STUDY

Requested by the ECON committee

European Parliament

Resilience of the Banking Union's Non-Cash Payment Systems

Disruptions Involving Third-Country Service Providers

Economic Governance and EMU Scrutiny Unit (EGOV)
Directorate-General Economy, Transformation and Industry
PE 764.370 – November 2025

EN

Resilience of the Banking Union's Non-Cash Payment Systems

Disruptions Involving Third-Country Service Providers

Abstract

This paper analyses the external dependencies and vulnerabilities in European payments, notably on cloud services or data privacy. It acknowledges that regulatory solutions enhance resilience but have limitations, while homegrown alternatives look tempting, but may be unfeasible, or come with major trade-offs. European institutions should carefully assess costs and benefits case by case, address short-term threats, while promoting strategic long-term planning, and push decisively for a Single Market in payment services.

This document was provided/prepared by the Economic Governance and EMU Scrutiny Unit at the request of the ECON Committee.

This document was requested by the European Parliament's Committee on Economic and Monetary Affairs.

AUTHORS
David RAMOS MUNOZ, University Carlos III of Madrid
Marco LAMANDINI, University of Bologna
Daniele D'ALVIA, Queen Mary University of London – Centre of Commercial Law Studies, and European Banking Institute

ADMINISTRATOR RESPONSIBLE
Kai Gereon SPITZER

EDITORIAL ASSISTANT
Ovidiu TURCU

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
The Economic Governance and EMU Scrutiny Unit provides in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact Economic Governance and EMU Scrutiny Unit or to subscribe to its newsletter please write to:
Economic Governance and EMU Scrutiny Unit
European Parliament
B-1047 Brussels
E-mail: egov@ep.europa.eu

Manuscript completed in November 2025

This document and other supporting analyses are available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

CONTENTS

LIST OF ABBREVIATIONS

AIS	Account Information Service
AISP	Account Information Service Provider
API	Application Programming Interface
AWS	Amazon Web Services
CBDC	Central Bank Digital Currency
CJEU	Court of Justice of the European Union
CLOUD ACT	Clarifying Lawful Overseas Use of Data Act 2018 (US)
DORA	Digital Operational Resilience Act – Regulation 2254/2022
EBA	European Banking Authority
ECMS	Eurosystem Collateral Management System
EIOPA	European Insurance and Occupational Pensions Authority
EMI	Electronic Money Institution
EMD2	Electronic Money Directive 2009/110/EC
EPI	European Payments Initiative
ESAs	European Supervisory Authorities
ESMA	European Securities and Markets Authority
EU	European Union
FINTECH	Financial Technology
FISA	Foreign Intelligence Surveillance Act (US)
FMI	Financial Market Infrastructure
IBAN	International Bank Account Number

ICT	Information and Communications Technology
MiCA	Regulation (EU) 2023/1114
PIS	Payment Initiation Service
PISP	Payment Initiation Service Provider
PIX	Instant Payments System created by the Bank of Brazil
PSD1	Directive 2007/64
PSD2	Directive 2015/2366
PSP	Payment Services Provider
SCA	Strong Customer Authentication
SCT	SEPA Credit Transfer
SCT Inst	Instant SEPA Credit Transfer
SEPA	Single Euro Payments Area
SIP	Instant Payment System (in Brazil)
SIPS	Systemically Important Payment System
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TPP	Third-Party Provider
UPI	Unified Payments Interface (payments system in India)

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY*

European retail payment services are dependent on global messaging networks, like SWIFT, foreign providers of Information and Communication Technology (ICT) services, like cloud services providers, and card networks, such as Visa and Mastercard. ICT services and card networks are dominated by US companies. This can be a source of risk in a context of cybersecurity threats or geopolitical tensions.

DORA (the Digital Operational Resilience Act) harmonizes the approach for managing ICT risks, reporting incidents, and supervising critical third-party providers, introducing a unified EU rulebook. However, it is only starting to function, and its ability to mitigate all relevant risks is still uncertain. Promoting diversification and back-up plans should be part of any strategy, but directly favouring EU providers is unlikely to work, and may hinder service quality. Pursuing a policy of locating services in the EU may be legally feasible for payment services, harder for ICT services, but that does not mean that it is advisable.

On data protection, the Schrems II case shows that fundamental differences between the EU and the US in the way security and privacy are weighed can become a source of operational risk. Differences of principle may not be fully solved. Thus, cooperation between authorities and robust contract frameworks should be prioritised to at least solve concrete practical problems. Any strategy should ensure that sensitive kinds of data remain in Europe, protected by high cyber-security and encryption, while for other use cases, data could be processed outside Europe, under appropriate standards.

Regulation – especially when 'simplified' – can strengthen operational resilience, but it cannot eliminate fundamental legal and geopolitical asymmetries. These include conflicting foreign surveillance laws, concentration risks in hyperscalers, and unavoidable interdependencies in global payment platforms. A resilient EU payment ecosystem must therefore rely on diversification, layered safeguards, and credible fallback pathways, rather than regulation alone.

The EU enjoys solid payments infrastructures, like TARGET, for interbank settlement, or SEPA, for retail payments, but they do not currently offer an alternative to existing card schemes. Experiences with successful homegrown fast retail payments systems in China, India or Brazil suggest that a more hands-on approach by the central bank/s and public authorities is needed.

The Digital Euro is promoted as an answer to the lack of homegrown payment systems and to threats to monetary sovereignty. As an end in itself, a Central Bank Digital Currency (CBDC) presents greater challenges than a fast payment system and is unlikely to replace existing solutions. However, as a *means* to an end a CBDC may provide the strong mandate needed to create a homegrown payments ecosystem.

* This Report greatly benefitted from exchanges with different people and stakeholders. We would like to express our deep gratitude to all, and to mention those that accepted to be mentioned expressly, including Professor Rosa María Lastra, Sir John Lubbock Chair in Banking Law and the Centre for Commercial Law Studies, Queen Mary University of London, and Mr. Charles Randell, Senior Consultant at Slaughter and May in London, and former Chair of the Financial Conduct Authority, for their invaluable guidance and expertise, and the excellent team from the EGOV unit, Kai Gereon Spitzer, Maja Sabol and Marcel Magnus, who, always precise and constructive in their reviews, this time went beyond the call of duty to ensure that the Report was as robust and comprehensive as possible. Needless to say, all errors remain our own.

1. INTRODUCTION

Non-cash payment systems keep the economy moving. They include large value payment systems and retail payment systems. Retail payment systems in particular involve at least three elements: the *instrument*, which is a liability of a specific issuer, e.g., bank deposits; the *infrastructure*, or technology, to facilitate transfer between users, which encompasses hardware and software, and the *scheme*, a set of rules, practices, standards to execute payments.[1] Some systems, such as e-money, emphasize the instrument, allowing operators to develop a closed loop infrastructure, supported by specific rules. Others, such as Fast Payment Systems (FPSs) focus on both the infrastructure (comprising a communications network to connect users, merchants and issuers, and a settlement system. Central Bank Digital Currencies (CBDCs) are designed with a focus on all three elements, including central bank money (instrument), an infrastructure typically owned and operated (at least in its core) by a central bank, and a scheme that encompasses the end user.[2] In addition, we normally speak of *payment instruments*, used to initiate a payment (e.g., card or bank account) *transaction channels*, to process the payment (web, mobile app, quick response (QR) codes) and *use cases*, as the needs covered (B2B, P2P, person-to-government, etc.[3]) Payment systems offer different combinations of instruments, public, private or hybrid infrastructures, and privately issued rules, public regulation, or a combination of both.[4]

The European payments system evolved in an era of openness, where global integration was seen as a way to enhance efficiency and inclusion. The current retrenchment and geopolitical tension, however, present external dependencies as a vulnerability, including foreign cloud services hyperscalers (Amazon Web services (AWS), Microsoft Azure, or Google Cloud services (GCS)), card networks (Visa and Mastercard), or international messaging systems (SWIFT), which can be subject to external pressures, or foreign laws reflecting principles that largely differ from those of EU law.

Spotting risks is simpler than eliminating them. Payments are finance's 'plumbing', and a complex system, formed by (i) public sector infrastructures, (ii) private providers and platforms, and (iii) a regulatory/institutional framework, including (1) **regulatory** norms, e.g., the Payment Services Directives PSD1, PSD2 and now PSD3 and PSR, or the Digital Operational Resilience Act (DORA), (2) **design** norms for **public infrastructures** (T2, T2S, or TIPS) or **private** infrastructures that have a strong role for **public authorities** (e.g., the Single European Payments Area (SEPA), or the Society for Worldwide Interbank Financial Telecommunication (SWIFT)) and (3) **private** norms, e.g., Visa or Mastercard card networks contracts.

---

1 Manisha Patel, Safari Kasiyanto, André Reslow 'Positioning Central Bank Digital Currency in the Payments Landscape' *IMF FinTech Notes*, NOTE/2024/006, p. 3.

2 Ibid, p. 4.

3 José Aurazo, Holti Banka, Jon Frost, Anneke Kosse, Thomas Piveteau 'Central bank digital currencies and fast payment systems: rivals or partners?' BIS Papers No 151 (December 2024).

4 In Europe, for instance, T2, TDS or TIPS are interbank settlement infrastructures owned and operated by the Eurosystem, while the SEPA Credit Transfer scheme is owned by the European Payments Council (EPC), which also adopts its rulebook, but this rulebook, in turn, is supported by a legal framework formed by Directives and Regulations (see *infra* Annex for further detail). In contrast to this 'hybrid' system, PIX, the main payment system in Brazil, has an infrastructure owned and operated by the central bank, and the scheme, also adopted by the central bank, encompasses end users (see *infra* section 5.3).

Norms coexist, although they were adopted at different times, with different sentiments. Europe's initial goal was to **promote the single market**, prioritising access, interoperability and user focus, as seen in the SEPA or PSD1, fitting into a global context of openness and communication, seen in SWIFT. After the 2007-2008 global financial crisis, access and interoperability were accompanied by **financial stability and user protection**, as seen in the PSD2, which balances Open Banking with user and data protection, or T2, T2S, or TIPS, which sought to ensure a stable, reliable system. The current emphasis on **risk, protection and fragmentation** presents the system's openness and diversity not as a success, but as a source of risk and vulnerability. Homegrown, airtight solutions, seen not long ago as duplicative and wasteful, are now perceived as a reliable source of comfort.

This paper's **Annex** describes EU payment rules' evolution and alphabet soup (SEPA, PSD1, 2, 3, TPP, PISPs, AISPs, TIPs etc.) in more detail, while the following sections focus on risks and vulnerabilities.

Section 2 of this paper introduces Europe's payments system and maps its dependencies and vulnerabilities. Section 3 focuses on risks arising from information and communication technology (ICT), in particular cloud services. Section 4 discusses privacy and data protection risks. We also assess regulatory initiatives, like the Digital and Operational Resilience Act (DORA) or data protection measures. Section 5 considers "home grown" solutions, as an alternative to regulation, drawing some lessons from other successful homegrown payment systems in China, India or Brazil for Euro-based payment solutions, or the Digital Euro. Section 6 concludes.

2. PAYMENT SYSTEM PROVIDERS: STRUCTURAL DEPENDENCIES AND RESILIENCE RISKS

Payments are a "system" that promotes concentration through network effects (Annex). The European Union built its normative framework with a primary focus on ensuring technical neutrality and promoting competition and access to the single market by operators and consumers (Annex, no. 2.) A pivot towards risk and systemic stability brought measures focused on public Financial Market Infrastructures (FMIs) (Annex, no. 3.), but this left some dependencies on technology infrastructures or retail payment networks untouched, which are now the main source of concern. This section maps the European payments landscape's dependencies and vulnerabilities, in light of past disruptions (2.1.), analyses existing supervisory frameworks (PISA and DORA) and their gaps and uncertainties (2.2.), and rates different scenarios in light of their potential impact (2.3.).

2.1. Dependency Mapping, Risk Assessment and Past Disruptions

To understand the exposure of the European Union to external disruptions we map out the critical components of the payment system. **EU-governed infrastructures** like the ECB's T2 settlement system (large-value transactions), and TIPS (instant retail payments), are under European public authority, jurisdiction and oversight (Annex, no. 3). However, cross-border settlement of high-value transactions often involve US dollar legs, requiring access to US payment systems like Fedwire and CHIPS.[5]

Furthermore, messaging, a core payments service depends on the messaging network SWIFT,[6] headquartered in Belgium, that has proven to be pliable to US influence through sanctions.[7] Retail card payments overwhelmingly rely on Visa and Mastercard, two US-based payment system platforms,[8] which, in 2023, handled roughly 7 trillion Euros in European payment volume and raised concerns due to their dominance[9] and subjection to US law. Likewise, cloud services are provided by US large tech companies ("hyperscalers"[10]) like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP). The market for AML services or core software is also relatively concentrated. **Table 1**

---

5 Santiago Carbo-Valverde, Charles M. Kahn, 'Payment Systems in the US and Europe: Efficiency, Soundness, and Challenges' (2016) 30 Revista de Estabilidad Financiera 11, 19 – 20.

6 Susan V. Scott, Markos Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community* (Routledge 2014), Chapters 1 and 2. SWIFT is not a clearing and/or settlement system, nor manages or holds funds or bank accounts. It creates a standardised process for the transmission of inter-bank transaction communications. SWIFT goes further by committing to neutrality, although such neutrality is challenged in the case of international sanctions.

7 Rosa Maria Lastra, 'Weaponisation of Money and Payments' in Chiara Zilioli, Regis Bismuth, Luc Thevenoz (eds.) *International Sanctions: Monetary and Financial Law Perspectives* (Brill, 2024), 102 – 122.

8 Carbo-Valverde, note 75, 30.

9 Claudia Pincovski, 'Breaking the Visa and Mastercard duopoly: Europe's path to innovation' (9 April 2025) The Paypers available at https://thepaypers.com/payments/expert-views/breaking-the-visa-and-mastercard-duopoly-europes-path-to-innovation, accessed on 21 November 2025.

10 Hyperscalers are large-scale data centers that provide a wide range of cloud computing and data solutions for businesses that need vast digital infrastructure, processing, and storage. People from the tech industry has used the term since the 2010s, but it has recently gone mainstream. See https://www.britannica.com/money/hyperscaler-data-centers, , accessed on 21 November 2025.

maps dependencies and vulnerabilities. Data privacy, while not a service, is a source of vulnerability due to external dependencies (infra no. 4) and was included as well.

Table 1: Comparative Overview of Critical Payment System Dependencies in the EU

System/Function	Provider Type	Main Provider	Third Country Risk	Jurisdiction
Interbank Messaging	Private Cooperative	SWIFT	Medium-High	Belgium/US influenced
Retail Card Payments	Private Company	Visa and Mastercard	High	US
Real-time Payment Infrastructure (TIPS)	Public infrastructure	Eurosystem	Low	EU
Cloud Hosting for Banks	Private Company	AWS, Microsoft Azure, Google Cloud	High	US
AML	Private Company	LexisNexis, Palantir, NICE Actimize	Medium – High	USA/Israel
Software of Core Banking	Mixed	Temenos, Oracle, SAP, Finastra	Medium	Switzerland, USA, and EU
Personal Data Transfer	Legal Framework	EU – US Data Privacy Framework	High	Bilateral

Disruptions or tensions have been rare, but noticeable. Some of those disruptions had technical causes. This is the case of some episodes with "hyperscalers", such as Azure's recent (September 2025) service disruptions and increased latency due to fibre optic cable cuts in the Red Sea,[11] or the CrowdStrike incident, where a Distributed Denial-of-Service (DDoS) cyberattack caused outages of essential Microsoft 365 services on 30-31 July 2024.[12] On that same day, AWS also suffered disruptions of some critical services for hosting or storage, impacting businesses dependent on them, including Amazon's own brands (Ring, Whole Foods or Alexa).[13] For Google Cloud, a faulty change in the Service Control system caused the outage of popular websites and apps.[14] Some of these incidents (e.g., the CrowdStrike one) affected some financial services.

[11] "Microsoft cloud services disrupted by Red Sea cable cuts. 7 September 2025. Available at: https://www.bbc.com/news/articles/c3rvx470yg8o. Accessed on 21 November 2025.

[12] Kate O'Flaherty "Microsoft Confirms New Outage Was Triggered By Cyberattack". Available at: https://www.forbes.com/sites/kateoflahertyuk/2024/07/31/microsoft-confirms-new-outage-was-triggered-by-cyberattack/. Accessed on 21 November 2025.

[13] Ibid.

[14] Google Cloud – Anatomy of a Systemic Failure. An Analysis of the June 2025 Google Cloud Outage and the Mandate for a New Cloud Resilience Strategy. 24 June 2025. https://hyperframeresearch.com/2025/06/24/google-cloud-anatomy-of-a-systemic-failure/. Accessed on 21 November 2025.

Other disruptions had political causes. This is notably the case for SWIFT. In 2012, SWIFT removed Iranian banks from its service,[15] showing US-EU coordination with a European Council resolution that followed US's guidelines. [16] However, the US showed willingness to act unilaterally if cooperation was not forthcoming. Unilateralism materialised in 2018, when the US withdrew from the Joint Comprehensive Plan of Action (JCPOA) for the monitoring of Iran's uranium enrichment, reimposing sanctions and pressuring SWIFT to disconnect Iranian banks again.[17] The EU supported the JCPOA,[18] objected to US extra-territorial sanctions[19] and updated its blocking statute to counter them.[20] SWIFT, however, complied with US demands and the EU set up the Instrument in Support of Trade Exchange (INSTEX) clearing house to continue trade with Iran,[21] showing US influence over SWIFT, and the EU's lack of it.[22] In 2022, prompted by the EU and its allies, SWIFT cut off access for certain Russian banks after the invasion of Ukraine, showing that SWIFT can be leveraged or 'weaponised'.[23]

Visa and Mastercard (and American Express) also suspended their services in Russia in March 2022, after the invasion of Ukraine. The main beneficiary was Mir, a domestic card scheme.

Finally, tensions (if not disruptions) arose when the Court of Justice, in *Schrems II* (case C-311/18), invalidated the EU-US Privacy Shield framework, casting doubt over data sharing frameworks of cloud service providers (see *infra* section 4).

2.2. Supervisory Frameworks (PISA, DORA) and Gaps

In 2016, the ECB updated its 'Oversight Policy Framework' aligning it with the CPMI-IOSCO Principles for Financial Market Infrastructures and relevant EU regulations, while National Central Banks had their own schemes, including one for SWIFT risk controls, led by the National Bank of Belgium, with G-10

---

15 Scott, Zachariadis, note 76, 133.

16 Simon Bale, 'SWIFT instructed to disconnect sanctioned Iranian banks following EU Council Decision' (15 March 2012). Available at: https://www.swift.com/insights/press-releases/swift-instructed-to-disconnect-sanctioned-iranian-banks-following-eu-council-decision. Accessed 21 November 2025.

17 Esfandyar Batmanghelidj, Axel Hellman, Europe, Iran and Economic Sovereignty: A New Banking Architecture in Response of US Sanctions (June 2018) European Leadership Network, available at https://otaghiranonline.ir/UFiles/Docs/2018/6/9/Doc20180609095510613.pdf. Accessed 21 November 2025.

18 Shirzad Azad, 'Saddled with SWIFT: the American withdrawal from the nuclear deal and its ramifications for Sino-Iranian financial and banking interactions'. Available at: https://www.ti.tku.edu.tw/ti/news/3c5fda7c-0efb-42ec-af37-610a30282925/xsrpxA1mMy5.pdf. Accessed 21 November 2025.

19 Morris P. Sean, 'SWIFT clouds between international legal storms? Bank Melli, the CJEU and Secondary Sanctions' (2022) 17 (9) Global Trade and Customs Journal, 404 – 407.

20 European Commission, 'Updated Blocking Statute in Support of Iran Nuclear Deal Enters into Force' (6 August 2018) Press Release, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_18_4805, accessed on 21 November 2025. The blocking statute was a landmark unified EU action to protect EU operators from extra-territorial application of third country laws (see Council Regulation (EC) No 2271/96) after in 1996 the US took unilateral measures against Cuba, Iran, and Libya.

21 Gregoire Mallard, Anna Hanson, 'Embedded extraterritoriality: US judicial litigation and the global banking surveillance of digital money flows' in Charlotte Beaucillon (ed.) *Research Handbook on Unilateral and Extraterritorial Sanctions* (Edward Elgar, 2021), 125.

22 Peter E. Harrell, Elizabeth Rosenberg, 'The outlook for US coercive economic measures' in *Economic Dominance, Financial Technology, and the Future of US Economic Coercion* (2019) Centre for a New American Security, 26.

23 Gary Robinson, Sabine Dorry, Ben Derudder, 'SWIFT: Trusted Infrastructure for Infrastructures' in Carola Westermeier, Malcolm Campbell-Verduyn, Barbara Brandl (eds.) *The Cambridge Global Handbook of Financial Infrastructure* (Cambridge University Press, 2025), 246; Lastra, 'Weaponisation of Money and Payments', note 77, 102 – 122.

central banks and the ECB. However, the Oversight Policy Framework focused primarily on clearing and settlement systems and did not fully cover Mastercard or Visa.

In 2021-2022, the ECB replaced previous frameworks with the PISA framework (for Payment Instruments, Schemes, and Arrangements), to include credit transfers and cards (among others) above a certain threshold of importance, like Visa and Mastercard. PISA focuses on payment schemes' governance bodies, legal, business, operational, cyber, interdependency, and financial risk. Thus, Visa and Mastercard began to be considered worthy of supervision only very recently, and, given the learning curve in supervisory activity, it is unlikely that there is a full grasp of the risks involved. Furthermore, the framework's generalist approach, and its focus on governance does not specifically address risks arising from geopolitical disruptions that characterise card network schemes.

Outsourced services are another source of vulnerability: under PSD2, banks and payment firms outsourcing important functions to third parties must maintain audit rights, data sovereignty, and termination rights, conduct due diligence, ensure access to data and business continuity, and even pre-arrange exit plans.[24] However, critical service providers headquartered outside the EU may be subject to conflicting obligations, e.g., a bank's audit or termination rights may be of little consequence if the provider has already handed over data due to a surveillance order under the US Cloud Act.

This explains the 2022 Digital Operational Resilience Act (DORA), which brings 'Critical ICT Service Providers' to the financial sector under the joint oversight of the European Supervisory Authorities (EBA, ESMA, EIOPA), including risk management requirements and audits. Major tech companies, especially hyperscalers like AWS, Azure, GCS, etc., are the primary focus, but Visa or Mastercard were not included in the initial list of critical ICT providers, since they are payment scheme operators, and may argue that they are not 'ICT providers'; and the European Supervisory Authorities confirm that the elements of governance or business processes do not count as ICT services.[25] Furthermore, DORA neither overrides existing contracts nor eliminates concentration risks. Supervision will begin now that critical ICT providers were designated in November 2025.

---

[24] EBA, *Final Report on EBA Guidelines on Outsourcing Arrangements* (25 February 2019), available at https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf, accessed on 21 November 2025.

[25] The initial list of designated critical ICT third-party service providers at Union level under Article 31(9) DORA includes the following entities: Accenture plc, Amazon web Services EMEA Sarl, Bloomberg L.P., Capgemini SE, Colt Technology Services, Deutsche Telekom AG, Equinix (EMEA) B.V., Fidelity National Information Services, Inc., Google Cloud EMEA Limited, International Business Machine Corporation, InterXion HeadQuarters B.V., Kyndryl Inc., LSEG Data and Risk Limited, Microsoft Ireland Operations Limited, NTT DATA Inc., Oracle Nederland B.V., Orange SA, SAP SE and Tata Consultancy Services Limited. See the List of 19 Designated critical ICT third-party services providers at Union Level, 18 November 2025. Visa and Mastercard are not included in that list. Some unofficial Questions and Answers (Q&A) documents published on May 2024 and on 28 March 2025 to help the industry with the dry run for the Register of Information (RoI) did not clarify the matter. See EBA Frequently Asked Questions (FAQs). Question 55 Reporting of registers of information under DORA. 28 March 2025, or Question 125 of DORA 2024 Dry Run exercise on reporting of registers of information. (accessed on 21 November 2025). Question 55 refers to the "official" Q&A document, question 161. Q 161, published on 14 November 2025 states that "any relevant service provided by providers of payment-processing activities or operating payments infrastructures that falls within the definition under Article 3(21) of DORA, should be considered as an ICT service under DORA. [...] It should, however, be noted that not all services provided by these providers, including payment card schemes, are to be considered ICT services. Services provided by a governance body of a scheme or business processes of the providers of payment-processing activities or operating payments infrastructure without a prevailing ICT component, such as clearing and settlement, should not be considered within the scope of ICT services under Article 3(21) of DORA." See Q 2024_7290 Definition and scope of ICT services, available at: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2024_7290, accessed 21 November 2025.

2.3. Risks and Resilience: Strategic Implications

The above illustrates that the potential risk scenarios can involve (i) **legal or extra-territorial enforcement actions by a foreign government** impacting **services** like SWIFT, or surveillance measures under the US CLOUD Act or similar laws affecting European banks' data stored with cloud providers; (ii) **a provider's termination** affecting proprietary software or platforms (core banking systems, card processing software, or security modules), or a termination/restriction by Visa or Mastercard to European institutions or regions (unlikely at present); or (iii) **technical disruptions through intermediary layers**, cloud services or other outsourced IT functions (e.g., incidents like AWS and Azure 2024-2025 outages, CrowdStrike (cyberattack), or the GCS's flawed update). These **risks are not mutually exclusive**, and may be prompted by other events, e.g., an invalidation by the Court of Justice of the data privacy framework. **Table 2** below rates these scenarios by impact, according to the authors' own assessment.

Table 2: Risk Vectors for Third-country Disruptions to EU Payment Systems

Risk Vector	Mechanism	Example	Impact Level
Extra-territorial sanctions	Third-country mandates cut-off access	SWIFT block on Iranian banks (2012 and 2018) and on Russian banks (2022), Visa suspension of services in Russia (2022)	High
Suspension of Data Transfers	Invalidated adequacy decision or regulatory order	*Schrems II* (2020), Privacy Shield annulment	High
Cloud Access Denial	Cloud provider withdrawal from EU contracts	Potential under US Cloud Act	Medium-High
Software license revocation	Termination of critical software updates	No EU-wide precedent yet	Medium
Legal enforcement under foreign law	National security orders to providers	Microsoft data case (2014)	Medium
Cybersecurity exploits	State-driven backdoors in software or firmware	SolarWinds (2020)	Medium - High

Source: Author's own assessment

This analysis identifies scenarios of potential disruptions; it does not assess their likelihood. However, thinking about such scenarios helps identify dependencies, and enhance safeguards and back-up plans. Responses range from regulations to enhance resilience, to homegrown alternatives to enhance strategic autonomy.

DORA represents the **regulatory approach**, embedding resilience in industry practice and culture, and subjecting critical ICT providers to EU scrutiny and risk controls. However, ICT critical providers were designated in 2025, and thus the process is ongoing, and the outcome is still uncertain. Furthermore,

the DORA's Oversight Forum,[26] due to the ESAs sectoral supervisory model, may find it difficult to muster the necessary expertise.

Homegrown alternatives entail their own challenges. The EU's instant payments regulation,[27] which will oblige all euro-area banks to offer instant credit transfers at affordable rates by 2025[28] and requires SEPA instant payments to be universally available, may become a fallback or substitute to card payments by promoting account-to-account payments, while consumer adoption will still shape the process. Conversely, GAIA-X,[29] a project that tries to promote cloud sovereignty with a federated and secure data infrastructure has so far failed to take off.[30] It has been criticised for a lack of clear objectives (trying to be too many things at once), internal tensions,[31] an excessively theoretical focus on standards, rather than on actions in the market,[32] and a flawed governance model, which included among its stakeholders the very US hyperscalers that prompted the quest for a European alternative in the first place.[33] In the short to medium term, policies of diversification of cloud providers seem more realistic than onshoring services inside Europe, due to a lack of European alternatives.

[26] To further evaluate the competences of the Oversight Forum see EBA, EIOPA, ESMA, 'Mandate of the Oversight Forum as a Joint Committee Sub-Committee of the European Supervisory Authorities' (29 November 2024), available at https://www.eba.europa.eu/sites/default/files/2025-01/6536449d-31f1-4376-ab90-4570f6c3b81e/JC_24_93_Mandate%20Oversight%20Forum.pdf, accessed on 21 November 2025.

[27] Regulation (EU) 2024/886 of the European Parliament and of the Council (13 March 2024).

[28] European Commission, 'Payment Services' available at https://finance.ec.europa.eu/consumer-finance-and-payments/payment-services/payment-services_en#:~:text=Payment%20service%20providers%20in%20the,possible%20for%20their%20clients%20to%C2%A0receive%C2%A0them, accessed on 21 November 2025.

[29] Simona Autolitano, Agnieszka Pawlowska, 'Europe's quest for digital sovereignty GAIA-X as a case study' (2021) Istituto Affari Internazionali, available at https://www.iai.it/sites/default/files/iaip2114.pdf, accessed on 21 November 2025.

[30] The Economist "Europe fantasises about an "Airbus of everything!" Can it fly?" May 29th, 2025. Available at: https://www.economist.com/europe/2025/05/29/europe-fantasises-about-an-airbus-of-everything-can-it-fly

[31] Clothilde Goujard, Laurens Cerulus "Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project" *Politico*, October 21, 2021. Available at: https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/ (accessed November 7, 2025).

[32] Euro Stack Conference notes (sept. 2024) 19 Nov. 2024. Available at: https://fermigier.com/blog/2024/11/eurostack-conference-notes.md/. Accessed on 7 November 2025 (remarks by Francesco Bonfiglio, former CEO of Gaia-X). See also Agathe Cherki "Gaia-X, ou les illusions perdues d'un cloud européen". 30 May 2022. Available at: https://www.contexte.com/fr/article/tech/gaia-x-souverainete-cloud_150712 (accessed November 7, 2025).

[33] Andreas Baur "European ambitions captured by American clouds: digital sovereignty through Gaia-X?" Information, Communication and Society (June 2025).

3. CLOUD SERVICES: DEPENDENCY, RISK AND REGULATIONS

This section specifically analyses the Banking Union's dependency on cloud service providers, examining market concentration (3.1.), risk vectors (legal and operational vulnerabilities) (3.2.), regulatory and supervisory responses (including DORA) (3.3.), identifies key aspects of resilience assessments (3.4.), and specifically analyses the legal feasibility (and operational limitations and risks) of relocation policies (3.5.).

3.1. European Financial Institutions, the Cloud, and its concentration

Cloud services have reshaped how financial institutions operate. Access to agile, scalable, on-demand IT resources without large in-house data centres allows banks to deploy applications and scale up services,[34] thus accelerating digitalisation.[35] Cloud platforms also provide advanced tools (big data analytics, AI services…)[36] that banks would struggle to develop alone. Thus, European banks' 'cloud first' strategy is due to cost efficiency (replacing upfront capital expenditures with flexible pay-as-you-go models), resilience and security capabilities (with geographically distributed data centres) or improvements in cybersecurity thanks to providers' expertise and flexible services, e.g., on-demand services, real-time analytics, or scalability during, e.g., spikes in online transactions. This trend accelerated after COVID.[37] A global study in July 2024 found that 98% of financial institutions had at least some data, applications, or operations in the cloud,[38]and some European banks are moving from peripheral applications like email to core banking systems; e.g., Banco Santander announced plans to migrate most of its core banking platform to the cloud by end-2024.[39] Some non-EU institutions have fully migrated; e.g., Capital One in the US.[40] The ECB has stated that 'digital transformation is a must' for banks to be competitive[41] and cloud services are key in this process.

However, as European financial institutions embrace cloud services, **concentration of such services** becomes a cause of concern. The cloud market is dominated by Amazon Web Services, Microsoft Azure

---

[34] Ravi Pratap Singh, Abid Haleem, Mohd Javaid, Ravinder Kataria, Sandeep Singhal, 'Cloud computing in solving problems of Covid-19 pandemic' (2021) 6 (2) Journal of Industrial integration and Management, 209 -219.

[35] European Commission, 'A new era for Europe: how the European Union can make the most of its pandemic recovery, pursue sustainable growth, and promote global stability' (2022), 9, 94.

[36] Manoj Kumar, 'The future of AI in Big Data: Cloud platforms are evolving to support machine learning and analytics' (2023) 1 (1) International Journal of Advancements in Computational Technology, 128 – 135.

[37] European Commission, 'A new era for Europe', note 108.

[38] Programme on International Financial Systems, 'Data localization, Cloud Adoption, and the Financial Sector' (July 2024) 4, available at https://www.pifsinternational.org/wp-content/uploads/2024/07/Report-on-Data-Localization-07.29.2024.pdf#:~:text=financial%20institu%02tions%20to%20scale%20up,8%20Some%20banks%20have, accessed on 21 November 2025.

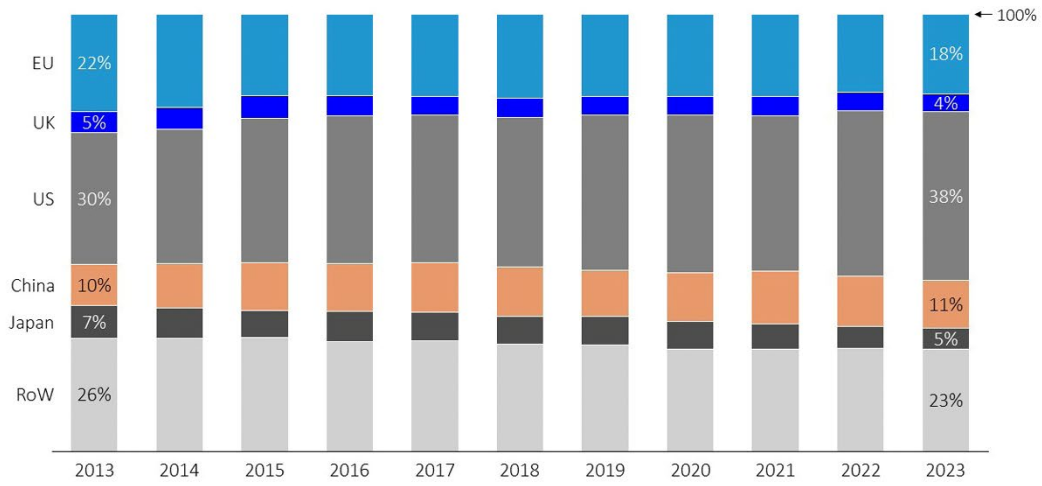
[39] Santander, 'Santander passes key milestone in its transformation after migrating its CIB banking platform to the cloud' (11 December 2023) available at https://www.santander.com/content/dam/santander-com/en/documentos/notas-de-prensa/2023/12/np-2023-12-11-santander-passes-key-milestone-in-its-transformation-after-migrating-its-cib-banking-platform-to-the-cloud.pdf, accessed on 21 November 2025.

[40] Capital one, 'Lessons from Capital One's cloud migration journey' (23 May 2024), available at https://www.capitalone.com/software/blog/cloud-migration-journey/, accessed on 21 November 2025.

[41] European Central Bank, 'The digital transformation of the European banking sector: the supervisor's prospective' (13 January 2022) available at https://www.bankingsupervision.europa.eu/press/speeches/date/2022/html/ssm.sp220113~8101be7500.en.html, accessed on 21 November 2025.

and Google Cloud, which represent two-thirds of the European Union's cloud infrastructure market[42]. Thus, European banks' data depend on US data centres (France's OVHcloud or Germany's T-Systems hold a minor fraction of the market[43]) while ICT revenues have significantly decreased between 2013 and 2023 (see below).

Figure 1: ICT global market share by geographic area, in % (2013-2023)



Source: IDC, 2024 (Draghi Report, The Future of European Competitiveness, Part B: In-depth analysis and recommendations)

This dependency, and the risks it entails, epitomises Europe's 'sovereignty gap'.[44] Europe's response to this 'technopolar' era is 'digital sovereignty', an ambiguous term, which can encapsulate closing the gap, or promoting European values, to counter the dominance (or threat) from the US, China or Russia.[45]

3.2. Cloud-Related Risk Vectors

The risks arising from European financial institutions' dependency on a concentrated market of non-EU providers can be classified in the following key risks areas.

Operational disruption risk. Banks moving critical functions to the cloud risk outages or incidents at their cloud providers propagating into service interruptions. A failure in a cloud data centre or misconfigured cloud service could suddenly knock out online banking, payment processing, or other essential operations for multiple institutions. Past incidents caused hours-long downtime for websites

---

42 Jennifer Johnson, George Hay, 'Europe will struggle to get Big Tech off its cloud' (27 January 2025) Reuters, available at https://www.reuters.com/commentary/breakingviews/europe-will-struggle-get-big-tech-off-its-cloud-2025-06-26/#:~:text=Amazon,priced%20services, accessed on 21 November 2025.

43 Ibid.

44 Claire Stolwijk, et. al., 'Bridging the Dutch and European Digital Sovereignty Gap' (21 March 2022) TNO Innovation for Life, 1 – 82, available at https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf, accessed on 21 November 2025.

45 Ian Bremmer, 'The technopolar moment' (2021) 100 (6) Foreign Affairs, 112 – 128; Rebecca Adler-Nissen, Kristin Anabel Eggeling, 'The discursive struggle for digital sovereignty: security, economy, rights and the Cloud Project GAIA-X' (2024) 62 (4) Journal of Common Market Studies, 993 – 1011; Carla Hobbs (ed.), Europe's Digital Sovereignty: from Rulemaker to Superpower in the Age of US-China Rivalry' (July 2020) European Council of Foreign Relations, available at https://ecfr.eu/archive/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf, accessed on 21 November 2025.

and applications, and regulators dread the prospect of such incidents affecting large parts of banking.[46] Sector-wide 'aggregate' outages are likelier with greater cloud concentration: in 2023, the top nine UK banks collectively suffered 33 days of unplanned IT outages, disrupting services for customers.[47] The causes ranged from hardware faults to software bugs and human error, but they exposed bank operations' complexity and fragility. Complexity increases as banks juggle hybrid on-premises and cloud systems. Cloud-specific incidents, e.g., a widespread authentication service failure, could have a 'butterfly effect' on multiple applications.[48] Operational resilience is key: banks need continuity plans (e.g. fallback systems or multi-region deployments), and regulators insist on rigorous testing of worst-case scenarios.

Security and data protection. Top cloud providers invest heavily in security, but the shared responsibility model means a bank is still responsible for securing its applications and data within the cloud. Inadequate access controls on cloud storage have led to data leaks in the past. Regulators expect strong encryption, isolation mechanisms, and monitoring, but cyber risk remains high, and banks' ability to 'see' into the provider's infrastructure to detect intrusions and audit security controls, though required in theory, is missing in practice. The US Treasury in 2023 highlighted this lack of transparency as the number one obstacle for banks managing cloud risk.[49]

Third-party governance. Cloud giants, due to their market power, may adopt a 'take-it-or-leave-it' approach with their European clients,[50] making it harder to adopt contractual safeguards, like audit rights or favourable exit options, or they may rely on sub-contractors (for networking, data storage, etc.) and complex chains of sub-providers, increasing complexity. Regulators insist on broad audit rights encompassing significant sub-contractors.

Compliance risk linked to GDPR. As discussed in point 4, fundamental legal differences between the US and EU frameworks make this an inescapable source of tension. Adding new rules like DORA makes cloud adoption legally more complex.[51]

Finally, **concentration risk** is a meta-risk affecting the entire industry,[52] which may morph into a systemic risk vector.

---

[46] Program on International Financial Systems, 'Cloud adoption in the financial sector and concentration risk' (April 2023), available at https://www.fsb.org/uploads/PIFS.pdf, accessed on 21 November 2025.

[47] UK Parliament, 'More than one month's worth of IT failures at major banks and building societies in the last two years' (6 March 2025), available at https://committees.parliament.uk/committee/158/treasury-committee/news/205611/more-than-one-months-worth-of-it-failures-at-major-banks-and-building-societies-in-the-last-two-years/, accessed on 21 November 2025.

[48] Hooman Shababi, 'The butterfly effect of technology: how various factors accelerate or hinder the arrival of technological singularity' (2025) Computer and Society, 1 – 20.

[49] US Department of the Treasury, 'Sector's adoption of Cloud services' (2023), available at https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf, accessed on 21 November 2025.

[50] White, note 124.

[51] European Central Bank, 'Comment on the ECB Guide on outsourcing cloud services to cloud service providers by Peter McGuigan' (July 2024), available at https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/cloudoutsourcing/ssm.cloudservices_comment_06.pdf, accessed on 21 November 2025..

[52] See note 130.

3.3. Regulatory and Supervisory Responses

European regulators have been proactive in addressing the risks of cloud outsourcing through guidelines, regulations, and supervisory oversight.

To start with, in 2017, the EBA issued its first recommendations on cloud outsourcing, which evolved into the **EBA Guidelines on Outsourcing Arrangements** of 2019.[53] Banks are required to duly perform pre-outsourcing risk assessments on prospective cloud providers and must contractually secure safeguards, including audit and access rights at the cloud provider's facilities. In addition, banks are required to develop recovery and contingency plans to transition off a cloud provider if needed. More explicitly, the ECB's cloud outsourcing guide asks banks to test worst-case scenarios.[54]

In July 2025, EBA published a **consultation**[55] (closed on 8 October 2025) on updated guidelines that aim to modernise the 2019 framework by extending its scope beyond credit institutions and investment firms to encompass payment institutions and other financial entities, reflecting the increased reliance on third-country providers a in non-cash payment systems.

Regulators have also set up notification and approval practices for the outsourcing of banks' critical functions to the cloud.

The **Digital Operational Resilience Act** entered into force in January 2025 and introduces direct oversight of critical third-party service providers, including big cloud computing firms. EBA, ESMA, and EIOPA have jointly designated certain tech providers as 'Critical ICT Third-Party Providers' (CTPPs) if deemed systematically important, subjecting them to their oversight, and according to the Oversight Guide for CTPPs[56] the supervisor shall perform annual risk assessments and set annual oversight plans for each critical provider, conducting inspections (on-site or remote) and thematic reviews, and may issue recommendations or orders to address vulnerabilities. EBA adjusted its original Guidelines on ICT risk to account for the fact that these are matters covered by DORA.[57] In parallel, however, the ECB issued a consultation to release already its final Cloud Outsourcing Guide.[58]

The fact that the ECB has already issued a guide on the point reflects the different supervisory mandates at play. The ECB's Cloud Outsourcing Guide applies immediately within the Single Supervisory Mechanism as supervisory expectations for significant institutions and therefore continue to shape operational practice, while the designation of CTPPs and the establishment of the Oversight Framework under DORA are still being operationalised. In other words, the ECB is providing guidance

---

[53] EBA, 'EBA Guidelines on Outsourcing Arrangements' (29 February 2019) EBA/2019/02, available at https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf, accessed on 21 November 2025.

[54] ECB, 'ECB guide on outsourcing cloud services to cloud service providers' (16 July 2025), available at https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides202507.en.pdf, accessed on 21 November 2025.

[55] EBA, 'Consultation paper on EBA Draft Guidelines on the sound management of third-party risk' (8 July 2025) – EBA/CP/2025/12.

[56] For the List of 19 ICT critical cervices providers, see supra footnote 25. For the oversight framework, see ESAs, 'Digital Operational Resilience Act (DORA): Oversight of critical third-party providers' (15 July 2025), available at https://www.eba.europa.eu/sites/default/files/2025-07/32044d65-455e-4fff-82d0-aa0d8ac2799f/JC%202025%2029%20%20DORA%20Oversight%20Guide.pdf, accessed on 21 November 2025.

[57] EBA, 'Guidelines amending Guidelines EBA/GL/2019/04 on ICT and security risk management' (11 February 2025) – EBA/GL/2025/02.

[58] See note 58.

to banks on how to manage cloud dependencies now, whereas EBA, ESMA, and EIOPA are still in the process of building the new oversight architecture for critical ICT providers under DORA. From a Banking Union scrutiny perspective, this sequencing is significant: the ECB is already influencing how institutions structure their cloud outsourcing frameworks, while the DORA oversight regime will only fully apply once critical providers are designated and oversight colleges become operational. The result is a staged transition in which the ECB supervisory expectations temporarily fill the gap pending the activation of DORA's direct oversight powers.

The Bank of England is similarly working on a regime to oversee critical cloud and technology providers for financial firms.[59]

3.4. Resilience Assessment and Strategic Implications

Given the banking sector's growing dependence on cloud services, regulators are developing disruption scenarios and resilience assessments to test and enhance readiness for outages, cyber-attacks, or even geopolitical events cutting off access to a cloud region. Banks, for their part, are expected to work on contingency planning (e.g., ECB Cloud Outsourcing Guidelines).

The resilience assessment also covers more **specific scenarios**. For example, data loss and recovery: if a bug in a cloud database service led to data corruption, does the bank have near-real-time replicas? Or network outage scenarios: if an internet backbone issue severed connectivity to the cloud can the bank re-route traffic or maintain some operations offline? In the CrowdStrike episode, it was the homonymous security vendor's misconfiguration that propagated through a cloud update causing system outages at some banks,[60] showing that even ancillary services can trigger disruptions. Banks are therefore broadening their scenario planning to include third-party failures.

Some large banks have adopted a multi-cloud strategy, distributing workloads across two or more providers; e.g., a bank might run its primary services on AWS and a secondary instance on Azure that it can activate in emergencies. This approach is complex and expensive, though, and regulators have not required all banks to use multiple clouds, but they do expect banks to carefully consider geographical concentration in their resilience planning. The ECB's cloud guide notes that resilience measures may include having multiple data centres in different locations, using hybrid cloud setups, or engaging multiple cloud providers.

Monitoring and early-warning capabilities are another aspect of resilience assessment. Banks are improving their monitoring of cloud services. Some even use real-time cloud outage alerts and synthetic transactions to detect cloud service degradation early. The faster an incident is detected; the sooner mitigation steps can start. Regulators in accordance with DORA also require significant incidents to be reported to authorities within tight timelines.

---

[59] Bank of England, 'Operational resilience: critical third parties to the UK financial sector' (12 November 2024) PS16/24, available at https://www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-policy-statement, accessed on 21 November 2025.

[60] BBC News, 'CrowdStrike and Microsoft: What we Know about Global IT Outage' (19 July 2024), available at https://www.bbc.co.uk/news/articles/cp4wnrxqlewo, accessed on 21 November 2025.

Whilst there are no easy fixes, the previous analysis suggests some actions:

- **Strengthen transparency and collaboration clients/cloud providers**: cloud service providers should be more transparent on their resiliency and security protocols; e.g., CSPs may be required to offer detailed information on their service architecture (dependencies between data centres, failover mechanisms, etc.) and promptly share root cause analysis reports for any major incidents.
- **Avoid one-size-fits-all mandates (e.g. on multi-cloud) and promote risk-based strategies**. Concentration is a real concern, but mandating every financial institution to use multiple cloud providers would likely be disproportionate. Regulators should, however, insist that banks consider alternatives (multi cloud or hybrid solutions depending on risks analysis tailored to each specific situation) and focus on outcomes, namely resilience and recoverability.
- **Maximum Harmonisation for regulatory requirements.** Banks operating in multiple member states face a patchwork of national expectations and duplicative notification processes when moving to the cloud. This could be better harmonised under DORA's umbrella (for example, using a common reporting format for cloud outsourcing registers and aligning timelines for pre-approval or notification across jurisdictions).
- **Enforce robust contractual and governance standards.** Model contract clauses for cloud services may be advisable and could be mandated.[61] Key provisions could include explicit customer audit and access rights to cloud facilities, notification and consent rights when CSPs engage sub-outsourcing (and termination rights if critical sub-contractors are deemed unsuitable), and commitments from CSPs on service level monitoring and reporting.
- **Invest in cloud expertise and operational resilience testing.** human capital is often the weakest link in technology transformations. Banks and supervisors must invest in developing cloud expertise. Training programs, cross-industry secondments, and regulator-led tech sprints could all help deepen the pool of knowledgeable professionals.
- **More than one approach leads to data sovereignty.** Not only broad data localisation mandates, but also technical safeguards such as encryption and anonymisation for sensitive data in the cloud can ensure effective data sovereignty. The EU could also implement a certification (e.g. under the upcoming EU Cloud Security Certification Scheme) for cloud services that meet stringent sovereignty criteria.
- **Enhance systemic oversight and crisis management protocols for cloud incidents**: clear incident response protocols for scenarios where a major cloud provider faces an outage or cyber-attack should be in place. This might include real-time-information-sharing arrangements between the provider, the bank and the supervisor, contingency measures, and public communication strategies to maintain confidence. The creation of the Oversight Forum under DORA, which bring together various regulators to prioritise actions for critical providers, is a good step forward.

[61] Mike Pierides, Charlotte Cavendish, James Mulligan, 'Coalition of European Banks Calls for Model Cloud Service Terms' (14 June 2021) Morgan Lewis, available at https://www.morganlewis.com/blogs/sourcingatmorganlewis/2021/06/coalition-of-european-banks-calls-for-model-cloud-services-terms, accessed on 21 November 2025.

3.5. Relocation policies?

Although the preferred, and **more realistic** solution, lies in **risk management**, EU policymakers may want to know **all** the range of options, **including relocation policies**, i.e., a requirement that certain functions be located within the European Union, should a scenario of unplugging by foreign cloud providers or card networks become less remote.

Regarding **ICT services**, an analysis of **DORA** offers mixed results. On one hand, financial entities can only make use of "critical" ICT third-party service providers established in third countries if these have established a subsidiary within the EU,[62] which already imposes a 'location' policy. On the other hand, DORA's recitals stress that this does not prevent the third party from providing services and technical support from facilities and infrastructure outside the Union, anywhere in the World, and that DORA does not impose a data location policy.[63] The ability of the Lead Overseer to conduct supervision outside the Union is based on cooperation arrangements,[64] and only if the Lead Overseer is unable to conduct the envisaged oversight activities can it exercise its powers based on the facts and documents available to it, and document and explain the consequences of this inability, and take these consequences into consideration for its recommendations.[65] Thus, this is conceived as an *ex post* remedy, in case it is not possible to conduct supervisory activities. Its use as an *ex ante* risk assessment tool, to, e.g., demand that certain services be rendered from inside the EU may be difficult. This is also complicated by the fact that DORA relies on financial institutions to conduct the risk assessment, leaving them flexibility, a framework where a direct request by competent authorities, or Lead Overseer, to provide certain services from inside the Union, does not sit well. The same reasoning would apply to card networks, should they be considered ICT services under DORA.

In **practical terms** it means that even if data storage or processing is physically located inside the EU, many key components such as software update pipelines, authentication modules, management consoles, remain governed by non-EU legal systems and intellectual property. Location therefore does not guarantee sovereignty unless control extends across the full operational stack.

Furthermore, if card networks are considered as payment arrangements, and not ICT services, in principle the legal basis would be a finding under the ECB's PISA framework that they pose one or more of the risks envisaged in the framework (including legal or operational risk), followed by a location decision, or policy. This decision would surely be challenged. There is a precedent, when the Eurosystem Oversight Policy Framework contemplated the location of Central Counterparties (CCPs) within the euro area. This was challenged before the General Court, which then annulled the location requirement.[66] However, the reason was that the ESCB's mandate is "to promote the smooth operation of payment systems" (Article 127 (2) 4th TFEU), and the ECB's competence to "make regulations, to ensure efficient and sound clearing and payment systems within the Union and with other countries"

---

62 Article 31 (12) DORA. The list of critical ICT services providers (see *supra* fn. 25) refers to the EU includes the EU subsidiaries.

63 Recitals (82), (83) DORA.

64 Article 36 (2) DORA.

65 Article 36 (3), and 35 (1) (d) DORA.

66 Judgment of the General Court of 4 March 2015, case T-496/11 United Kingdom and others v ECB, EU:T:2015:133.

(Article 22 of the ESCB/ECB Statute) did not encompass securities settlement systems). Although the ECB would, for sure, be confronted with arguments that card networks are not "payment systems", it could argue that their role is fundamental for the "smooth operation" of said payment systems. A different matter is whether any decision on this front would pass the scrutiny of European Courts under the principles such as proportionality, or the duty to state reasons.[67] It would very much depend on the context, and the way any decision was to be adopted, and justified.

Hence, mandating relocation of cloud workloads or payment-processing functionalities would require multi-year restructuring across the financial sector. Lessons from past transitions (PSD2, cloud migrations) show that such transformations introduce their own operational fragilities. A rigid location policy could therefore reduce rather than enhance resilience during long transition windows. In fact, a forced shift to a small pool of EU-based providers may inadvertently increase systemic concentration. If most EU institutions converge on the same limited set of local providers, a single outage or cyber incident could have disproportionate effect. Divarication across jurisdictions and architectures is often a more robust resilient strategy than localisation. Rather than geographic mandates, authorities could require:

- EU-controlled encryption key management;
- contractual "kill switches' immune to foreign orders;
- local EU-based audit and incident-response mirrors;
- supervisory stress-tests specifically covering conflicts of laws;
- technical separation between EU-regulated workloads and foreign-governed support services.

These mechanisms target the underlying risks – loss of control – without imposing rigid geographic constraints.

[67] See M. Lamandini, D. Ramos-Muñoz *Finance, Law and the Courts. Financial Disputes and Adjudication*, OUP, 2023, chapter 6.

4. DATA PRIVACY CHALLENGES

Payment and financial services rely on intense data flows, which create tensions between the EU General Data Protection Regulation (GDPR) and other countries' (notably US') laws on national security. This section briefly discusses the EU legal framework and uses the *Schrems II* judgment as an example of the problem (4.1.), discusses subsequent legal developments and unsolved tensions (4.2.) and provides a brief analysis of plausible scenarios (4.3.)

4.1. Cross-Border Data Transfers under GDPR, and the *Schrems II* judgment

The EU GDPR promotes the adoption of EU-like rules internationally as a condition to receive Europeans' data. Chapter V of the GDPR (Articles 44 – 49) prohibits exporting personal data to third countries unless there are adequate privacy safeguards. The general principle is that any transfer must maintain compliance with the Regulation's requirements regardless of destination (Article 44 GDPR). Unrestricted data transfers may occur if the **EU Commission** issues an **'adequacy' decision** (Article 45 GDPR) about third country laws' 'essential equivalence' to EU standards, after assessing data subject rights, oversight authorities, and available remedies. The Commission issued adequacy decisions (Article 45 GDPR) for Switzerland, Japan, New Zealand, and the US, resulting in the *Schrems* litigation (discussed below).

Absent a finding of **adequacy**, data exporters must rely on **approved safeguards** (Article 46 of GDPR), such as (i) the European Commission's Standard Contractual Clauses (**SCCs**), a template data protection clause to be signed between EU data exporters and foreign importers, with duties on data security, purpose limitation, and sub-processor controls, as well as legal remedies for EU individuals, (ii) Binding Corporate Rules (**BCRs**), which are internal codes of conduct approved by EU Data protection authorities, governing intra-group transfers, or (iii) approved codes of conduct or certification schemes (less common in practice).

Absent an **adequacy decision or appropriate safeguards** there can be **case by case derogations** (Article 49 of GDPR), e.g., if the individual explicitly consents after being informed of the risks, if the transfer is necessary for a contract's performance, or for reasons of public interest, e.g. international cooperation on tax or competition enforcement, or to exercise legal claims or to protect an individual's vital interests. Such transfers must be 'occasional and necessary',[68] and thus interpreted narrowly, though.

Data transfers to the United States were initially authorised by the **EU-US Privacy Shield**, a Commission adequacy decision (2016/1250) to enable transfers to US companies that self-certified to a set of privacy principles. In the ***Schrems II*** decision (*Data Protection Commissioner v. Facebook Ireland & Schrems* (case C-311/18[69])) the Court of Justice invalidated the Privacy Shield, finding that US surveillance laws, e.g., Section 702 of the FISA and Executive Order 12333 (US) granted US government agencies access to Europeans' data without constraints based on proportionality or

[68] Recital (11) GDPR.

[69] Judgment of the Court, 16 July 2020 (Grand Chamber) EU:C:2020:559.

necessity. Furthermore, Europeans lacked the ability to challenge such data accesses in court. An ombudsperson mechanism created by Privacy Shield was deemed inadequate because it was not independent nor vested with effective powers to remedy abuses. Both fell short of the 'essential equivalence' standard.

The Court's annulment of the Privacy Shield **removed the legal basis** for over 5,000 companies' data imports. This had been in place for four years, since the *Schrems I* decision[70] in 2015 struck down the Safe Harbor Framework of 2000[71] on similar grounds. Companies had to pivot overnight to alternative transfer tools, e.g., SCCs were updated in 2021,[72] or to specific derogations. The Court accepted SCCs as viable, with caveats, e.g., data exporters and importers had to verify whether the receiving country's laws allowed compliance with SCC commitments, and if government interference breached the SCCs' guarantees, the parties should adopt additional safeguards. European Data Protection Authorities' guidance stressed this message too,[73] warning that transfers of sensitive data for cloud services might have to be paused or re-routed if no effective safeguards could be ensured in the destination country.

***Schrems II* highlighted the tension between EU privacy versus US security**. Assurances short of legally binding solutions fell short of the Court's standard, forcing the parties back to the negotiation table for the third time in two decades, and prompting a global re-thinking of data transfer compliance.

4.2. The EU-US Data Privacy Framework, and the unsolved tension between privacy and surveillance access

In the wake of *Schrems II*, EU and US officials restarted negotiations, culminating in the **EU-US Data Privacy Framework** (**DPF**), formally adopted by the European Commission in July 2023 as a new adequacy decision. US Executive Order 14086, signed by President Biden in October 2022 and accompanying regulations pledged to bind US intelligence agencies to new limitations, e.g., signals intelligence activities would be conducted only to the extent **'necessary and proportionate'** to defined national security objectives, procedures would be established to ensure compliance with these limits, and the US Privacy and Civil Liberties Oversight Board would monitor intelligence agencies' adherence.

Commercially, the DPF, like the former Privacy Shield is based on **companies' self-certification** to the Department of Commerce, and the **principles** remain **largely the same** (e.g. purpose limitation, data integrity, security, transparency, etc.), with some updated definitions and requirements, and enforcement by the US Federal Trade Commission or Department of Transportation, while the Department of Commerce monitors participants' privacy practices. Annual US-EU joint reviews are foreseen to verify compliance.

---

[70] Maximillian Schrems v Data Protection Commissioner, case C-362/14, judgment of 6 October 2015 (Grand Chamber), EU:C:2015:650

[71] Decision 2020/520/EC of the Commission of 26 July 2000 pursuant to Parliament and Council Directive 95/46/EC on the adequacy of the protection provided by Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

[72] European Commission, 'Commission implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council' (4 June 2021).

[73] European Data Protection Board, 'Guidelines 02/2024 on Article 48 GDPR Version 2.1 Adopted on 4 June 2025' (4 June 2025).

The agreement is **still vulnerable**. The 'necessary and proportionate' language is now official policy. Only time will tell whether it will also be part of intelligence agencies' actual practice. Broad national security objectives could continue to justify bulk data collection. Basic statutes have not changed. It remains to be seen if this good faith attempt at compromise may in the end withstand possible future legal scrutiny.

The reason is a **long, deep-seated tension** between the relative weights of privacy and national security in the US and the EU. Already after 9/11 US Treasury subpoenas to obtain European financial messaging data (SWIFT -based) to track terrorist financing[74] raised alarms in the EU about bulk transfer of Europeans' banking data to US authorities without privacy guarantees, eventually resulting in an EU-US agreement (TFTP) with stricter safeguards. Currently, Article 48 GDPR forbids EU companies from disclosing such data to foreign governments or courts unless under an international agreement or an EU law. This limits the use of US subpoenas or regulatory orders as a *carte blanche* to extract EU personal data but can lead to stalemates. US authorities may reciprocate, refusing to share the data needed by EU banking and payments supervisors, hindering cooperation, e.g., on Anti-Money Laundering (AML).

As it can be seen, Schrems-type annulments are often treated as narrow compliance issues, but for the payments ecosystem they constitute a systemic operational risk. A sudden invalidation of a transfer mechanism can trigger sector-wide contractual remediation, service disruptions, supervisory uncertainty, and emergency technical workarounds comparable to a cyber incident.

4.3. Scenario analysis: Managing the Tension v Precipitating a Collision

Banks, payment providers, and other financial institutions handle sensitive personal data (account holder information, transaction records, KYC data) subject to privacy laws and essential for supervisory purposes. Much of this data is processed cross-border. **EU authorities must ensure access to data, and respect for safeguards**. This can be tricky when other authorities are involved.

Starting with **access**, EU authorities have insisted on access rights clauses. The European Central Bank's outsourcing guidelines require outsourcing agreement (e.g. with cloud providers) to allow the bank and its supervisors to inspect and audit relevant data and systems, even if located abroad.[75] DORA places certain critical ICT service providers under direct EU oversight, subject to inspections, on-site visits, and information requests by the ESAs. Firms are encouraged or required to maintain data localisation or mirroring to keep key records within the EU. EU data protection authorities have recognised regulators' legitimate interest to access personal data in financial records. It is, however, too soon to tell whether these mechanisms will suffice to ensure access and close any gaps, and how non-EU authorities may react.

---

[74] Council of the European Union, 'Processing and protection of personal data subpoenaed by the Treasury Department from the US based operation centre of the Society of Worldwide Interbank Financial Telecommunication (SWIFT)' (28 June 2007) Press 157, available at https://data.consilium.europa.eu/doc/document/ST-11291-2007-REV-2/en/pdf, accessed on 21 November 2025.

[75] ECB, note 138.

On **safeguards**, GDPR's Article 48 can be a broad 'blocking statute' against extra-territorial data demands, e.g., of EU-resident customers' data, or EU subsidiaries of non-EU banks. The question is how to move from this baseline. Regulatory cooperation is key. If non-EU authorities submit requests via European regulators rather than directly to the company, this would sidestep Article 48, since access would be governed by EU law. Sectoral laws and agreements may include data-sharing gateways.

However, **differences of principle are 'sticky'**, and not every situation can be anticipated. US-based hyperscalers, on which EU institutions depend for payments' real-time processing, clearing, and settlement, are subject to FISA or Executive Order 12333. US intelligence and law enforcement agencies could demand from cloud service providers access to payment transaction records and user account metadata of European users without clear remedies for such users under the EU privacy legal framework. Indeed, even if this is incompatible with EU privacy laws, between a rock and a hard place, hyperscalers may prefer compliance with US national security law rather than EU privacy obligations.

Therefore, a collapse of the current adequacy framework would not only undermine GDPR compliance; it would immediately complicate DORA requirements concerning auditability, oversight access, and the enforceability of exit strategies. Institutions may find themselves simultaneously non-compliant with GDPR and unable to meet DORA's risk management obligations. As it can be seen, EU institutions relying on US cloud providers face "dual exposure": EU law prohibits unauthorised governmental access, while US law may require cloud providers to grant it. Contracts cannot fully resolve this structural conflict.

For payment systems – which depend on continuous, legally compliant real-time data handling – this incompatibility represents a persistent, non-mitigable risk factor. It necessarily follows that from a DORA perspective, the issue is not the governmental access request itself, but the resulting uncertainty as to whether a financial entity can continue to guarantee the confidentiality and integrity of its ICT systems and data. In this sense, the vulnerability is not a service outage, but the legal and operational exposure arising when a firm cannot be certain that it can uphold EU-mandated safeguards while using extra-territorial could infrastructure. Furthermore, DORA assumes that ICT risks must be managed, mitigated, or ultimately eliminated where necessary to maintain operational resilience. This may include, in certain cases, exercising termination or exit rights where a provider can no longer guarantee compliance with EU confidentiality and access-governance requirements. However, if all viable alternative providers are subject to the same extra-territorial legal constraints, termination does not itself resolve the systemic exposure; it simply displaces it.

As it can be seen, there is **no easy way out** of this dilemma. DORA assumes that vulnerabilities are handled, not endured. An unsolvable clash of unyielding legal principles is hard to fit in this framework. Furthermore, **contracts** must ensure termination rights in case of breaches of law, regulations or contract terms by ICT providers, but if the replacement entity is affected by the same legal challenges (because they are all in the US) there is no clear answer. Thus, some regulators and policymakers now advocate for **digital sovereignty** measures, such as favouring EU-based cloud infrastructure, restricting sensitive data transfers entirely, or requiring data mirroring within EU borders. This reflects not an assumption that EU-based solutions are technologically inferior, but rather than governance

certainty – knowing which legal framework ultimately controls the data – is itself a component of operational resilience under DORA.

In conclusion, privacy considerations are as central to the strategic outlook for EU payments' data flows as they are hard to solve. The core challenge is not performance, but control: who defines the legal conditions under which critical financial data may be accessed. Authorities should deepen their cooperation as a matter of practice. If US authorities can be restrained in their requests for data involving European citizens and residents, and ideally channel them through EU authorities, and these can, in their turn, be swift and responsive, the clash of principles may not arise. Furthermore, given the likelihood of renewed litigation against the EU-US Data Privacy Framework, financial institutions should adopt layered contingency architectures: EU-located encrypted replicas for high-sensitivity payment data, technical separation of workloads, and flexible routing arrangements to localise sensitive flows in the event of invalidation.

5. HOMEGROWN ALTERNATIVES: CHALLENGES, COMPARATIVE CASES, AND THE DIGITAL EURO

The euro area payments system is open to external dependencies. DORA tries to mitigate risks by insisting on preparedness and resilience, but its functioning is still ongoing and uncertain, and some tensions cannot be eliminated, e.g., on data privacy. Thus, one question is whether homegrown alternatives can be a solution. First, we discuss the limitations of homegrown alternatives in cloud services, which are central for financial institutions (5.1.). Next, we discuss the EU's gradual development of homegrown payment infrastructures, which, however, stop short of full-blown payments systems (5.2.). Then, we look at the experiences of homegrown payment systems in China, India or Brazil (5.3.).We use these experiences to draw some lessons for a potential European *payments* solution, and the challenges it would face (5.4.). Finally, we analyse the Digital Euro project as an end in itself, which goes beyond *payments*, and will encounter challenges, and as a means to use a broader mandate to promote a European payments ecosystem (5.5.).

5.1. Sovereignty in the Cloud, and its Limits

If market concentration on few non-EU cloud service providers is a source of concern, an alternative may be to promote **EU cloud solutions**. Alas, this is easier said than done. Gaia-X, unveiled in 2020 by France and Germany was conceived as a federated ecosystem or set of standards that would allow European cloud and data services to interoperate seamlessly under common rules on data portability, security, and transparency. However, Gaia-X has encountered **significant obstacles**: the initiative grew to include hundreds of members, yet disagreements emerged on fundamental issues and, as of 2025, Gaia-X has had a quite minimal impact.

Other examples, like the '*Cloud de Confiance*' (trusted cloud) initiative, led to partnerships like Bleu, a joint venture between Orange and Capgemini and Microsoft,[76] which provides Azure's cloud technology and software hosted in France by a locally owned entity, with data stored in-country and strict controls to prevent data access by non-French authorities. Microsoft has no direct access to the data in Bleu's cloud. In turn, Thales launched in France a joint venture with Google called 'S3NS' to offer Google's cloud services in a way that meets French requirements (with encryption and local oversight),[77] while,

[76] Capgemini, 'Capgemini and Orange are pleased to announce the launch of commercial activities of Blue, their future "cloud de confiance"' (15 January 2024), available at https://prod.ucwe.capgemini.com/wp-content/uploads/2024/01/2024_01_15_Launch-of-Bleus-commercial-activities.pdf, accessed on 21 November 2025.

[77] Thales, 'Thales introduces S3NS in partnership with Google Cloud and unveils its offering in a first step towards the French trusted cloud label' (30 June 2022), available at https://www.thalesgroup.com/en/group/press_release/thales-introduces-s3ns-partnership-google-cloud-and-unveils-its-offering-first, accessed on 21 November 2025.

in Germany, Deutsche Telekom's T-Systems partnered with Google Cloud[78] and in Italy, reportedly, there are plans and ongoing initiatives for a national cloud for government data.[79]

However, sovereign cloud initiatives face the challenge of **scale and cost**, which far exceed current public investments, or market demand, since private-sector users are reluctant to pay a premium or accept lower performance for a 'home-grown' service, even leaving aside switching costs.

And there is, still, a **technical gap**. Cloud computing is not just about owning servers; it is about cutting-edge software automation, global networks, and an ecosystem of developers. European providers like OVHcloud or Scaleway can offer basic cloud infrastructure, but they trail in offering the breadth of services (e.g. AI platforms, serverless computing, etc.) that US incumbents do. That's why many banks may still opt for solutions like client-side encryption on US servers(?), wherein they encrypt data with keys that they (the customer) hold, before storing it in a public cloud. Client-side encryption can ensure that even if a cloud provider were coerced to hand over data, the data would be unintelligible without the customer's key.

This example faces the EU with a **hard truth**: Europe lost the first wave of digital innovation, and is set to lose another, due to a lack of financing of late-stage projects,[80] and even more, due to regulatory barriers (proliferation, fragmentation, and burdens). Specific solutions via industrial policy will not solve the main problem, which lies in Europe's insufficient zeal to deepen the Single Market in digital services.

5.2. European initiatives on payments *infrastructures*

Leaving aside services that are very important to, but are not themselves, payments systems, Europe has also considered or promoted initiatives on payment infrastructures. These offer varying degrees of promise.

On **messaging** and communications, SWIFT looks hard to replace entirely, given its global reach. However, it is positive to assess vulnerabilities, and consider investment in complementary networks or agreements, e.g., leveraging ISO 200022 messaging standards, not to prepare for a shutdown, but perhaps to strengthen the EU's hand in a future negotiation or standoff.

On payment **infrastructures**, the ECB and national central banks have developed the TARGET clearing and settlement system into TARGET 2 / TARGET 2 Securities (T2/T2S), adding a new function for retail payments (TIPS) and showing that they can work efficiently with large volumes (see Annex 6.2). However, these are **"backstage" infrastructures**, whereas the **users'** leg (especially the retail users' leg) of the system relies on payment schemes like **card networks**. The joint effort by EU institutions as regulators, and the banking industry support, through the European Payments' Council (**EPC**) resulted

[78] T-Systems, 'T-Systems Sovereign Cloud Powered by Google Cloud', available at https://www.t-systems.com/de/en/sovereign-cloud/solutions/sovereign-cloud-powered-by-google-cloud#:~:text=The%20T%2DSystems%20Sovereign%20Cloud,cloud%20functionality%20of%20a%20hyperscaler., accessed on 21 November 2025.

[79] Ivan Cimmarusti, 'Digital Sovereignty: Europe divided in the cloud, Italy protects sensitive data' (25 May 2025) Il SOLE 24 ORE, available at https://en.ilsole24ore.com/art/digital-sovereignty-europe-divided-cloud-italy-protects-sensitive-data-AH47xsv?refresh_ce=1, accessed 21 November 2025.

[80] Draghi Report, pp. 24, 30, 34.

in the SEPA Credit Transfer (**SCT**) and Instant Credit Transfer (SCT Inst), which can compete in speed with card payments. However, they are transfer-based means of payment resulting from a regulatory obligation. Transfers still represent a minority of euro area payments.[81] Their ease of use and user experience (based on IBAN numbers, as opposed to tapping a card or phone) do not yet appear as a substitute to, e.g., card-based payments.

The idea of **Euro-based cards** is not new, and it gained new momentum in 2020, when a consortium of European banks pursued the European Payments Initiative (EPI; branded "Wero"),[82] a unified card and digital wallet system, with a pilot program for an instant account-to-account payment wallet in France and Germany,[83] which was welcomed by the ECB.[84] However, creating a viable alternative to existing card schemes requires large investments and wide membership, and the initiative has so far **failed to take off**, and does not offer card-based solutions.

5.3. Homegrown retail payments initiatives in China (UnionPay), India (UPI) and Brazil (PIX)

Europe has successfully developed several schemes for payments infrastructures, while stopping short of a full-blown system for retail payments. To assess the feasibility of such a project, we discuss some of the world's most notable examples in China (UnionPay), India (UPI) and Brazil (PIX).

UnionPay is the dominant card network in China, and the largest card scheme in the world by users and by transaction volume.[85] UnionPay was created in 2002 with approval of the People's Bank of China (PBoC) and the State Council and owned by a consortium of shareholders including large state-owned commercial banks (e.g. ICBC, China Construction Bank) plus smaller credit institutions. The government role was strong, and UnionPay was granted a legal monopoly for domestic bank card clearing, which, though subsequently eliminated,[86] ensured the card network's widespread acceptance and dominant position. Internationally, UnionPay has partnered with thousands of overseas institutions, but a large majority of its transactions occur inside China, or in Asia-pacific and tourist regions. Initially touted as an alternative to Visa and Mastercard in Russia after those left the country, some Chinese

---

81 Card payments accounted for 57% of payments in the euro area, credit transfers for 21%, direct debits for 15%, and e-money payments for 6%. See https://www.ecb.europa.eu/press/stats/paysec/html/index.en.html, accessed on 21 November 2025.

82 Ewald Judt, Malte Krueger, 'The European Payment Initiative: the next big thing in European payments?' (2021) 15 (3) Journal of Payments Strategy and Systems, 319 – 331.

83 Anthony Maymont, 'Les ambitions de l'European Payments Initiative' (2021) 5 Contracts, Concurrence, Consommation; Huw Jones, 'More banks join European instant payments pilot from end 2023' (25 April 2023) Reuters, available at https://www.reuters.com/technology/more-banks-join-european-instant-payments-pilot-end-2023-2023-04-25/#:~:text=EPI%2C%20which%20had%20appealed%20for,account%20payments%20across%20European%20countries, accessed on 21 November 2025.

84 European Central Bank, 'ECB welcomes the EPI's progress on building a European payment solution' (23 April 2023) MIP News, available at https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews230425.en.html#:~:text=With%20this%20step%2C%20in%202023,and%20covering%20multiple%20use%20cases, accessed on 21 November 2025.

85 The Economist "National payment systems are proliferating". 3 May 2024. See https://www.economist.com/special-report/2024/05/03/national-payment-systems-are-proliferating, accessed on 21 November 2025.

86 This was also a result of the findings by an WTO dispute settlement body. See DS413 China — Certain Measures Affecting Electronic Payment Services. Available at: https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds413_e.htm, accessed on 21 November 2025.

banks and mobile operators stopped accepting UnionPay cards to avoid sanctions.[87] UnionPay developed Cloud Quick Pass for digital payments. In this area it coexists with AliPay, the main digital payments solution for mobile and online platform payments in China, owned by Ant Financial, and accepted by 80-90 million merchants in the World.[88]

Chinese retail payments form part of a broader ecosystem of settlement, financing and messaging, where the push to de-dollarize transactions by Chinese institutions, and foreign trade in general, has only accelerated in recent times. China has dramatically increased the share of its currency in its own trade in goods and services, and its inbound payments,[89] Chinese banks have drastically reduced their dollar-denominated lending abroad, resulting in a notable decrease of cross-border dollar lending to emerging economies (EMEs),[90] the PBoC has expanded access to renminbi swap lines for other central banks,[91]and China promotes its CIPS messaging system as an alternative to SWIFT.[92]

The **Unified Payments Interface (UPI) is** operated in **India** by the National Payments Corporation of India (NPCI), a Section-8 (not-for-profit) industry utility created and capitalized by a consortium of banks, with the guidance of the Reserve Bank of India (RBI) and the Indian Banks' Association (IBA), which acts as the retail-payments infrastructure provider, publishing product rules and PFMI disclosures, while operational governance remains bank-led but subject to RBI oversight.[93] The UPI processes tens of billions of transactions per year, making UPI a dominant retail rail in India.[94]

---

87 UnionPay physical cards could be used, at least initially, as they were linked to the MIR system. China Deals Major Blow to Russia with Payments Ban. *Newsweek*. 28 February 2024. Available at: https://www.newsweek.com/china-russia-unionpay-huawei-pay-sanctions-1874226, accessed on 21 November 2025. The assessment by these firms is unclear. "Primary" sanctions are imposed on the specific country affected and its nationals and entities. "Secondary" sanctions can be imposed on the sanctioning country's nationals or companies for dealing with the sanctioned country's nationals or companies. See John Forrer 'Secondary Economic Sanctions: Effective Policy or Risky Business?' Atlantic Council. May 2018. Thus, the legal assessment by Chinese companies operating in Russia is not entirely clear but seems to have followed a warning by the Chinese government. See Nicholas Gordon 'Visa and Mastercard have already cut ties with Russian banks. Now China's largest credit card brand might be pulling out too' *Fortune,* April 22, 2022. Available at: https://fortune.com/2022/04/22/unionpay-china-credit-card-sberbank-secondary-sanctions-russia/, accessed on 21 November 2025.

88 The Digital Banker "More than 90 million Global Merchants Leverage Alipay+ Payment and Digitalisation Solutions to Attract and Engage Travellers this Chinese New Year", 3 February 2025. Available at: https://thedigitalbanker.com/more-than-90-million-global-merchants-leverage-alipay-payment-and-digitalisation-solutions-to-attract-and-engage-travellers-this-chinese-new-year/#:~:text=Alipay+%20supports%20over%2035%20international,users%20to%20its%20global%20merchants, accessed on 21 November 2025.

89 The Economist "China is ditching the dollar, fast" 10 September 2025, available at: https://www.economist.com/china/2025/09/10/china-is-ditching-the-dollar-fast, accessed on 21 November 2025.

90 Laurie DeMarco; Joshua Walker "Chinese Banks' Dollar Lending Decline", FEDS. Notes, May 16, 2025. Available at: https://www.federalreserve.gov/econres/notes/feds-notes/chinese-banks-dollar-lending-decline-20250516.html, accessed on https://www.economist.com/china/2025/09/10/china-is-ditching-the-dollar-fast

91 Julian Watrous; Stephen Paduano "The Lender of First Resort? Chinese Swap Lines, the IMF and the Changing International Financial Architecture" GCI Working Paper 042 04/2025. Available at: https://www.bu.edu/gdp/files/2025/04/GCI-WP-42-PBOC-Swap-Lines-FIN.pdf, accessed on 21 November 2025.

92 Martin Chorzempa; Lukas Spielberger "Significant, but not Systemic: The Challenge of China's Efforts to Rival Western Financial Predominance" CSDS Policy Brief 11/2025. Available at: https://csds.vub.be/publication/significant-but-not-systemic-the-challenge-of-chinas-efforts-to-rival-western-financial-predominance/#:~:text=The%20powers%20the%20dollar%20bestows,use%20in%20cross%2Dborder%20activity, accessed on 21 November 2025. See also Joe Baker "Is China's cross-border payments network on the rise?" FXC Intelligence, 4 July 2025. Available at: https://www.fxcintel.com/research/analysis/cips-growth-may-2025, accessed on 21 November 2025.

93 https://www.website.npci.org.in/purpose-value, accessed on 21 November 2025. See also Jazira Asanova; Yonghwi Kwon; Pratyush; John Owens "Leveraging Lessons Learned from India's Unified Payments Interface for Digital Transformation in Asia and the Pacific" ADB briefs, no. 299, April 2024.

94 https://www.npci.org.in/what-we-do/upi/product-statistics, accessed on 21 November 2025

This is due to some of **UPI's features**. First, participation by banks is voluntary, but NPCI being industry owned, there is a strong incentive to enter; and participation is also open to authorised non-bank payment service providers that meet NPCI/RBI criteria, while commercial banks can and do sponsor many smaller providers through sponsorship/aggregator models, enabling fintech PSPs to participate.[95] Second, UPI is suited to mobile payments: users need a basic bank or regulated payment account and device/app, and they transfer money between accounts via apps or QR codes using a Virtual Payment Address (VPA) or identifier (mobile/Email/ID). Third, near-zero consumer fees for most P2P transfers, and measures like merchant discount rate (MDR) for small merchants[96] incentivize onboarding. This is linked to the aim to use UPI to promote financial inclusion: governments and PSPs used UPI to distribute social transfers and pensions, driving formal financial activity.

NPCI's international arm (NIPL) exports UPI/RuPay via merchant acceptance partnerships and bilateral linkages, showing some successes, like the UPI–PayNow corridor with Singapore,[97] or a merchant acceptance pilot with the UAE. Broader global deployment requires deeper engagement by local regulators and acquirers. UPI has performed reliably, but there were episodic outages and latency incidents in 2025.[98] There have also been some UPI-targeted scams and social-engineering frauds,[99] prompting technical and regulatory tightening, as it is dependent on participant bank safeguards.

PIX is Brazil's instant retail-payment scheme operated via Brazil's Instant Payments System (SPI) under the Central Bank of Brazil (Banco Central do Brasil - BCB).[100] It has fast become the dominant retail payment mechanism, reaching 5.71 billion transactions settled in December 2024 and a total value settled in 2024 of R$ 22.12 trillion.[101] It is the most widespread form of non-cash payment, larger than credit and debit cards combined,[102] praised by different studies.[103]

---

95 Ibid.

96 See Advancing Cashless India ₹1,500 Cr Incentive Scheme for Low-Value BHIM-UPI Transactions. 24 March 2025 Available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2114335, accessed on 21 November 2025.

97 Major UPI Apps Enabled to Receive Remittances from Singapore via UPI-PayNow Linkage. 11 January 2024. Available at: https://www.npci.org.in/PDF/npci/press-releases/2024/Major-UPI-Apps-Enabled-to-Receive-Remittances-from-Singapore-via-UPI-PayNow-Linkage.pdf, accessed on 21 November 2025.

98 Tanusha Tiagi "UPI at Scale: Outages and the Push for Resilient Systems". 21 June 2025. Available at: https://www.orfonline.org/expert-speak/upi-at-scale-outages-and-the-push-for-resilient-systems#:~:text=The%2012%20April%202025%20outage,the%20system%20can%20gradually%20decline, accessed on 21 November 2025.

99 Unified Payments Interface (UPI) fraud cases surge by 85% in FY24: Ministry of Finance. 29 November 2024. Available at: https://visionias.in/current-affairs/news-today/2024-11-29/security/unified-payments-interface-upi-fraud-cases-surge-by-85-in-fy24-ministry-of-finance#:~:text=Since%202022%2D23%2C%20UPI%2D,as%20per%20RBI%20annual%20report, accessed on 21 November 2025.

100 Technically, PIX is the payments' scheme (rulebook), while the infrastructure is the SPI. Since both are operated by the central bank, we will use 'PIX' to refer to the whole system.

101 SPI Sistema de Pagamentos Instantâneo (Instant Payments System) Annual Report 2024. Available at: https://www.bcb.gov.br/content/financialstability/spi_annual_reports/SPI_2024.pdf, accessed on 21 November 2025.

102 The Economist "Brazil's government-run payments system has become dominant". 3 April 2025. Available at: https://www.economist.com/the-americas/2025/04/03/brazils-government-run-payments-system-has-become-dominant, accessed on 21 November 2025.

103 Matheus C Sampaio; Jose Renato H Ornelas Payment technology complementarities and their consequences on the banking sector: evidence from Brazil's Pix. BIS Papers No 152: Faster digital payments: global and regional perspectives. Available at: https://www.bis.org/publ/bppdf/bispap152.pdf, accessed on 21 November 2025.; International Monetary Fund (IMF) Pix: Brazil's

Success is due to **key design and institutional features**. First, it is open to commercial banks, regulated by the BCB, but also to non-banks, which are nonetheless subject to specific supervision as payment services providers.[104] Second, the largest institutions (> 500,000 active customer accounts) *are required* to participate in PIX ("mandatory participants") allowing a quick scale up of the system.[105] Third, PIX is **focused on consumers and businesses**. Users only need a transaction account (checking, savings or a regulated payment account) at a participating institution, where they may register one or more "PIX keys" (chave PIX) identifiers that map easily to accounts (CPF/CNPJ, mobile number, email, or a random key). Use of keys is easy and intuitive, apt for users with low digital literacy, and the user-facing UX is designed for mobile apps and internet banking. Payments without a key are also possible by supplying account details or via QR codes at point-of-sale. PIX integration by merchants is easy, and the BCB facilitates tools to improve user experience (e.g., reconciliation tools to compare the financial transactions in company records with bank records), FAQs or manuals.[106] Fourth, PIX was conceived under a **financial inclusion** objective and thus entails a zero fee for individuals and low-cost for merchants (lower than traditional card fees[107]). And the BCB and banks have been committed to steady innovation, offering new features, such as "PIX Automático", for (recurring payments), PIX for government transfers and tax collection, or simplified account types, e.g., for social-transfer recipients, small merchants and consumers without credit cards.

The system is reliable, but there were cyber-security incidents amongst ICT services providers and PSPs,[108] prompting the BCB to introduce incident-reporting rules, anti-fraud guidelines, transaction limits for non-authorised intermediaries, and consumer-protection measures (e.g., temporary holds on suspicious transfers).[109] A different threat came from the Trump Administration. The Office of the United States Trade Representative (USTR) opened a formal Section-301 style investigation[110] and senior U.S. officials publicly criticized PIX as an unfair, state-backed form of policy that disadvantages U.S. payment providers, and threatened coercive measures.[111] Although this may say less about PIX's features than about US-Brazil diplomatic relations, it illustrates the kind of challenges that homegrown payment systems may encounter, even when not sought.

Successful Instant Payment System, 31 July 2023. Available at: https://www.elibrary.imf.org/view/journals/002/2023/289/article-A004-en.xml, accessed on 21 November 2025.

104 IMF Pix: Brazil's Successful Instant Payment System, p. 55.

105 SPI Sistema de Pagamentos Instantâneo (Instant Payments System) Annual Report 2024 https://www.bcb.gov.br/content/financialstability/spi_annual_reports/SPI_2024.pdf, accessed on 21 November 2025.

106 https://www.bcb.gov.br/en/financialstability/, accessed on 21 November 2025.

107 SPI Sistema de Pagamentos Instantâneo (Instant Payments System) Annual Report 2024.

108 Ibid. See also https://www.bcb.gov.br/content/financialstability/spi_annual_reports/SPI_2024.pdf, accessed on 21 November 2025.

109 Central Bank publishes Resolution on information security incidents involving personal data in the PIX system. 4 de October de 2023. https://www.kasznarleonardos.com/en/central-bank-publishes-resolution-on-information-security-incidents-involving-personal-data-in-the-pix-system/, accessed on 21 November 2025.

110 Title III of the Trade Act of 1974 (Sections 301-310, 19 U.S.C. §§2411-2420) covers "Relief from Unfair Trade Practices," and is often collectively referred to as "Section 301."

111 "USTR Announces Initiation of Section 301 Investigation of Brazil's Unfair Trading Practices", July 15, 2025. Available at: https://ustr.gov/about/policy-offices/press-office/press-releases/2025/july/ustr-announces-initiation-section-301-investigation-brazils-unfair-trading-practices, accessed on 21 November 2025.

5.4. Lessons for European payments solutions

The previous examples offer **lessons for EU homegrown payments solutions** that can compete with existing card networks, although not all cases are equally useful.[112] China, with the dominance of state-owned banks,[113] and the initial monopoly of UnionPay on card settlement is less valid as a precedent. The ECB/ESCB would also find it difficult to give existing schemes, like the EPI, anything beyond vocal support under its mandate of "to promote the smooth operation of payment systems" (Article 127 (2) 4th TFEU). UPI and PIX offer more valuable lessons. Both are fast payment systems with a solid infrastructure and robust schemes (rulebooks), which invites optimism in the EU. The SEPA ICT is a reliable system, benefitting from a robust scheme, and can be a precedent for new payment mechanisms, while TIPS is a reliable interbank infrastructure, capable of handling large flows.

However, both UPI and PIX had a clear strategy to ensure widespread acceptance and user experience, with a **central role for the central bank and government institutions**. For **UPI**, the key was an **active partnership with the private sector**: users can use UPI apps, banks' mobile apps or any UPI-enabled app to make transactions, eliminating the need to maintain multiple accounts or download multiple apps.[114] Payment does not depend on full bank account numbers (as in SEPA); a mobile phone number or a QR code suffices. This model would still require a **hands-on approach** by the ECB and the Eurosystem, stretching the limits of a "catalyst" of private sector initiatives.[115] At the same time, allowing third-party applications means that Big Tech companies may become dominant, as Google Pay (US), and Phone Pe (India) did in India.[116] However, in case of disruption of those apps, a 'system' app (in India, the UPI app) can ensure a substitute. **PIX** shows a successful homegrown system with an **even stronger role for the central bank**, which operates the sole centralised alias database and the instant payments system, although private operators can provide transaction account services to end users, or settlement services to other participants.[117] The ESCB could probably not mandate participation by banks and other payment services providers under its mandate to "promote the smooth operation of payments systems" (Article 127 (2) 4th TFEU), and would also face criticism for "unfair" competition, which could turn into a legal challenge for acting against the principle of "an open market economy with free competition" (Articles 119 (1) and (2) and 127 (1) TFEU), as the Bank of Brazil has faced. The (policy) counter-argument could be that, by putting the ECB in charge of a robust

[112] We have not discussed the case of MIR, a Russian card scheme, because its development was prompted by the imposition of sanctions due to the invasion of Ukraine in 2014, and then its growth was also partly due to the decision in 2022 of Visa and Mastercard to pull out of the country. Our assumption is that any homegrown payments system in Europe would have to be developed facing the competition of Visa and Mastercard.

[113] The Industrial and Commercial Bank of China, the Agricultural Bank of China, China Construction Bank and Bank of China are the largest banks in the World by assets. See S&P market Intelligence. https://www.spglobal.com/market-intelligence/en/news-insights/articles/2025/4/the-worlds-largest-banks-by-assets-2025-88424232, accessed on 21 November 2025.

[114] Giulio Cornelli, Jon Frost, Leonardo Gambacorta, Sonalika Sinha, Robert M Townsend 'The organisation of digital payments in India – lessons from the Unified Payments Interface (UPI)' BIS Papers No 152: Faster digital payments: global and regional perspectives, 18 December 2024, p. 63.

[115] https://www.ecb.europa.eu/paym/integration/retail/ecb/html/index.en.html, accessed on 21 November 2025.

[116] Ibid, p. 64.

[117] Carlos Ragazzo and Lucas Caminha 'Central Banks as Regulators and (also) Operators of Instant Payments Schemes: Confronting the Criticisms of "Needless Intervention" and "Unfair Competition"' European Journal of Risk Regulation (2025), 16, 263–278.

infrastructure would allow private operators compete on products,[118] in fact enabling the growth of a new ecosystem. In legal terms, support could be given by combining a regulation adopted by the co-legislators to provide the regulatory mandate, while ECB Guidelines based on Article 127 (2) 4th and complementary SEPA rules could underpin the system itself. Still, it might be difficult to muster the political support for a payment solution.

UPI and PIX also suggest that any initiative should include banks and non-bank PSPs and should pay special attention to the social dimension. In India and Brazil, this was ensured by the emphasis on usability, and the zero or very low transaction fees.[119] On this, the EU already has a strong precedent in the Payments Account Directive, which codifies the right to a bank account.[120]

5.5. The Digital Euro and Payments: Ends and Means

In the EU, concerns about digital and financial resilience are mixed with concerns about monetary sovereignty, due to stablecoins, a form of privately issued crypto asset designed to maintain a stable value, often by pegging it to another asset, e.g., dollar-denominated assets. Stablecoins' risk is in their potential to disrupt the monetary system,[121] a concern that has increased with the US Genius Act, which provides a firmer basis for stablecoins.[122] All these perceived risks have given momentum to the Digital Euro,[123] a Central Bank Digital Currency (CBDC).

Central Bank Digital Currencies (CBDCs) can be a central bank liability, denominated in an existing unit of account, serving both as a medium of exchange and a store of value.[124] CBDCs can be 'wholesale', issued to clearing banks, to facilitate high-value inter-bank settlements, or 'retail', issued to the public. Retail CBDCs, in turn, can follow an 'indirect' or 'hybrid' model, where the central bank keeps a central ledger recording CBDC balances and processing payments, but commercial banks manage customer account services, or a 'direct' model, where the central bank takes over these steps. CBDCs can also be interest-bearing, and impose a cap on individual holdings, or not.[125] CBDCs differ from Fast Payment Systems (FSP) such as UPI, PIX or SEPA's ICT in the instrument, which is central bank money. Thus, while a FSP allows different governance options, in a CBDC, the central bank must operate key parts of the infrastructure and rulebook. While the relationship between FSPs and CBDCs

---

118 Ibid.

119 By way of example, in Brazil Lei 12,865 of 9 October 2013, which regulates payment institutions, expressly mentions 'financial inclusion' in its Article 7 VI as a guiding principle in the development of payments systems and the regulation of payment institutions.

120 Articles 1(2) and 16 of Directive 2014/92/EU on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.

121 Manisha Patel, Safari Kasiyanto, and André Reslow Patrick Honohan, 'House of Lords – Economic Affairs Committee: corrected oral evidence on central bank digital currencies' (9 November 2021), available at https://committees.parliament.uk/oralevidence/2993/html/, accessed on 21 November 2025; Lastra, International Financial and Monetary Law (OUP, 2015) 12.

122 Alex Rogers, Akila Quinio, 'US Congress passes landmark bill to regulate stablecoins' (17 July 2025) Financial Times. https://www.ft.com/content/4c41e6e8-374c-4b1a-ac7f-88c245fb18c8, accessed on 21 November 2025.

123 Proposal for a Regulation of the European Parliament and Council on the establishment of the digital euro, COM/2023/369, 28.06.2023.

124 Committee on Payments and Market Infrastructures, 'Central Bank Digital Currencies' (March 2018), available at https://www.bis.org/cpmi/publ/d174.pdf, accessed on 21 November 2025.

125 Interest-bearing CBDCs can help control demand for CBDCs and facilitate pass-through of interest rate decisions, but their 'deposit-like' features may trigger a 'run to CBDC' during a crisis. Tiering interest rates by volumes held could tackle this risk, but at the price of increasing complexity. BIS, note 56.

depends on their features, most central banks tend to see them as complements, rather than substitutes.[126]

The Digital Euro is seen by some as a response to the threats to monetary sovereignty and vulnerabilities,[127] by way of a secure, efficient, and accessible means of payment.[128] The proposal has a **two-tier architecture**:[129] issuance by the Eurosystem and distribution through intermediaries (banks and payment providers). Users would hold their Digital Euro in an electronic wallet and could make everyday payments with a phone app or card (online and offline). The Eurosystem has explored leveraging TIPS[130] as a reliable infrastructure, and it would not replace cash.[131]

Geopolitically, the Digital Euro seeks to boost the Euro's international standing, enhance 'strategic autonomy', mitigating reliance on third-country providers like Visa and Mastercard,[132] and resilience against, e.g., cyberattacks, in line with EPI or DORA (see section 3). **Commercially**, the rules would require merchant acceptance, but the Digital Euro also needs widespread user adoption, and design choices matter.[133] The ECB's investigation phase (October 2021 – October 2023) explored key features like ease of use (including integration into existing banking apps and cards); privacy safeguards (higher for offline, low-value payments); offline functionality (payments should work without internet or power); and broad accessibility across all EU Member States.[134]

Privacy and anti-money laundering rules are balanced with a transaction model (UTXO or unspent transaction outputs) that allows fast processing and validation without revealing users' payment patterns or account balances to the Eurosystem',[135] or centralising sensitive personal data. In offline mode, Digital Euro could be stored locally or exchanged directly between devices with no internet connection, enabling payments during network outages or in remote areas, and with a high degree of anonymity (transaction details would be known only to the payer and payee).

---

126 Aurazo et al. (2024) supra note 3.

127 Nikou Asgari, 'EU speeds up plans for digital euro after US stablecoin law' (22 August 2025) Financial Times.

128 European Central Bank, 'Report on a Digital Euro' (October 2020), available at https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf, accessed on 21 November 2025.; Bank for International Settlements, 'Central Bank Digital Currencies: Foundational Principles and Core Features' (9 October 2020), available at https://committees.parliament.uk/writtenevidence/40053/pdf/, accessed on 21 November 2025.

129 Philip R. Lane, 'The digital euro: maintaining the autonomy of the monetary system' (20 March 2025), available at https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250320_1~41c9459722.en.html, accessed on 21 November 2025.

130 Ulrich Bindseil, 'TARGET Services: the backbone of European Financial Markets' (14 July 2025), available at https://www.ecb.europa.eu/press/blog/date/2025/html/ecb.blog20250714~9676bef78b.en.html, accessed on 21 November 2025.

131 Piero Cipollone, 'Shifting payment landscape: what a digital euro will bring' (10 July 2025), available at https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250710~7d5aeae662.en.html, accessed on 21 November 2025.

132 Fabio Panetta, Valdis Dombrovskis, 'Why Europe needs a Digital Euro' (28 June 2023), available at https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog230628~140c43d2f3.en.html, accessed on 21 November 2025.

133 Emanuele Urbinati, et. al., *A Digital Euro: Contribution to the Discussion on Technical Design Choices* (July 2021) 10 Institutional Issues Banca D'Italia, 7 – 67.

134 See the ECB dedicated page on the topic at https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html#pubs, accessed on 21 November 2025.

135 ECB, 'Digital Euro – Prototype Summary and Lessons Learned' (2023), available at https://www.ecb.europa.eu/pub/pdf/other/ecb.prototype_summary20230526~71d0b26d55.en.pdf, accessed on 21 November 2025.

Central banks tend to see CBDCs as presenting more challenges than payment systems, including financial stability, transmission of monetary policy, disintermediation, resilience, or cyber security.[136] Experiences in **China, India and Brazil,** which launched or are launching their CBDCs pilot projects caution against excessive optimism. In China, regions with active PBoC promotion show more frequent and larger e-CNY transactions, more wallet creations, and greater merchant adoption, but overall, **users stick to existing electronic payment apps**.[137] The **Indian e-rupee** pilot project was launched in 2023 as a wholesale CBDC, followed by a retail program shortly thereafter, and its circulation reached 10,16 billion by March 2025[138] – still a **low amount** when compared with payments' transaction volume. Brazil's BCB has been working since 2022 on a pilot project for combining the digital real (**DREX**), private crypto assets and other services into a single app, with a Phase 2, focused on expanding use cases by engaging the public to submit ideas, and engaging the private sector in 2024, and a Phase 3, in 2025, focused on tokenisation and access to credit, but **blockchain and tokenisation were abandoned in August 2025**, pointing at scalability and privacy challenges.[139]

As **an end in itself**, the Digital Euro adds the challenges of a CBDC (financial stability or disintermediation) on top of the challenges of a payment system (scalability, user acceptance and user experience, etc.) There is scepticism about its adoption by users, and criticism of the holding limits so far being discussed, i.e., between EUR 3,000 and 4,000, as very low.[140] Without the prospect of widespread adoption, the cost-benefit is unclear. However, the Digital Euro may also be seen as a **means to an end**, i.e., as a catalyst to create a homegrown payments system. After all, as seen before, the obstacles to create a homegrown FSP, like the ECB's uncomfortable 'promotional' position are difficult to overcome with a 'payments' mandate only. Conversely, a CBDC's additional challenges (financial stability or disintermediation) have a more familiar note, and, in exchange, the ECB obtains a stronger legal mandate. This can help overcome the reluctance towards a hands-on approach by the central bank (which in a CBDC is a necessity), or the mandatory participation of (bank) payment service providers, and acceptance by payees,[141] while including non-bank payment service providers.[142] This proactive role could help the ECB promote the kind of ecosystem formed by applications, solutions, and services that results in a homegrown *payments system*. If that is the endgame, the Digital Euro may be worth the effort.

---

136 Aurazo et al. (2024) supra note 3, p. 20.

137 HaiChen Bai, Lin William Cong, Mei Luo, Ping Xie "Adoption of central bank digital currencies: Initial evidence from China" Journal of Corporate Finance, 91 (2025), 102735.

138 "RBI to explore cross-border CBDC pilots as e-rupee circulation surges to Rs1,016 crore" *The Times of India*, May 29, 2025. Available at: https://timesofindia.indiatimes.com/business/india-business/e-rupee-circulation-rises-to-rs-1016-crore-rbi-to-explore-cross-border-cbdc-pilots/articleshow/121493447.cms, accessed on 21 November 2025.

139 Aaron Stanley "Brazil Abandons Blockchain For Its Drex CBDC Project", *Forbes*, August 13, 2025. Available at: https://www.forbes.com/sites/digital-assets/2025/08/13/brazil-abandons-blockchain-for-its-drex-cbdc-project/, accessed on 21 November 2025.

140 Ignazio Angeloni 'Digital Euro: When in doubt, abstain (but be prepared)' EGOV PE 741.507 – April 2023; Cyril Monnet 'Digital Euro: An assessment of the first two ECB progress reports' EGOV, PE 741.508 – April 2023; Seraina Günewald 'A legal framework for the digital euro' EGOV PE 741.518 – May 2023.

141 Articles 7 (payees) and 14 (credit institutions operating a payment account).

142 Article 13 Digital Euro proposal.

6. CONCLUSIONS

The EU non-cash payment ecosystem features **critical dependencies** in messaging services (SWIFT), ICT services (by cloud hyperscalers) and card networks (Visa or Mastercard), which expose it to technical, or political, disruptions. The EU's strategic choices can combine regulations that promote resilience and promote homegrown alternatives that enable autonomy.

Regulatory frameworks like DORA can push financial firms to make a more honest assessment of their dependencies and vulnerabilities and perhaps seek greater diversification and backup plans, while allowing EU authorities to have a closer look at the finance-technology links. However, backup solutions are expensive, the ability to replace existing solutions is uncertain, and some sources of tension, like the diverging US and EU frameworks on data privacy vs. national security, cannot be fully solved.

This has whetted the **appetite for homegrown solutions**. As tempting as these may appear at first sight, **the EU must realistically assess** existing risks, and weigh pros and cons, costs and risks. On cloud services, the EU has probably lost the race and can only insist on relatively niche sovereign cloud solutions. On messaging services, Europe may explore complementary channels, e.g., enhanced SEPA cross-border capabilities or multilateral real-time payment linkages, while relying on SWIFT's global reach. The SEPA works well but is unlikely to replace dominant card schemes, and the industry is hesitant to promote EU-based card schemes. Experiences in China, India or Brazil suggest that a hands-on approach by the ECB/ESCB, and a partnership with the private sector, may help a homegrown payments solution to emerge, expanding the TIPS and SEPA infrastructures, with easier identification mechanisms, and better user experience, leaving private players to innovate with their own apps and new services. This centralised approach, however, presents challenges (including legal challenges) in the EU.

So far, rather than focusing on a retail fast payments solution, the ECB and the Commission are putting their focus on the **Digital Euro,** a **more ambitious** solution. A well-designed CBDC could answer many challenges. Its outcome depends design choices, as much as on **political will, flawless infrastructure, and industry support**. As an **end in itself**, its success is not guaranteed. However, Europe's policymakers may see it **as the means** to overcome some of the challenges faced by payment solutions. A CBDC requires a strong mandate, which can justify the hands-on approach needed to create the ecosystem of applications, providers and services that forms a homegrown payment system.

A forward-looking EU payments strategy must recognise that some vulnerabilities – particularly those rooted in foreign surveillance law or structural ICT concentration – cannot be entirely regulated away. This requires a pragmatic form of caution: diversification of providers, modular architectures, credible fallback options, and governance-based safeguards. Strategic autonomy in payments is more likely to emerge form layered resilience and operational optionality than from rigid localisation or attempts at complete insulation.

To this end, a **suitable solution** for the EU will involve a **case-by-case assessment** of risks and vulnerabilities. The EU should continue to **modernise and simplify its regulatory framework**, support **innovation** in **homegrown solutions**, especially if strong involvement by authorities is important, including the Digital Euro, and deepen operational cooperation with international partners while

preparing realistic contingency pathways for scenarios in which legal or geopolitical tensions challenge the continuity of Europe's payment systems. However, any attempt to do so should seek to create an ecosystem of providers and servicers that is more competitive and focused on user experience.

REFERENCES

- Alexander, *Principles of Banking Regulation* (CUP, 2019).
- Adler-Nissen, Eggeling, 'The discursive struggle for digital sovereignty: security, economy, rights and the Cloud Project GAIA-X' (2024) 62 (4) Journal of Common Market Studies, 993 – 1011.
- Annunziata, Hadjiemmanuil, Joosen, *Central Bank Digital Currency: the Birth of the Digital Euro* (Palgrave Macmillan, 2025).
- Armour, Awrey, Davies, Enriques, Gordon, Mayer, Payne, *Principles of Financial Regulation* (OUP, 2016).
- Asanova, Jazira; Kwon, Yonghwi; Pratyush; Owens, John "Leveraging Lessons Learned from India's Unified Payments Interface for Digital Transformation in Asia and the Pacific" ADB briefs, no. 299, April 2024.
- Autolitano, Pawlowska, 'Europe's quest for digital sovereignty GAIA-X as a case study' (2021) Istituto Affari Internazionali.
- Baker, Joe "Is China's cross-border payments network on the rise?" FXC Intelligence, 4 July 2025.
- Barresi, 'The evolution of the finality of payment or "how RTGSs, Instant Payment Systems, and DLT Platforms" change the concept of money' in Zatti, Barresi (eds.) *Digital Assets and the Law: Fiat Money in the Era of Digital Currency* (Routledge, 2024), 253 – 277.
- Barroso, Laborda, 'Digital transformation and the emergence of the fintech sector: systematic literature review' (2022) Digital Business, 1 – 18.
- Berger, Molyneux, Wilson (eds.) *The Oxford Handbook of Banking* (OUP, 2nd edn., 2014)
- Beaucillon, *Research Handbook on Unilateral and Extraterritorial Sanctions* (Edward Elgar, 2021).
- Binder, Saguato (eds.) *Financial Market Infrastructures: Law and Regulation* (OUP, 2021).
- Bremmer, 'The technopolar moment' (2021) 100 (6) Foreign Affairs, 112 – 128.
- Carbo-Valverde, Kahn, 'Payment Systems in the US and Europe: Efficiency, Soundness, and Challenges' (2016) 30 Revista de Establidad Financiera, 11 – 33.
- Casanova, Savoie (eds.), *Payment Services – Law and Practice* (Edward Elgar Publishing, 2025)
- Chakravorti, Roson, 'Platform competition in two-sided markets: the case of payment networks' (2004) Federal Reserve Bank of Chicago Working Papers No. 2004-09, 1 – 44.
- Chaplin, 'Single Euro Payments Area: is Europe's card business making the major changes that were widely predicted or is the whole initiative going flat?' (2009) 3 (1) Journal of Payments Strategy & Systems, 17 – 23.
- Chiu, Deipenbrock (eds.), *Routledge Handbook of Financial Technology and Law* (Routledge, 2021)

- Chorzempa, Martin; Spielberger, Lukas "Significant, but not Systemic: The Challenge of China's Efforts to Rival Western Financial Predominance" CSDS Policy Brief 11/2025.
- Christensen, *EU Payment Services: Regulation and Innovation* (OUP, 2025).
- D'Alvia, *The Speculator of Financial Markets: How Financial Innovation and Supervision Made the Modern World* (Palgrave Macmillan, 2023).
- D'Alvia, 'Legal constants and the 'constant' outside of the law: mobile payments in comparative prospective under European Union law' (2021) 28 (3) Maastricht Journal of European and Comparative Law, 333 – 354.
- D'Alvia, 'Payments and Merger Regulation: A case Law Analysis' in Gabriella Gimigliano (ed.) *Bitcoin and Mobile Payments: Constructing a European Union Framework* (Palgrave Macmillan, 2016), 251 – 267.
- DeMarco, Laurie; Walker, Joshua "Chinese Banks' Dollar Lending Decline", FEDS. Notes, May 16, 2025.
- Diehl, Heid, Tobiasch, 'The consolidation of TARGET2 and TARGET2-Securities: how is the Eurosystem exploring synergies across its infrastructures, and how will this impact day-to-day operations?' (2019) 11 (3) Journal of Securities Operations and Custody, 198 – 212.
- European Commission, Gentiloni Report, 'A new era for Europe: how the European Union can make the most of its pandemic recovery, pursue sustainable growth, and promote global stability' (2022).
- Evans, 'Industrial organisation of markets with two-sided platforms' (2007) 3 (1) Competition Policy International, 151 – 179.
- Ewald, Krueger, 'The European Payment Initiative: the next big thing in European payments?' (2021) 15 (3) Journal of Payments Strategy and Systems, 319 – 331.
- Farrell, Saloner, 'Standardisation, Compatibility, and Innovation' (1985) 16 (1) Rand Journal of Economics, 70 – 83.
- Gimigliano, Bozina Beros (eds), *The Payment Services Directive II: A commentary* (Elgar Commentaries in Financial Law, Edward Elgar Publishing, 2021).
- Goodhart, Lastra, 'Border Problems' (2010) 13 (3) Journal of International Economic Law, 705 – 718.
- Harrell, Rosenberg, *Economic Dominance, Financial Technology, and the Future of US Economic Coercion* (2019) Centre for a New American Security, 26.
- Herrera, 'PSD3 and the Regulation on Payment Services in the Context of Crypto Assets as a Means of Payment' in Carmen Pastor Sempere (ed.) *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities, and Data Spaces* (Springer, 2025), 373 – 394.
- Hobbs (ed.), Europe's Digital Sovereignty: from Rulemaker to Superpower in the Age of US-China Rivalry' (July 2020) European Council of Foreign Relations.
- International Monetary Fund (IMF) Pix: Brazil's Successful Instant Payment System, 31 July 2023.

- Janczuk Gorywoda, 'Evolution of EU Retail Payments Law' (40) 6 European Law Review, 852 – 876.
- Jans, *Electronic Payments in the European Market* (Palgrave Macmillan, 2024).
- Katz, Shapiro, 'Network externalities, competition and compatibility' (1985) 3 (75) The American Economic Review, 424 – 440.
- Kempaainen, 'Competition and regulation in European retail payment systems' (2003) 3 (77) Bank of Finland Bulletin, 25 – 28.
- Klapper, Lusardi, Panos, 'Financial literacy and its consequences: evidence from Russia during the financial crisis' (2013) 37 (10) Journal of Banking and Finance, 3904 – 3923.
- Kumar, 'The future of AI in Big Data: Cloud platforms are evolving to support machine learning and analytics' (2023) 1 (1) International Journal of Advancements in Computational Technology, 128 – 135.
- Lambach, Oppermann, 'Narratives of digital sovereignty in German political discourse' (2023) 36 (3) Governance, 693 – 709.
- Lastra, 'Weaponisation of Money and Payments' in Zilioli, Bismuth, Thevenoz (eds.) *International Sanctions: Monetary and Financial Law Perspectives* (Brill, 2024), 102 – 122.
- Lastra, *International Financial and Monetary Law* (OUP, 2015).
- Madir (ed.), *FinTech Law and Regulation* (Elgar Financial Law and Practice, 2nd edn., Edward Elgar Publishing 2021)
- Maymont, 'Les ambitions de l'European Payments Initiative' (2021) 5 Contracts, Concurrence, Consommation.
- Mersch, 'Making Europe's financial infrastructure a bulwark of financial stability' (April 2016) 20 Banque de France – Financial Stability Report, 71 – 77.
- Moloney, Ferran, Payne (eds.), *The Oxford Handbook of Financial Regulation* (OUP, 2015).
- Remund, 'Financial literacy explicated: the case for a clearer definition in an increasingly complex economy' (2010) 44 (2) The Journal of Consumer Affairs, 276 – 295.
- Robinson, Dorry, Derudder, 'SWIFT: Trusted Infrastructure for Infrastructures' in Westermeier, Campbell-Verduyn, Brandl (eds.) *The Cambridge Global Handbook of Financial Infrastructure* (Cambridge University Press, 2025), 246 – 249.
- Rochet, Tirole, 'Two-sided markets: a progress report' (2006) 37 (3) The Rand Journal of Economics, 645 – 667.
- Romanova, Grima, Spiteri, Kudinska, 'The payment services Directive II and competitiveness: the perspective of European fintech companies' (2018) 21 (2) European Research Studies Journal, 3 – 22.
- Sampaio, Matheus C; Ornelas, Jose Renato H "Payment technology complementarities and their consequences on the banking sector: evidence from Brazil's Pix" BIS Papers No 152.

- Sapkal, Heisnam, Kusi, 'Evolution of Cloud Computing: Milestones, Innovations, and Adoption Trends' (2024) 11 (3) International Research Journal of Engineering and Technology, 548 – 563.
- Scott, Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community* (Routledge 2014).
- Schmalensee, Evans, 'Industrial organisation of markets with two-sided platforms' (2007) 3 (1) Competition Policy International, 151 – 179.
- Sean, 'SWIFT clouds between international legal storms? Bank Melli, the CJEU and Secondary Sanctions' (2022) 17 (9) Global Trade and Customs Journal, 404 – 407.
- Shababi, 'The butterfly effect of technology: how various factors accelerate or hinder the arrival of technological singularity' (2025) Computer and Society, 1 – 20.
- Silva, Ramalho, Vieira, 'The impact of SEPA in credit transfer payments: evidence from the euro area' (2016) Research in International Business and Finance, 404 – 416.
- Singh, Haleem, Javaid, Kataria, Singhal, 'Cloud computing in solving problems of Covid-19 pandemic' (2021) 6 (2) Journal of Industrial integration and Management, 209 -219.
- Smits, 'The European Community's Second Banking Directive' in Robert C. Effros (ed.) *Current Legal Issues Affecting Central Banks Voume IV* (International Monetary Fund, 1997) 83 – 103.
- SPI Sistema de Pagamentos Instantâneo (Instant Payments System) Annual Report 2024.
- The Economist "National payment systems are proliferating". 3 May 2024.
- The Economist "Brazil's government-run payments system has become dominant". 3 April 2025.
- The Economist "China is ditching the dollar, fast" 10 September 2025.
- Tiagi, Tanusha "UPI at Scale: Outages and the Push for Resilient Systems". 21 June 2025.
- Urbinati, et. al., *A Digital Euro: Contribution to the Discussion on Technical Design Choices* (July 2021) 10 Institutional Issues Banca D'Italia, 7 – 67.
- Vardi, 'Bit by bit: assessing the legal nature of virtual currencies' in Gabriella Gimigliano (ed.), *Bitcoin, and Mobile Payments: Constructing a European Union Framework* (Palgrave 2016), 55 – 72.
- Watrous, Julian; Paduano, Stephen "The Lender of First Resort? Chinese Swap Lines, the IMF and the Changing International Financial Architecture" GCI Working Paper 042 04/2025.
- Zaimovic, Torlakovic, Arnaut-Berilo, Zaimovic, Dedovic, Nuhic, 'Mapping financial literacy: a systematic literature review of determinants and recent trends' (2023) 15 (12) Sustainability, 1 – 30.

ANNEX: BASIC FACTS ON PAYMENTS IN EUROPE

1. Why the Payment "System" favours concentration

Non-cash payments occupy a central role in debates about the 'cashless society',[143] decentralised finance,[144] or Central Bank Digital Currencies.[145] However, the payments' 'system', formed by its infrastructure, operators, and norms, is largely a consequence of payments' unique features. Cash does not require final settlement; the delivery of coins and currency is final.[146][147] Non-cash (bank-based) payments require finality, which depends on a system underpinning transaction verification.[148] Thus, more than in other areas, there is a seamless continuity between operators, platforms, technologies and technical protocols, and the rules that regulate them.

This explains two features. First, the interconnectedness within the market, which produces network effects in the form of two-sided markets.[149] In card payments, consumers are only interested in cards if there is a large number of merchants who use them, and vice-versa. This, and the large costs to create an infrastructure, encourage the growth of large providers and a highly concentrated market structure,[150] or the cooperation between operators, which, in turn, explains the close scrutiny of competition authorities.[151] [152] Second, the relevance of standardisation of technical standards, which lower development and operating costs, enhancing efficiency,[153] as it happens with SWIFT for international inter-bank payments or the IBAN, initially developed by the European Committee for

[143] Cecilia Skingsley, 'Considerations for a cashless future' (22 November 2018) public speech at Sveriges Riksbank, available at https://www.riksbank.se/globalassets/media/tal/engelska/skingsley/2018/skingsley_considerations-for-a-cashless-future.pdf, accessed on 21 November 2025.

[144] Executive Order No. 14178, 'Strengthening American Leadership in Digital Financial Technology' (31 January 2025) available at https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, accessed on 21 November 2025.

[145] Atlantic Council, 'Central Bank Digital Currency Tracker', available at https://www.atlanticcouncil.org/cbdctracker/, accessed on 21 November 2025.

[146] Rosa Lastra, *International Financial and Monetary Law* (OUP, 2015), 12.

[147] David Humphrey, 'Payments and Payment Systems' in Allen N. Berger, Philip Molyneux, John O. S. Wilson (eds.) *The Oxford Handbook of Banking* (OUP, 2nd edn., 2014), 409.

[148] Rosa Giovanna Barresi, 'The evolution of the finality of payment or 'how RTGSs, Instant Payment Systems, and DLT Platforms change the concept of money' in Filippo Zatti, Rosa Giovanni Barresi (eds.) *Digital Assets and the Law: Fiat Money in the Era of Digital Currency* (Routledge 2024), 253 – 277.

[149] Michael L. Katz, Carl Shapiro, 'Network externalities, competition and compatibility' (1985) 3 (75) The American Economic Review, 424 – 440; Joseph Farrell, Garth Saloner, 'Standardisation, Compatibility, and Innovation' (1985) 16 (1) Rand Journal of Economics, 70 – 83. See also Fraile, Villar, Ramos Muñoz et al Competition Issues in the Area of Financial Technology (FinTech) 2019, PE 631.061 – April 2019, available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631061/IPOL_IDA(2019)631061_EN.pdf, accessed 21 November 2025.

[150] Kari Kempaainen, 'Competition and regulation in European retail payment systems' (2003) 3 (77) Bank of Finland Bulletin, 25 – 28.

[151] The avoidance of market abuse of dominant position and the preservation of positive network externalities is particularly important in mobile payment solutions operated by virtue of digital mobile wallets (see Daniele D'Alvia, 'Payments and Merger Regulation: A case Law Analysis' in Gabriella Gimigliano (ed.) *Bitcoin and Mobile Payments: Constructing a European Union Framework* (Palgrave Macmillan 2016), 251.

[152] See D'Alvia, Payments and Merger Regulation, note 9, 252.

[153] Bank for International Settlements (BIS), 'Core Principles for Systemically Important Payment Systems' (January 2001).

Banking Standards[154] and the International Payment Instruction established standards at European level.

2. EU normative framework: technical neutrality, PSD1, 2, 3

In the European Union, the launch of SEPA in 2008 was a crucial step in cross-border harmonisation of euro-denominated credit transfers and direct debits, built upon the First and the Second Banking Directives and the Settlement Finality Directive (98/26/EC),[155] and reaching operational coherence with the first Payment Service Directive of 2007 (PSD1), revised in 2015 with PSD2. By reducing dependency on traditional bank intermediaries, the retail payments framework can be characterized as 'regulation for competition'[156] and the link between services and new technologies.

Financial innovation's defining role[157] explains the principle of technological neutrality, whereby, e.g., 'The definition of payment services [...] should allow for the development of new types of payment services, while ensuring equivalent operating conditions for both existing and new payment service providers' (PSD2 Recital (22)). This also means that users must enjoy the same level of protection regardless of the technology supporting the means of payment. Thus, since FinTech innovations have blurred the boundaries between operators, financial rules should follow a functional approach, and, possibly, bring non-banks into regulated financial activities.[158]

The first Payment Service Directive (PSD1) was adopted in 2007 (Directive 2007/64/EC) to establish a harmonised legal framework for a single market in payment services (SEPA), with a single license regime for payment institutions, subject to 'passporting' and common conduct rules which standardised transparency of fees, execution times, value dating, and liability for unauthorised transactions. PSD1 and SEPA enabled EU customers and businesses to make intra-EU electronic payments as easily as within one country, with features like next-day payment execution (by 2012) or refund rights for direct debits. All this enhanced consumer confidence, while opening the field for new entrants, such as online payment processors, remittance companies, etc.

The PSD2[159] followed a stocktaking of technological innovation and new means such as internet and mobile payments,[160] which put some services, such as third-party PSPs, outside the PSD1's scope, and was accompanied by a Regulation on Multilateral Interchange Fees.[161] The new rules recognised

---

154 The European Committee for Banking Standards (ECBS) was formed in December 1992 by leading European banking associations. In 2006 its functions were taken over by the European Payments Council and the committee was disbanded.

155 EU Regulation No 260/2012 underpinned the Single European Payment Area (SEPA). Rene Smits, 'The European Community's Second Banking Directive' in Robert C. Effors (ed.) *Current Legal Issues Affecting Central Banks - Volume IV* (International Monetary Fund, 1997) 83 – 103.

156 Agnieszka Janczuk Gorywoda, 'Evolution of EU Retail Payments Law' (40) 6 European Law Review, 852, 858.

157 Daniele D'Alvia, *The Speculator of Financial Markets: How Financial Innovation and Supervision Made the Modern World* (Palgrave Macmillan, 2023); Inna Romanova, et. al., 'The payment services directive II and competitiveness: the perspective of European fintech companies' (2018) 21 (2) European Research Studies Journal, 3, 5.

158 Charles A. E. Goodhart, Rosa Lastra, 'Border Problems' (2010) 13 (3) Journal of International Economic Law, 705.

159 Directive on Payment Services in the Internal Market, Amending Directive 2002/65/EC, 2009/110/EC, and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, [2015] OJ L 337/35, n. 2366.

160 European Commission, *Towards an Integrated European Market for Card, Internet and Mobile Payments* (2012) Green Paper.

161 Regulation on Interchange Fees for Card-based Payment Transactions [2015] OJ L 123/1, n. 751.

payment institutions (under PSD2) and e-money institutions (under the Electronic Money Directive[162]). PSD2 notably introduced **Open Banking** and Third-Party Access to Accounts, requiring banks and building societies (termed 'Account Servicing Payment Service Providers') to open their systems via secure application programming interfaces (APIs) to licensed third-party providers (TPP), like FinTech firms, to access bank customers' payment accounts (with consent). These TPPs provided (i) Payment Initiation Services (PIS, provided by PISPs) and (ii) Account Information Services (AIS, provided by AISPs).[163] AISPs allowed businesses to gather customer data to tailor their product list to customers, while PISPs helped them to provide their customers with a better overall experience, e.g., collecting payments and lowering operating costs and processing fees. Although banks initially dubbed this an 'expropriation' of their customer data, PSD2 also opened opportunities for banks, and outlawed practices like screen-scraping, where TPPs used consumers' online banking passwords to collect data. PSD2 embraced non-bank innovators rather than leaving them entirely unregulated.

PSD2 also provides a full license regime (Article 5) and capital requirements (Article 7) with differences between services (e.g., lower for money remittances, higher for PIS), and some exemptions for smaller PSPs providing certain services (Article 32) and AISPs (Article 33). To counter fraud, it also introduced the Strong Customer Authentication (SCA), requiring two-factor authentication for most online and card payments, tasking the EBA (Article 98 (1)) with developing Regulatory Technical Standards (RTS).

The proposal for a PSD3,[164] and a new Payment Services Regulation (**PSR**),[165] represents both continuation and modernisation, reinforcing PSD2's open banking and strong customer authentication, while mitigating fragmentation, inconsistencies and arbitrage by introducing a regulation, and consolidating the payment institutions and e-money institutions within a unified licensing regime. It also strengthens consumer protection and fraud prevention, requiring firms to safely share fraud data and implement verification (e.g., IBAN-name matching on credit transfers) and granting consumers clearer reimbursement rights in 'authorised' push payment fraud (e.g., impersonation-based scams). The proposals further clarify open banking rules, prohibiting obstacles to TPP access, and acknowledging an industry 'premium API' space (via schemes like SEPA Payment Account Access) to encourage innovation beyond free minimum services.

One challenge is that distributed ledger technology (DLT) made it possible to create tokens (representations of value and rights), transmissible electronically. The Market in Crypto-Assets (MiCA) Regulation (2023/1114) regulates stablecoins, electronic money tokens and asset-referenced tokens, raising the question whether crypto assets with a payment function regulated by MiCA are also

---

[162] Directive 2009/110/EC of 16 September 2009 (Electronic Money Directive 2 or EMD2) to establish common standards in terms of prudential supervision of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

[163] AISPs provide account information services, and can access and collect data across bank accounts, but cannot initiate payments. PISPs provide payment initiation services, i.e., access and collect financial data from bank accounts but also trigger payments from them.

[164] European Commission, *Proposal for a Directive of the European Parliament and of the Council on Payment Services and Electronic Money Services in the Internal Market Amending Directive 98/26/EC and Repealing Directives 2015/2366/EU and 2009/110/EC*, COM (2023) 366 final.

[165] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Payment Services in the International Market and Amending Regulation (EU) No. 1093/2010*, COM (2023) 367 final. The Council reached a compromise in June 2025, and trilogue negotiations are proceeding, with adoption expected by end 2025.

'payment services', covered by PSD2, and whether certain transactions are payment transactions.[166] The EBA has recently discussed the interplay between PSD2 and MiCA, pointing out that 'exchange of crypto-assets for funds' and 'exchange of crypto-assets for other crypto-assets' as defined in MiCA are not deemed to be 'payment services' under PSD2.[167]

3. EU payments infrastructures, public (T2, T2S, TIPS) and private (credit card networks)

Financial market infrastructures (FMIs) are the backbone of modern financial markets.[168] FMIs encompass payment, clearing and settlement systems, central clearing counterparties and trade repositories. They are defined as "a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions" (Articles 4 (7) PSD2, 2(7) PSD3 proposal). Thanks to their features, they enhance financial stability and promote better risk management, but they can also concentrate risk via interdependencies and can themselves be a source of systemic risk. Focusing on payments, there are four key types of systems:

- Large Value Payment Systems
- Retail Payment Systems
- Real-time Gross Settlement Payment Systems
- Net Settlement Payment Systems

The Eurosystem has promoted financial market infrastructures to integrate money and capital markets.[169] Article 127 (2) TFEU provides that the ESCB's basic tasks include defining and implementing monetary policy; conducting foreign-exchange operations; and promoting the smooth operation of the payment systems. Under the ESCB/ECB Statute the ECB and national central banks may open accounts for credit institutions, public entities and other market participants and accept assets as collateral (Article 17) or provide facilities, and (the ECB) enact regulations for efficient and sound clearing and payment systems (Article 22).

'TARGET Services' are the Euro area's wholesale and instant payment plumbing, comprising:

- Large Value Payment Systems the new-generation T2 wholesale payment system (with its Central Liquidity Management module)
- TARGET2-Securities for securities settlement (T2S)
- The TARGET2 – T2S Consolidation Project has merged TARGET2 and TARGET2-Securities into a single platform to enhance liquidity management.

---

166 Lucia Alvarado Herrera, 'PSD3 and the Regulation on Payment Services in the Context of Crypto Assets as a Means of Payment' in Carmen Pastor Sempere (ed.) *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities, and Data Spaces* (Springer, 2025), 373, 375.

167 EBA, *Opinion of the European Banking Authority on the interplay between Directive EU 2015/2366 (PSD2) and Regulation (EU) 2023/1114 (MiCA) in relation to crypto-asset service providers that transact electronic money tokens*, (10 June 2025).

168 Jens-Hinrich Binder, Paolo Saguato (eds.) *Financial Market Infrastructures: Law and Regulation* (OUP, 2021).

169 Martin Diehl, Christoph Heid, Katharina Tobiasch, 'The consolidation of TARGET2 and TARGET2-Securities: how is the Eurosystem exploring synergies across its infrastructures, and how will this impact day-to-day operations?' (2019) 11 (3) Journal of Securities Operations and Custody, 198 – 212.

- TARGET Instant Payment Settlement or TIPS, an extension of TARGET services (integrated with them) for 24/7 retail payments, enabling real time fund transfers with settlement in central bank money (supporting the SEPA Instant Credit Transfer scheme).

TARGET Services are subject to the Eurosystem Oversight Framework for Financial Market Infrastructures, which is aligned with the CPMI – IOSCO Principles for Financial Market Infrastructures,[170] which emphasize solid governance, comprehensive risk management, operational reliability, and transparency access policies. The ECB regularly issues oversight assessments and technical guidelines.[171] The legal framework also includes the Settlement Finality Directive (98/26/EC), which underpins irrevocability and finality of payments and securities settlement and protects T2 transactions from insolvency proceedings. The new-generation framework of TARGET Services is codified under the ECB Guideline (EU) 2022/912,[172] amended by Guideline (EU) 2023/2415,[173] which sets, *inter alia*, the operational and functional rules for T2, with a harmonised messaging environment based on ISO 20022, and a central liquidity account architecture.

Consolidation strengthens the euro area's capacity to withstand shocks: the central liquidity allows banks to deploy collateral and balances efficiently across flows in T2 and settlement obligations in T2S and TIPS, while a single legal basis and ISO 20022-based messaging reduces complexity and improves interoperability. In June 2025, the Eurosystem launched the Eurosystem Collateral Management System (ECMS),[174] a complementary system for to unify collateral assets management, and facilitate the flow of cash, securities, and collateral across Europe. **Table 3** summarizes the increase of activity in TARGET Services:

[170] Bank for International Settlements, 'Committee on Payment and Settlement Systems, Technical Committee of the International Organisation of Securities Commissions – Principles of Financial Market Infrastructures' (April 2012), available at https://www.bis.org/cpmi/publ/d101a.pdf, accessed on 21 November 2025.

[171] The Eurosystem's SIPS regime governs resilience. Regulation (EU) No 795/2014 (ECB/2014/28) on oversight requirements for systemically important payment systems sets the high-level risk management, governance, operational and settlement requirements for systemically important systems, in line with CPMI-IOSCO standards. Decision (EU) 2019/1349 (ECB/2019/25) specifies procedures for competent authorities' enforcement powers *vis-à-vis* SIPS. Within that framework, the Eurosystem applies cooperative oversight models (e.g. SWIFT) and direct oversight for its own infrastructures to ensure business continuity, cyber resilience, and effective incident management. For TARGET Services, these rules sit along the specific TARGET Guidelines.

[172] ECB, 'Guideline (EU) 2022/912 of the European Central Bank of 24 February 2022 on a new-generation Trans-European Automated Real-Time Gross Settlement Express Transfer System (TARGET) and repealing Guideline 2013/47/EU (ECB/2012/27)', available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022O0912, accessed on 21 November 2025.

[173] ECB, 'Guideline (EU) 2023/2415 of the European Central Bank of 7 September 2023 amending Guideline (EU) 2022/912 on a new-generation Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET) (ECB/2022/8) (ECB/2023/22)', available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302415, accessed on 21 November 2025.

[174] European Central Bank, 'Guideline (EU) 2024 of the European Central Bank on the management of collateral in Eurosystem credit operations' (13 August 2024) ECB/2024/22. The new harmonised rules came into force in June 2025. For further information about ECMS see ECB, 'What is the Eurosystem Collateral Management System, available at https://www.ecb.europa.eu/paym/target/ecms/html/index.en.html, accessed on 21 November 2025.

Table 3: Comparative Activity in TARGET Services 2023 vs. 2024

		Volume (number of transactions)			Value (EUR billions)		
		2023	2024	Change (%)	2023	2024	Change (%)
T2	Total	104,273,922	107,999,982	+3.6%	486,793.1	463,735.6	-4.7%
	Daily average	408,917	421,875	+3.2%	1,909.0	1,811.5	-5.1%
T2S	Total	177,766,588	202,602,542	+14.0%	200,746.6	248,939.7	+24.0%
	Daily average	699,868	791,416	+13.1%	790.3	972.4	+23.0%
TIPS	Total	269,766,787	1,354,847,183	+402.2%	173.1	324.0	+87.1%
	Daily average	741,118	3,681,650	+396.8%	0.5	0.9	+85.1%
Total	Total	551,807,297	1,665,449,707	+201.8%	687,712.8	712,999.3	+3.7%
	Daily average	1,849,903	4,894,941	+164.6%	2,699.8	2,784.8	+3.1%

Source: European Central Bank, TARGET Services Annual Report 2024.

TIPS has experienced a dramatic increase in volume and value of transactions. Part of this may be due to the Eurosystem's harmonised policy[175] to allow non-bank PSPs (subject to PSD2 and EMD2) to access TARGET Services. TARGET Services are public FMIs operated by a system of central banks. The consolidated T2 platform marks a technology change, and a step towards strategic resilience.

However, such resilience depends on the interaction between public infrastructures and private global card schemes dominated by Visa and Mastercard networks. Thus, although transactions may ultimately result in interbank movements under TARGET Services, these only provide the settlement infrastructure for a network where the transaction mechanics between issuing banks, acquiring banks and merchants are governed by Visa and Mastercard proprietary contractual frameworks regulating authorisation, clearing, settlement, fees, dispute management and liability, and defining, e.g., reimbursements, chargebacks and refunds, or consumer and merchants rights. Thus, a large part of Europe's retail payments at the point of sale and in e-commerce, is governed by legal and operational frameworks external to European policymaking, and any vulnerabilities arising from this cannot be mitigated through more robust TARGET systems.

[175] ECB, 'Eurosystem sets policy on access by non-bank payment service providers to its central bank payment systems' (19 July 2024), available at https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews20240719.en.html, accessed on 21 November 2025.

This paper analyses the external dependencies and vulnerabilities in European payments, notably on cloud services or data privacy. It acknowledges that regulatory solutions enhance resilience but have limitations, while homegrown alternatives look tempting, but may be unfeasible, or come with major trade-offs. European institutions should carefully assess costs and benefits case by case, address short-term threats, while promoting strategic long-term planning, and push decisively for a Single Market in payment services.

This document was provided by the Economic Governance and EMU Scrutiny Unit at the request of the ECON Committee).

PE 764.370
IP/A/ECON-BU/FWC/2020-003/LOT2/C2/SC5

Print ISBN 978-92-848-3144-9 | doi:10.2861/9808403 | QA-01-25-251-EN-C
PDF ISBN 978-92-848-3143-2 | doi:10.2861/7397632 | QA-01-25-251-EN-N