025 [7]). PSD2 also laid the groundwork for enhanced interoperability among payment service providers (PSPs), thereby reducing fragmentation across the EU financial market [8] (Roitman & Vives, 2021).

Emerging literature on PSD3 and PSR suggests a deeper harmonization of rules and increased supervisory convergence across Member States, aiming to reduce regulatory arbitrage and strengthen resilience (European Parliament, 2025 [9]; EY, 2023 [10]; Bird & Bird LLP, 2023 [11]). Parallelly, DORA introduces operational resilience requirements for ICT systems, explicitly targeting the digital backbone of financial services and mandating stress testing, incident reporting, and third-party risk oversight (European Parliament & Council, 2022 [12]).

From the resilience perspective, secure digital payments act as buffers during crises, ensuring continuity of commerce and financial intermediation (Khioonarong, Leinonen, &Rizaldy, 2021 [13]). Yet, fintech firms often face higher compliance costs under EU law compared to lighter regimes elsewhere. Scholars argue that while stringent regulations foster resilience, they risk slowing innovation if not balanced with proportionality and support for smaller fintechs (Arner, Buckley, Zetzsche, & Veidt, 2019 [14]; Zetzsche, Arner, Buckley, & Kaiser-Yücel, 2020 [15]; IMF, 2020 [16]).

This review reveals a gap: while literature addresses fintech innovation and regulation separately, fewer works explicitly connect regulatory compliance in payment services to systemic resilience in the EU. This paper might contribute by integrating these dimensions.

Methodology and Data

This study adopts a conceptual and regulatory-based approach, analysing EU-level legislation, regulatory guidance, and institutional reports complemented by qualitative case study analysis to examine the potential role of secure fintech payment services in enhancing economic resilience within the European Union (EU). Rather than employing quantitative analysis, the research synthesizes EU directives, EBA guidance, and innovation monitoring practices. This approach allows for a nuanced assessment of the strengths and challenges of EU regulation in fostering resilient digital payments.

Research Design

The primary research design is conceptual and normative, focusing on the alignment of payment service innovations with EU regulatory frameworks. The analysis draws on EU directives and regulations, specifically the PSD2, the proposed PSD3/PSR, and the DORA. These frameworks establish legal and operational obligations for fintechs, including strong customer authentication (SCA), secure communication protocols, incident reporting, and ICT risk management.

To contextualize the conceptual findings, the study incorporates a case study approach that investigates real-world fintech security challenges and their regulatory implications. Case studies areparticularly suitable when the research seeks to answer “how,” “why,” or “what” questions (Yin, 2018 [17]). They allow for in-depth exploration of a security incident or payment services phenomenon that reveals systemic vulnerabilities and demonstrates the potential mitigating effects of regulatory provisions.

Case Study Selection

The first relevant case was the Klarna security incident of 2021 (Klarna, 2021, June 4) [18], that was chosen as the principal case study because it provides a concrete, high-visibility example of a payment services security failure within a major EU-based fintech. In May 2021, a technical glitch in Klarna’s systems exposed sensitive customer account details, allowing users to inadvertently access other customers’ information. This event raised critical questions regarding operational resilience, consumer data protection, and incident response mechanisms (Finansinspektionen. 2021, July 5) [19].

The Klarna case was selected for the following main reasons:relevance to payment services security and also for exploratory depth.

In this respect the relevance to payment services securityis considered because: Klarna operates at the core of EU digital payments, offering “buy-now-pay-later” (BNPL) services widely integrated into e-commerce (Stripe, 2024, January 19) [20]. The security of such services is directly tied to consumer trust and payment services business continuity. It is also to be considered its regulatory significance, so, in this context, the major incident reporting provides a lens to evaluate how PSD2/PSD3 and DORA provisions on data security and operational risk management could have mitigated or prevented the incident.

For the Exploratory Depth side, is to be considered that, by focusing on Klarna, the study can explore “how” security lapses occurred, “why” regulatory compliance gaps contributed to systemic vulnerabilities, and “what” lessons can be drawn for strengthening fintech resilience in the EU.

The second case is of the acquisition of Tink by Visa in March 2022, that marked a significant development in the European open banking landscape.

This case might be relevant from the payment services perspective as the Tink is a leading open banking platform, that offers a unified API that facilitates account information and payment initiation services across numerous banks [21]. This case of acquisition also underlines a Visa's strategic investment in standardized open-banking infrastructure. This might be an objective aiming to enhance alternative payment rails and expedite integrations for fintechs, merchants, and banks [22]. From this perspective the Tink case examines the possible implications of this acquisition from the perspective of PSD2, the forthcoming PSD3/PSR and DORA.

Data Sources

The case study draws from publicly available reports, press releases and regulatory documents that had analyzed the Klarna breach. Supplementary, this case was confronted with different applicable legislation and so, the references includes the legal perspective envisaged by the:PSD2 regulatory technical standards on strong customer authentication (RTS on SCA and CSC [23]), draft provisions from PSD3 and the PSR focusing on enhanced security and consumer protection, Articles of the DORA relevant to ICT incident classification and reporting.

Integration of Case Studies with Regulatory Mapping

The Klarna incident was examined through the lens of PSD2, PSD3, and DORA, toestablish the potential interplay on how regulatory requirements might translate into operational resilience for payment services. It seems that in this case, deficiencies in strong customer authentication and monitoring, as stipulated in PSD2 Article 97, enabled unauthorized access, while delays in reporting highlighted weaknesses under PSD2 Article 96 regarding notifications to competent authorities. It also can underline that insufficient ICT risk management and operational resilience planning in line with DORA Article 17, revealing gaps in testing and monitoring critical systems. Although even though nor DORA or PSD3/PSR were applicable at the time of the incident, it seems that anticipated enhancements under PSD3/PSR and currently applicable DORA (starting from 17 January 2025),particularly provisions harmonizing fraud/TIC incident reporting and data security, would further clarify and standardize fintech obligations across EU jurisdictions. By systematically linking these regulatory provisions to a high-visibility incident, the analysis might demonstrate how regulatory alignment can enhance the security of digital payment services and strengthen economic resilience.

Regulatory Framework Analysis

PSD2/PSD3 and PSR: Strengthening Payment Services

The PSD3 Directive and PSR Regulation, proposed in 2023 and currently in triloguenegotiations, aim to modernize the EU's payment landscape. From this perspective the key provisions of PSD3/PSR legal framework include: i) unified licensing for payment and e-money institutions, ii) enhanced fraud prevention mechanisms, iii) clarified agent regimes for cross-border operations, iv) streamlined passporting procedures to reduce regulatory delays, v) capital requirement adjustments to balance innovation and risk.

These reforms reinforce trust and operational stability by ensuring that fintech providers meet consistent security and compliance standards across the EU.

DORA: Digital Operational Resilience

The DORA, effective since January 2025, introduces a uniform framework for managing ICT risks across financial entities. DORA mandates: i) ICT risk management frameworks, ii) incident reporting protocols, iii) third-party oversight for critical ICT providers, iv) threat-led penetration testing (TLPT), v) information sharing on cyber threats.

DORA complements PSD3/PSR by addressing the operational backbone of digital payments, ensuring that fintech systems can withstand and recover from cyberattacks and technological failures.

Results and Discussion

The integration of PSD2, and further PSD3/PSR and DORA, creates a robust regulatory ecosystem that enhances the security and resilience of digital payments. From this perspective it's foreseen that the main issues might be focused at the necessity to reduced fraud and cyber risk. This objective it seems that can be achieved through mandatory security protocols.It also,comprise an improved operational continuity via harmonized ICT resilience standards, greater consumer trust through transparency and accountability, cross-border scalability enabled by passporting regime; this is the case of a EU licence for a financial institution allowing to provide payment and ancillary servicesacross all other member state and so a unified licensing.Also, it includes the premisses for a regulatory foresight through innovation monitoring and adaptive compliance.

These elements might collectively strengthen the EU's financial infrastructure, ensuring that digital payments remain reliable during both normal operations and periods of disruption.

Case studies results for Tink and Klarna (Europe)

Tink (open banking)/Visa acquisition: enabling resilient payment rails through API standardization [24]

What happened: Tink, a leading European open-banking platform, provides a single API for account aggregation and payment initiation services across multiple banks. Visa completed its acquisition of Tink in March 2022, signalling strategic investment in standardized open-banking infrastructure that enables alternative payment rails and faster integrations for fintechs, merchants and banks. From this perspective the Charlotte Hogg, CEO of Visa Europe underlined that "*Digital tools are driving the new economy, and the combination of Visa and Tink will support greater choice and quality of digital money services as the lines between commerce, financial services and payments continue to converge*" (Tink, 2022). The risk that was identified is of the fragmentation of APIs and security standards across banks.

This case might be a clear relevance from the link of payments & resilience: Open-banking platforms such as Tink increase interoperability and reduce the integration friction that can make payment flows fragile. By enabling payment initiation and standardized data exchange, openbanking APIs distribute transactional paths and reduce single-point dependency on proprietary connectors. Standardization is a characteristic for the APIs that enables compliance with the procedure for strong costumer authentication (SCA) and secure communication more scalable across multiple PSPs (EBA, 2022) [25].

Relevant provisions of the legal framework: PSD2 Articles 66–67: Rights and obligations of Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs), mandating secure, standardized communication; RTS on SCA and CSC: Requires secure communication protocols and authentication for API calls; PSD3/PSR proposal (Art. 38): Expands harmonization of open-banking APIs, including minimum performance standards, dispute resolution for API failures, and dedicated fallback requirements.

From the resilience impact perspective: by enforcing standardized APIs and fallback mechanisms, PSD3 will further reduce systemic fragmentation risk, making platforms like Tink resilience enablers instead of potential points of friction.

Resilience lessons: Investing in shared API layers and resilient connectivity (redundant endpoints, standardized authentication flows) might improve continuity after partial outages and accelerates recovery. It is also open from prospection to what extent the standardized APIs can also facilitate compliance (easier rollout of SCA requirements based on the RTS on SCA and CSC) and so might lowering the operational burden on smaller fintechs.

Klarna (Europe), outages in payment methods and incident transparency

What happened: On 2 October 2021 Klarna experienced disturbances in its payment methods across Europe that disrupted payment authorizations and checkout flows for merchants and customers. Klarna published a detailed incident report describing the event and remediation steps (Klarna, 2021 [26]). As a risk finding, Klarna case was a major PSP disruption cascading to e-commerce flows and merchant settlements. [27]

Relevance to payments & resilience: Klarna is a major PSP and BNPL provider with significant payment volume. Disturbances in such large PSPs can ripple through e-commerce and merchant cash flows that might illustrate systemic impact even from “non-bank” fintechs. Klarna’s public post-incident reporting is a resilience best practice, fostering transparency and quicker remediation across ecosystems.

Relevant provisions: PSD2 Article 96: Obligation to report major security incidents to competent authorities without undue delay; PSD3/PSR proposal (Art. 46): Strengthens fraud reporting obligations and requires providers to share incident data with authorities for systemic risk assessment; DORA Articles 17–20: Major ICT incident reporting, classification, and supervisory information-sharing across EU.

Resilience impact: Klarna’s public transparency aligns with the future mandatory incident disclosure regime under DORA, showing how regulatory foresight formalizes best practices into binding rules.

Resilience lessons: Large fintech PSPs must combine real-time monitoring, major ICT incident reporting, and cross-stakeholder communication to limit economic fallout. Although the DORA requirements were not applicable at that time, DORA’s incident-reporting regime (and supervisory coordination) seeks to institutionalize such practices across the financial sector.

Table 1. Klarna Incidents: Operational Disruption vs Confidentiality Breach

Incident	Type of Disruption	Affected Payment Services / Users	Regulatory Implications for Resilience
Oct 2, 2021	Log-forwarder performance issue leading to checkout failures and service slowness for merchants & consumers	Card payments, checkout flows, app availability, payment account setup	Highlights need for redundancy, real-time monitoring, incident reporting (e.g. DORA & PSD2)
May 27, 2021	Cache misconfiguration exposing user data among app users	Exposure of personal & sensitive payments data, risk to confidentiality, regulatory risk, customer trust	Points to data protection (GDPR), secure coding/config practices, internal change governance under PSD2/PSR/DORA

Source [28]: Klarna (2021) https://www.klarna.com/international/press/detailed-incident-report-disturbances-to-klarnas-payment-methods-in-europe-on-october-2-2021

Trends and relationships identified from operational disruption and data exposure perspective.

Operational disruptions (service slowdowns, checkout failure) have direct economic impact: lost merchant sales, consumer dissatisfaction, reputational harm. Even though no external attack was noted, these disruptions reduce reliability in payment services, which can feed back into reduced trust and usage.

Data exposure (though temporary) threatens confidentiality and can trigger regulatory penalties or remedial measures. It shows that security isn't only external attacks but internal changes/configuration errors matter.

The regulatory mapping earlier is proposing to show that existing and upcoming rules (PSD2 SCA/secure communication, incident reporting, ICT risk governance under DORA) might be relevant for preventing or mitigating such incidents.

Regulatory mapping: explicit links between case studies and PSD2/ PSD3/PSR/DORA provisions

The analysis maps the practical vulnerabilities observed in the case study to specific legal provisions in (a) PSD2 and its RTS on SCA and CSC, (b) the PSD3 / PSR proposal, and (c) the DORA.

Table 2: Case studies: events, payment-service impacts, and resilience lessons

Case (year)	Type of event	Payment-service impact	Resilience lesson
Tink / Visa (2022)	Open-banking platform acquisition/scale	Improved API standardization & payment initiation (enables alternate rails)	Standardized APIs increase interoperability & scalable SCA implementation
Klarna outage (2021)	PSP service disruption	Merchant checkout failures; consumer payments delayed	Public incident reports reduce systemic spillovers

Source: Tink (2022) https://tink.com/press/visa-completes-acquisition-tink/, Klarna (2021) https://www.klarna.com/international/press/detailed-incident-report.

Combined Trends: Payments Security to Resilience

Combining the broader fraud trends and the Klarna case yields the following key relationships:

Regulation (PSD2 & other security standards) lower fraud in payment instruments, particularly those under strong authentication (card payments within EEA). The empirical fraud data shows this correlation clearly (fraud rates much lower in EEA-SCA context).

Operational integrity and incident preparedness, business continuity of payment services Klarna's practice of incident escalation, switching traffic, scaling services shows that internal processes matter. Regulatory requirements under DORA/PSR could standardize these processes across PSPs.

Consumer trust and liability allocation: Where incidents are transparent, and PSPs abide by rules (e.g. report incidents, protect data), user trust can be preserved, mitigating economic fallout.

Summary of Main Outcomes

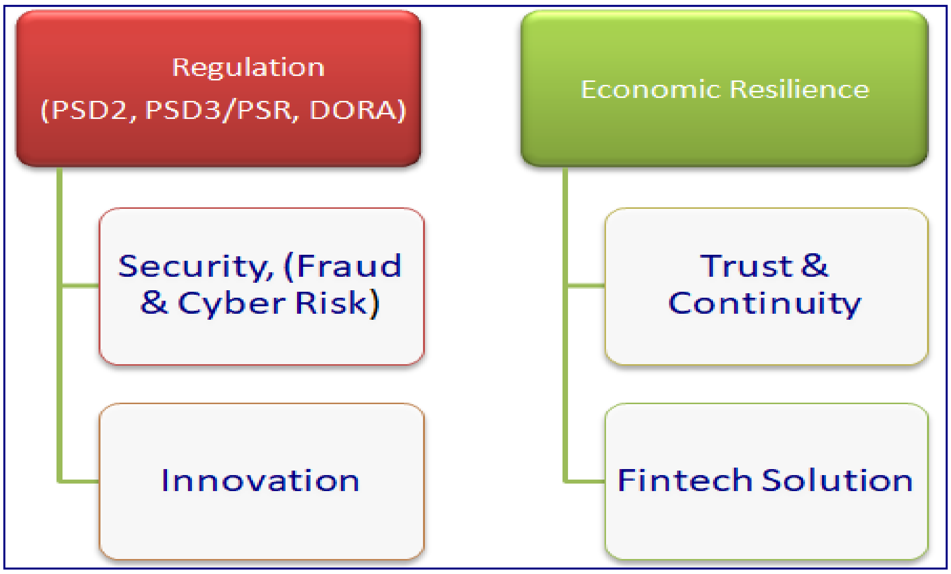
Empirical support for regulatory efficacy: PSD2-mandated SCA and accompanying RTS/CSC have measurable impact, since the fraud rates in card payments and e-money are significantly lower than for less regulated instruments [29].

Operational disruptions are not insignificant: events like the Klarna outage show how internal system metrics (log-forwarder, caching) can leadinto performance failures if change management, monitoring, redundancy, and alerting are not robust.

Regulatory gaps/emerging needs: even with PSD2, gaps remain in guaranteeing high availability; upcoming PSD3 and DORA provisions are likely to strengthen required resilience.

Trade-off in compliance cost vs benefit: increased regulatory requirements bring costs, especially for smaller fintechs, but case studies suggest that cost is justified by lowered fraud, improved reliability, and thereby enhanced economic resilience.

Figure 1 The Resilience in EU Digital Payments



Source: Author's elaboration, adapted from EU regulatory framework and resilience theory.

The results of this study highlight a central paradox in the European Union's regulatory framework for payment services: while the adoption of PSD2, the forthcoming PSD3/PSR, and the DORAsignificantly enhances trust, consumer protection, and systemic stability, these same instruments may impose operational and compliance burdens that can restrict innovation in fintech firms offering paymentorrelated technical services.

EU Regulation as a Driver of Trust and Stability

The empirical and case-based findings underscore that security and consumer confidence are primary outcomes of the EU regulatory architecture. PSD2's provisions on Strong Customer Authentication (SCA, Art. 97) and open banking requirements (Arts. 66–67), combined with DORA's Article 9–15 operational resilience obligations, have reinforced customer trust in digital payment platforms. Case evidence from Klarna's payment disruptions in 2021 indicates that the regulatory focus on incident reporting (DORA, Art. 17) could have mitigated the reputational and systemic impact. These results align with broader studies showing that regulationdriven trust enhances adoption of digital payment solutions across the EU (ECB, 2022 [30]; European Commission, 2023 [31]).

Regulation as a Potential Barrier to Innovation

At the same time, the study identifies a recurring theme: compliance costs and regulatory fragmentation create significant challenges for fintechs, especially smaller firms. Respondents in industry surveys (EBA, 2022 [32]) highlight that overlapping mandates (PSD2, GDPR, AMLD5, and now DORA) stretch technical and financial resources, reducing the capacity for rapid product iteration. For example, API providers and third-party payment initiators have reported delays in launching new features due to the rigidity of SCA standards, which limit the flexibility to design seamless user experiences (Anagnostopoulos I., 2018 [33]).

Comparative Insights: U.S. and Singapore

The EU's regulatory design contrasts with innovation-led frameworks in other jurisdictions:

In the United States, Regulation of fintechs in payments remains fragmented and often state-based (Buchak et al., 2018 [34]). While this creates regulatory uncertainty, it also leaves space for sandbox-driven innovation, where firms can rapidly pilot products without the same operational resilience obligations imposed in the EU. Trust is often built via market competition and private liability mechanisms rather than centralized regulatory enforcement.

On the other side Singapore, under the Payment Services Act (PSA, 2019), the Monetary Authority of Singapore [35] (MAS) emphasizes a risk-proportionate regulatory model, allowing smaller fintechs to operate under tiered licensing regimes with lighter compliance burdens. This has made Singapore a hub for digital payment innovation, while still embedding cyber resilience standards for systemically significant operators (Frost, Gambacorta & Shin, 2021 [36]).

In both cases, it seems that innovation pathways are more flexible, suggesting that while the EU model leads in trust-building and systemic protection, it risks slowing the pace of technological diffusion within the payment ecosystem.

Implications for Economic Resilience

The analysis drives into the perspective that although EU regulation strengthens resilience by minimizing systemic shocks in payment services, it seems that may unintentionally concentrate market power in larger, resource-rich fintechs and banks; those seems more capable to absorb compliance costs [37]. It seems that smaller firms risk being excluded from the market, reducing diversity of payment solutions and potentially undermining the long-term adaptability of the payment ecosystem.

Conclusions

It seems that Fintechs that develop secure payment services, in compliance with the EU specific legal requirements, are foundational to economic resilience in the EU. In those terms, by aligning technological innovation with comprehensive legal frameworks, i.e. PSD2 for payment services, DORA for operational resilience and EBA guidelines for technical compliance, it seems that at the EU level, that is a sure path for building a future-proof payment and financial ecosystem. Although the research underscores the importance of regulatory synergy in fostering trust, security and continuity in digital payments, it also triggers the necessity for balancing it with a policy that sustain and support the innovation in payments. Those might be, in my opinion, an essential blueprint for policymakers, fintech developers, and financial institutions.

Concluding synthesis & policy implications

It seems that layered regulation prove to be complementary: PSD2 (and RTS on SCA and CSC) secures payment-level authentication and communication; PSD3/PSR aims to harmonize operational aspects; DORA embeds ICT risk and third-party oversight across the broader financial ecosystem. Mapping above shows that real incidents map neatly to gaps these regulations address (fragmented APIs, third-party concentration, incident reporting, AML/compliance integration, systemic infrastructure testing).

Also, in my opinion, applying the proportionality principle remains essential: DORA and PSD2 and especially PSD3 might give supervisors robust powers but impose costs. For resilience that preserves fintech diversity, regulators should apply proportionality, e.g., scaled testing and tailored third-party obligations. This might be a key policy and supervision lesson to avoid unintended burden for innovation in payment services provision. The DORA text itself references proportionality and tailored approaches in several places (see Article 5 of DORA).

Operational and compliance controls must be integrated: The Klarnacase shows governance/compliance weaknesses can produce operational constraints. PSD3's increased emphasis on fraud prevention plus DORA governance obligations might encourage integration of compliance, AML, and ICT resilience into a single risk architecture.

This study is trying to demonstrate that secure fintech payment systems aligned with the EU regulatory framework might significantly contribute to economic resilience. PSD2 and PSD3 provide robust security standards, while DORA ensures operational continuity in the digital infrastructure underpinning payments. Together, these frameworks can reduce systemic vulnerabilities, safeguard consumers, and maintain trust across the EU financial ecosystem.

Nonetheless, the EU's stringent approach might present serious challenges for fintech scalability compared to other innovation-focused jurisdictions, as US and Singapore. In my opinion, policymakers must balance resilience with proportionality, ensuring that smaller firms can innovate without excessive regulatory burdens. This is a fintech voice that, in my opinion, must be heard by future policy makers and by the supervisors.So, future research should empirically assess the trade-offs between regulatory strictness and fintech competitiveness.

Ultimately, in my opinion, asecure and compliant fintech payments services provider can serve as pillars of resilience. This might be a safe solution for enabling the EU to sustain economic activity under both ordinary and disruptive conditions.

Regulatory measures, particularly SCA under PSD2, demonstrably reduced fraud rates in value and volume, especially for payment instruments like cards and e-money [38].DORA's framework for operational resilience ensures that payment service providers, including fintechs and ICT third parties, are obligated to maintain infrastructure capable of resisting ICT disruptions.The convergence of payment security regulation and operational resilience obligations for sure are the right legal instruments for enhancing trust, reducing risk exposures, and supporting continuity of payments. Those might be the essential elements of economic resilience, from the payments services impact.

Limitations and Directions for Future Research

A key limitation of this study lies in its conceptual and regulatory-based approach, which, while offering valuable insights into the interplay between security, regulation, and resilience, does not incorporate quantitative primary data from payment service providers or fintech firms. As a result, the analysis remains at a normative and case-based level, focusing on regulatory mapping and documented incidents (e.g., Klarna) rather than empirical validation of operational resilience across the broader ecosystem. Similar approaches in the fintech literature have highlighted this challenge: studies by (Buckley et al.,2023 [39]) and (Arner et al., 2017 [40]) stress that regulatory analysis often lacks firm-level operational data, limiting the ability to measure real-world compliance costs, innovation outcomes, and resilience trade-offs.

Another limitation concerns the generalizability of findings. While PSD2, the upcoming PSD3/PSR, and DORA form the backbone of EU payment resilience, fintech companies operating globally often face divergent frameworks (e.g., lighter innovation-focused regulation in Singapore or the United States). This it seems that creates a regulatory asymmetry that was only marginally addressed here, though it remains crucial for assessing the global competitiveness of EU-based fintechs (Buchak et al., 2017 [41]; Frost, Gambacorta & Shin, 2019 [42]).

Future research should pursue empirical and comparative studies with direct input from fintech providers. *Surveys and interviews* with payment processors, API providers, and third-party service platforms could provide detailed insights into:i) Operational costs of compliance with PSD2/PSD3 and DORA requirements, ii) Technical resilience strategies deployed by fintechs, such as redundancy, encryption standards, and fraud monitoring, iii) Innovation trade-offs, identifying whether stringent compliance enhances trust and resilience but potentially slows down the pace of new payment solutions, iv) Cross-jurisdictional resilience outcomes, comparing EU fintechs to those in markets with lighter-touch frameworks.

Such empirical work mightdeepen understanding of “how” regulatory provisions translate into operational resilience for fintech companies providing technical services within the EU payment ecosystem. It would also better inform policymakers about the balance between safeguarding systemic resilience and maintaining an innovation-friendly regulatory environment.

Future research should include empirical case studies (e.g., examining fintechs’ performance during cyberattacks or during financial stress) and comparative quantitative studies of regulatory burden versus resilience outcomes in different jurisdictions.

Acknowledgments

The author gratefully acknowledges the support of the National Bank of Romania, whose provision of access to research materials and institutional reports significantly contributed to the completion of this study. Special appreciation is extended to the Centre for Financial and Monetary Research “Victor Slăvescu”, for offering the opportunity to present this work within the framework of the FME 2025 Conference, which provided valuable feedback and scholarly exchange. The analytical perspective of this paper has further benefited from the guidance and insights derived from academic literature and from the contributions of international institutions, including the European Banking Authority (EBA), the European Central Bank (ECB), and the European Commission, whose regulatory publications and policy initiatives have been instrumental in shaping the study’s conceptual and regulatory analysis.

Text notes

[1]*** (2015). DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing

Directive 2007/64/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366, [Accessed August15, 2025].

[2]*** (2023). 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. https://eur-lex.europa.eu/resource.html?uri=cellar:e09b163c-1687-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF, [Accessed August 15, 2025].

[3] *** (2023). 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.https://eur-lex.europa.eu/resource.html?uri=cellar:04cc5bd5-196f-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF,[Accessed August 15, 2025].

[4]Douglas W. Arner, Jànos Barberis & Ross P. Buckley, *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 Nw. J. Int'l L. & Bus. 371 (2017).https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2.

[5]Arner, D.W., Buckley, R.P., Zetzsche, D.A. *et al.* Sustainability, FinTech and Financial Inclusion. *Eur Bus Org Law Rev* **21**, 7–35 (2020). https://doi.org/10.1007/s40804-020-00183-y.

[6] *** (2022). 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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554, [Accessed October 1, 2025]

[7]Marangwanda, A., Mubanga, M., & Chaurura, P. (2025). The dual role of regulation in the insurance sector: Protecting consumers and fostering innovation. International Journal of Advanced Business Studies, 4(1), 38–50. https://doi.org/10.59857/PTTC9900

[8]Roitman, R., & Vives, X. (2021). PSD2, open banking, and the future of retail banking. Journal of Banking Regulation, 22(2), 121–138.

[9]European Parliament. (2025, August 29). Payment services framework. European Parliamentary Research Service (EPRS Briefing). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775891

[10] EY. (2023, July). How PSD3 and the PSR will shape trends in EU financial services. Ernst & Young Global Limited. https://www.ey.com/en_gl/insights/financial-services/emeia/how-psd3-and-psr-will-shape-trends-in-eu-financial-services.

[11]Bird & Bird LLP. (2023, July 5). Proposed PSD3 and Payment Services Regulation (PSR).https://www.twobirds.com/-/media/new-website-content/insights/pdfs/proposed-psd3-and-payment-services-regulation_050723.pdf.

[12]European Parliament & Council. (2022, December 14). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.

[13] Khioonarong, T., Leinonen, H., &Rizaldy, R. (2021). Operational resilience in digital payments: Experiences and issues (IMF Working Paper No. 288). International Monetary Fund. https://doi.org/10.5089/9781616355913.001.A001

[14]Arner, D. W., Buckley, R. P., Zetzsche, D. A., & Veidt, R. (2019). Sustainability, FinTech and Financial Inclusion (EBI Working Paper 2019/41). University of Luxembourg Law Working Paper No. 006-2019; University of Hong Kong Research Paper No. 2019/038. https://ssrn.com/abstract=3387359.

[15]Zetzsche, D. A., Arner, D. W., Buckley, R. P., & Kaiser-Yücel, A. (2020). Fintech Toolkit: Smart Regulatory and Market Approaches to Financial Technology Innovation (University of Hong Kong Faculty of Law Research Paper No. 2020/027). SSRN.

[16]International Monetary Fund. (2020). Fintech in Europe: Promises and Threats (IMF Working Paper No. 241).

[17]Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). Sage Publications.

[18] Klarna. (2021, June 4). Detailed incident report: Incorrect cache configuration leading to Klarna app exposing personal information. Klarna. https://www.klarna.com/international/blog/detailed-incident-report-incorrect-cache-configuration-leading-to-klarna-app-exposing-personal-information

[19]Finansinspektionen. (2021, July 5). FI investigates IT incident at Klarna. https://www.fi.se/en/published/ news/2021/fi-investigates-it-incident-at-klarna/Finansinspektionen

[20]Stripe. (2024, January 19). A guide to Klarna payments. Stripe. https://stripe.com/gb/resources/more/klarna-an-in-depth-guide

[21]Tink. (2025). European open banking platform. Retrieved from https://tink.com/

[22] Feyen, E. (2021). Fintech and the digital transformation of financial services. Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap117.pdf

[23]*** (2018). COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389, [Accessed August 16, 2025]

[24]Tink press release (Visa completes acquisition). (Tink, 2022). https://tink.com/press/visa-completes-acquisition-tink/

[25]EBA. (2022). Final Report Draft Regulatory Technical Standards amending Commission Delegated Regulation (EU) 2018/389. https://www.eba.europa.eu/sites/default/files/document_library/Publications/ Draft%20Technical% 20Standards/2022/EBA-RTS-2022-03%20RTS%20on%20SCA%26CSC/1029858/Final%20Report%20on% 20the% 20amendment %20of%20the%20RTS%20on%20SCA%26CSC.pdf.

[26]Klarna. (2021, October). Detailed incident report: Disturbances to Klarna's payment methods in Europe on October 2, 2021. https://www.klarna.com/international/press/detailed-incident-report-disturbances-to-klarnas-payment-methods-in-europe-on-october-2-2021

[27]Klarna. (2021, October). Information about the disturbances to Klarna's payment methods in Europe on October 2, 2021. https://www.klarna.com/international/press/information-about-the-disturbances-to-klarnas-payment-methods-in-europe-on-october-2-2021.

[28]Klarna incident report. (Klarna, 2021). https://www.klarna.com/international/press/detailed-incident-report-disturbances-to-klarnas-payment-methods-in-europe-on-october-2-2021

[29] European Banking Authority & European Central Bank. (2024, August 1). ECB and EBA joint report on payment fraud. https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-ecb-release-joint-report-payment-fraud

[30] European Central Bank (ECB). (2022). Payment statistics: 2021 update. Frankfurt: ECB.

[31] European Commission. (2023). Digital Finance Package: Towards PSD3 and PSR. Brussels: EC.

[32] European Banking Authority (EBA). (2022). EBA Report on the impact of FinTech regulation on payments. Brussels: EBA.

[33]Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. Journal of Economics and Business,Pages 7-25,ISSN 0148-6195,https://doi.org/10.1016/j.jeconbus.2018.07.003.

[34]Buchak, Greg and Matvos, Gregor and Piskorski, Tomasz and Seru, Amit, Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks (May 1, 2017). Columbia Business School Research Paper No. 17-39, Journal of Financial Economics (JFE), Forthcoming, Available at SSRN: https://ssrn.com/abstract=2941561

[35] ***(2019). Payment Services Act 2019, https://www.mas.gov.sg/regulation/acts/payment-services-act [Accessed October 3, 2025]

[36]Frost, J., Gambacorta, L., & Shin, H. S. (2021). BigTech and the changing structure of financial intermediation. Economic Policy, 36(106), 271–318.

[37]European Banking Authority (EBA). (2019). EBA Report on the impact of Fintech on payment institutions'and e-money institutions' business models. Brussels: EBA.https://www.eba.europa.eu/sites/default/files/documents/ 10180/2551996/32ff1cbb-a6c3-4a01-94f2-4d129386fa0a/EBA%20thematic%20report%20on%20the% 20impact%20of%20FinTech%20on%20PIs%27%20and%20EMIs%27%20business%20models.pdf

[38]European Banking Authority & European Central Bank. (2024, August 1). ECB and EBA joint report on payment fraud. https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-ecb-release-joint-report-payment-fraud

[39]Buckley, Ross P. and Arner, Douglas W. and Zetzsche, Dirk Andreas, FinTech: Finance, Technology and Regulation - Introduction (June 21, 2023). R. Buckley, D. Arner & D. Zetzsche, FinTech: Finance, Technology and Regulation (Cambridge University Press 2023), Chapter 1, UNSW Law Research Paper No. 23-28, FutureFinTech Working Paper Series, Available atSSRN: https://ssrn.com/abstract=4486054.

[40]Arner, Douglas W. and Zetzsche, Dirk Andreas and Buckley, Ross P. and Barberis, Janos Nathan, Fintech and Regtech: Enabling Innovation While Preserving Financial Stability (January 1, 2017). (2017) 18(3) Georgetown Journal of International Affairs 47, UNSW Law Research Paper No. 18-41, University of Hong Kong Faculty of Law Research Paper No. 2018/036, SSRN: https://ssrn.com/abstract=3211708

[41]Buchak, Greg and Matvos, Gregor and Piskorski, Tomasz and Seru, Amit, Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks (May 1, 2017). Columbia Business School Research Paper No. 17-39, Journal of Financial Economics (JFE), Forthcoming, Available atSSRN: https://ssrn.com/abstract=2941561

[42]Frost, Jon and Gambacorta, Leonardo and Huang, Yi and Shin, Hyun Song and Zbinden, Pablo, BigTech and the Changing Structure of Financial Intermediation (April 9, 2019). BIS Working Paper No. 779, Available at SSRN: https://ssrn.com/abstract=3369011

References

1. Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business,Pages 7-25,ISSN 0148-6195,https://doi.org/10.1016/j.jeconbus.2018.07.003*
2. Arner, Douglas W. and Zetzsche, Dirk Andreas and Buckley, Ross P. and Barberis, Janos Nathan, Fintech and Regtech (2017) . Enabling Innovation While Preserving Financial Stability (January 1, 2017). (2017) 18(3) Georgetown Journal of International Affairs 47, UNSW Law Research Paper No. 18-41, University of Hong Kong Faculty of Law Research Paper No. 2018/036, SSRN: https://ssrn.com/abstract=3211708, https://doi.org/10.2139/ssrn.3211708.
3. Arner, D. W., Buckley, R. P., Zetzsche, D. A., & Veidt, R. (2019). *Sustainability, FinTech and Financial Inclusion* (EBI Working Paper 2019/41). University of Luxembourg Law Working Paper No. 006-2019; University of Hong Kong Research Paper No. 2019/038. https://ssrn.com/abstract=3387359.
4. Arner, D.W., Buckley, R.P., Zetzsche, D.A. *et al.* Sustainability, FinTech and Financial Inclusion. *Eur Bus Org Law Rev* **21**, 7–35 (2020). https://doi.org/10.1007/s40804-020-00183-y.

5. Bird & Bird LLP. (2023, July 5). *Proposed PSD3 and Payment Services Regulation (PSR).*https://www.twobirds.com/-/media/new-website-content/insights/pdfs/proposed-psd3-and-payment-services-regulation_050723.pdf.
6. Buchak, Greg and Matvos, Gregor and Piskorski, Tomasz and Seru, Amit, Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks (May 1, 2017). Columbia Business School Research Paper No. 17-39, Journal of Financial Economics (JFE), Forthcoming, Available at SSRN: https://ssrn.com/abstract=2941561, https://doi.org/10.2139/ssrn.2941561.
7. Buckley, Ross P. and Arner, Douglas W. and Zetzsche, Dirk Andreas, FinTech: Finance, Technology and Regulation - Introduction (June 21, 2023). R. Buckley, D. Arner & D. Zetzsche, FinTech: Finance, Technology and Regulation (Cambridge University Press 2023), Chapter 1, UNSW Law Research Paper No. 23-28, FutureFinTech Working Paper Series, Available at SSRN: https://ssrn.com/abstract=4486054, https://doi.org/10.2139/ssrn.4486054.
8. Douglas W. Arner, Jànos Barberis & Ross P. Buckley, *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 Nw. J. Int'l L. & Bus. 371 (2017). https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2
9. European Banking Authority (EBA). (2019). EBA Report on the impact of Fintech on payment institutions' and e-money institutions' business models. Brussels: EBA. https://www.eba.europa.eu/sites/default/files/documents/ 10180/2551996/32ff1cbb-a6c3-4a01-94f2-4d129386fa0a/EBA%20thematic%20report%20on%20the% 20impact%20of%20FinTech%20on%20PIs%27%20and%20EMIs%27%20business%20models.pdf
10. European Banking Authority (EBA). (2022a). EBA Report on the impact of FinTech regulation on payments. Brussels: EBA.
11. EBA. (2022b). Final Report Draft Regulatory Technical Standards amending Commission Delegated Regulation (EU) 2018/389. https://www.eba.europa.eu/sites/default/files/document_library/Publications/ Draft%20Technical% 20Standards/2022/EBA-RTS-2022-03%20RTS%20on%20SCA%26CSC/1029858/Final%20Report%20on% 20the% 20amendment %20of%20the%20RTS%20on%20SCA%26CSC.pdf.
12. European Banking Authority & European Central Bank. (2024, August 1). ECB and EBA joint report on payment fraud. https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-ecb-release-joint-report-payment-fraud.
13. European Central Bank (ECB). (2022). *Payment statistics: 2021 update*. Frankfurt: ECB.
14. European Parliament. (2025, August 29). *Payment services framework.* European Parliamentary Research Service (EPRS Briefing). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775891
15. European Commission. (2023). Digital Finance Package: Towards PSD3 and PSR. Brussels: EC.
16. EY. (2023, July). *How PSD3 and the PSR will shape trends in EU financial services.* Ernst & Young Global Limited. https://www.ey.com/en_gl/insights/financial-services/emeia/how-psd3-and-psr-will-shape-trends-in-eu-financial-services.
17. Feyen, E. (2021). *Fintech and the digital transformation of financial services*. Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap117.pdf
18. Finansinspektionen. (2021, July 5). FI investigates IT incident at Klarna. https://www.fi.se/en/published/ news/2021/fi-investigates-it-incident-at-klarna/Finansinspektionen
19. Frost, Jon and Gambacorta, Leonardo and Huang, Yi and Shin, Hyun Song and Zbinden, Pablo, BigTech and the Changing Structure of Financial Intermediation (April 9, 2019). BIS Working Paper No. 779, Available at SSRN: https://ssrn.com/abstract=3369011
20. International Monetary Fund. (2020). *Fintech in Europe: Promises and Threats* (IMF Working Paper No. 241).
21. Khioonarong, T., Leinonen, H., &Rizaldy, R. (2021). *Operational resilience in digital payments: Experiences and issues* (IMF Working Paper No. 288). International Monetary Fund. https://doi.org/10.5089/9781616355913.001.A001
22. Klarna. (2021, June 4). Detailed incident report: Incorrect cache configuration leading to Klarna app exposing personal information. Klarna. https://www.klarna.com/international/blog/detailed-incident-report-incorrect-cache-configuration-leading-to-klarna-app-exposing-personal-information

23.Klarna. (2021, October). *Detailed incident report: Disturbances to Klarna's payment methods in Europe on October 2, 2021*. https://www.klarna.com/international/press/detailed-incident-report-disturbances-to-klarnas-payment-methods-in-europe-on-october-2-2021.
24.Klarna. (2021, October). *Information about the disturbances to Klarna's payment methods in Europe on October 2, 2021*. https://www.klarna.com/international/press/information-about-the-disturbances-to-klarnas-payment-methods-in-europe-on-october-2-2021.
25.Marangwanda, A., Mubanga, M., & Chaurura, P. (2025). The dual role of regulation in the insurance sector: Protecting consumers and fostering innovation. *International Journal of Advanced Business Studies, 4*(1), 38–50. https://doi.org/10.59857/PTTC9900.
26.Roitman, R., & Vives, X. (2021). PSD2, open banking, and the future of retail banking. Journal of Banking Regulation, 22(2), 121–138.
27.Stripe. (2024, January 19). A guide to Klarna payments. Stripe. https://stripe.com/gb/resources/more/klarna-an-in-depth-guide
28.Tink.(2025). *European open banking platform*. Retrieved from https://tink.com/
29.Tink. (2022). Tink press release (Visa completes acquisition). https://tink.com/press/visa-completes-acquisition-tink/
30.Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). Sage Publications.
31.Zetzsche, Dirk Andreas and Arner, Douglas W. and Buckley, Ross P. and Kaiser-Yücel, Attila, Fintech Toolkit: Smart Regulatory and Market Approaches to Financial Technology Innovation (May 11, 2020). University of Hong Kong Faculty of Law Research Paper No. 2020/027, Available at SSRN: https://ssrn.com/abstract=3598142, https://doi.org/10.2139/ssrn.3598142.
32.*** (2018). COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389, [Accessed October 1, 2025]
33.*** (2015). DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366, [Accessed October 1, 2025];
34.*** (2022, December 14). European Parliament & Council. *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)*. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554, [Accessed October 1, 2025]
35.***(2019). Payment Services Act 2019, https://www.mas.gov.sg/regulation/acts/payment-services-act [Accessed October 1, 2025]
36.*** (2023). 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. https://eur-lex.europa.eu/resource.html?uri=cellar:e09b163c-1687-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF, [Accessed October 1, 2025];
37.*** (2023). 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. https://eur-lex.europa.eu/resource.html?uri=cellar:04cc5bd5-196f-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF, [Accessed October 1, 2025];
38.*** (2022). 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. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554, [Accessed October 1, 2025]