EUROPEAN CENTRAL BANK
BANKING SUPERVISION

Occasional Paper Series

Phoebus Athanassiou, Stephanie Czák-Ludwig,
Nico Di Gabriele

Neo-conglomerates and EU regulatory perimeter challenges – state of play and evaluation of policy options

No 394

Contents

Abstract **3**

1 Non-technical summary **4**

2 Introduction: regulatory perimeter monitoring and its relevance for financial stability **5**

3 EU legal and regulatory context **8**

4 Trends, gaps and developments at the boundary of the regulatory perimeter **12**

4.1 Unbundling and re-bundling of financial activities 12

4.2 Partnerships between financial and non-financial entities 14

4.3 Market places 15

4.4 Buy now, pay later arrangements 15

4.5 AI and data access 16

4.6 Decentralisation and DeFi 18

Box 1 *Crypto-based staking, lending and borrowing* 20

4.7 Data and information-sharing gaps 22

5 Case studies **24**

5.1 Cross-border white label arrangement 24

5.2 Complex multi-partner white label arrangement 26

Box 2 *Examples from the United States of white labelling risks and enforcement* 29

5.3 Large neo-conglomerate 29

Box 3 *Limits of traditional conglomerate regulation* 32

5.4 Borderless fintech with bank-like activities 33

5.5 From fintech to banking and crypto-assets 34

6 Policy options and supervisory approaches **37**

6.1 Risk assessments and monitoring 37

6.2 General regulatory approaches 37

6.3 Approaches for groups 38

6.4 Perimeter adjustment practices 39

7 EU-specific considerations 42

7.1 Enhanced collaboration on regulatory perimeter monitoring and risk assessments 43

7.2 Reviewing EU-wide reporting 45

7.3 Enhancing the EU regulatory framework 47

Box 4 *Approaches of other jurisdictions to parent companies* 52

8 Conclusion 56

Abstract

This paper examines the implications of the provision, in the European Union, of bank-like services, including payment services, by large non-bank groups (i.e. groups that do not comprise entities with a banking licence), and evaluates policy options to address the emergence of so-called neo-conglomerates by recalibrating the regulatory perimeter.

Drawing on five EU case studies (a messaging app white-label arrangement, a complex multi-partner "super-app" model, a systemic payment group, a borderless financial technology firm (fintech) and a bank) – this paper illustrates how financial services may be delivered through digital unbundling and re-bundling, embedded distribution and white-label partnerships. It maps the business models, licensing structures, fintech partnership chains and data frictions that may obscure group-wide risks and complicate home-host supervisory cooperation. The cases were included for illustrative purposes only, and implying no judgement at all on the soundness or governance of the firms concerned, nor on the effectiveness or adequacy of the actions taken by the relevant supervisory authorities. The paper also identifies potential "blind spots" in the regulatory frameworks applicable at the time of writing and misalignments in prudential, conduct and operational objectives.

Building on guidance from standard-setting bodies and international organisations on supervisory approaches to financial innovation, fintech and Big Tech, the paper identifies four priority areas for consideration, with a view to limit regulatory arbitrage and systemic interdependencies, while at the same time preserving innovation. In particular, the paper proposes (i) improving the monitoring of bank-like activities, harmonising definitions and calibrating intervention powers ("perimeter governance"); (ii) enhancing transparency and supervisory reach for complex multi-partner and white-label distribution models by direct licensing, on-site supervisory powers over agents and disclosure; (iii) introducing group-wide oversight for neo-conglomerates, in the form of a European Union financial holding structure for large and complex non-bank groups, with holistic and risk-based prudential requirements, reporting and supervisory colleges; and (iv) improving cooperation, coordination and information-sharing across authorities, supported by EU-level sandboxes and forward-looking risk assessments.

JEL codes: G28, E58, K23, O33, F36, G32

Keywords: regulatory perimeter, regulatory arbitrage, group-wide supervision, neo-conglomerates, systemic risk

1 Non-technical summary

Why does the regulatory perimeter matter? Financial services are increasingly embedded/integrated in non-financial platforms, such as online marketplaces or messaging apps, or are offered by unregulated entities. Large, technology-driven groups ("neo-conglomerates") increasingly use digital platforms, partnerships and innovative business models to offer a bundle of financial services, including payments, lending, investments and crypto-assets, to millions of Europeans, often under less stringent regulatory and supervisory rules than those applicable to licensed banks. Accordingly, some of the activities of neo-conglomerates do not fall within the regulatory perimeter, defined as the body of rules governing which financial services are regulated, and how.

What are the main challenges? The combination, within the same group, of regulated and unregulated activities that straddle different financial market sectors and borders, makes it harder for supervisors to detect risks, understand interdependencies and ensure the application to these groups of adequate regulatory, supervisory and oversight safeguards.

Where are the gaps? The regulatory, supervisory and oversight rules currently in place in the EU are largely sector-specific, targeting banks, investment firms or the issuers of financial assets, while some activities – such as crypto lending – remain altogether unregulated. Where financial activities, notably in the field of payments, crypto, and non-bank lending, are split and then re-bundled, their risks and interdependencies can go undetected. This may result in capital requirements that are too low to ensure adequate safeguards or in oversight requirements that do not account for the full range of activities pursued by financial actors. Similarly, supervisors may lack the data and enforcement tools necessary to assess and address risks, with an adverse effect on the efficacy of their supervision.

To preserve the safety and integrity of the financial system, the paper proposes: (1) legislative adjustments, to harmonise the definitions of bank-like activities, ensure the integration within the regulatory perimeter of new services, and granting intervention powers to the competent authorities (CAs);
(2) a harmonisation of the regulatory treatment of new business, cooperation and distribution models and introducing licensing requirements for complex, multi-partner arrangements;
(3) group-wide, cooperative supervision for neo-conglomerates engaged in providing financial services in the EU; and
(4) improved cooperation and data-sharing among national and EU authorities, and the use of EU-level sandboxes to monitor new business models and their risks.

Why is this important? Regulation needs to keep pace with innovation, supporting growth and inclusion while preventing regulatory loopholes and systemic vulnerabilities. As long as regulatory and supervisory gaps exist, risks outside the purview of supervisors could build up, potentially threatening financial stability, free competition and consumer protection.

2 Introduction: regulatory perimeter monitoring and its relevance for financial stability

Financial systems are dynamic and constantly evolving ecosystems: new market players, instruments and business models routinely emerge, both on the fringes of regulation and oversight and outside their perimeter, creating scope for blind spots, which, if not identified and monitored, may morph into systemic vulnerabilities. Early identification and reaction – also through appropriate supervision and oversight – can help to prevent regulatory arbitrage, reduce the risk of contagion and ensure a level playing field, safeguarding market confidence, supporting financial system resilience and ultimately underpinning systemic stability.

International organisations and standard-setting bodies (SSB) commonly assert regulatory perimeter[1] monitoring as a core, financial stability-driven responsibility of regulators and supervisors[2]. They also stress the importance of regularly updating laws, regulations, and prudential standards to ensure their continued effectiveness (see the 2013 Financial Stability Board (FSB) policy recommendations for strengthening oversight and regulation of non-bank financial institution (NBFI) entities[3], as well as the Basel Core Principles[4] and other sector-level standards[5]). The International Monetary Fund (IMF) has reinforced this stance through its *Bali Fintech Agenda* (2018), which highlights the importance of continuous monitoring of financial innovation to support timely and effective policy responses.[6] The evaluation of the effectiveness of regulatory perimeter monitoring is part of the IMF's Financial Sector Assessment Program (FSAP).

Recent years have seen the emergence of large non-bank groups, often organised through complex structures, that engage in technology-enabled financial intermediation across jurisdictions and sectors (referred to as "neo-conglomerates" in

1 For the purposes of this paper, the term "regulatory perimeter" refers to the scope of financial activities and entities that fall within the application of existing financial sector legislation. Activities or entities not subject to such legislation are considered outside the regulatory perimeter.

2 Also referred to as "competent authorities" in this paper.

3 See FSB (2013), Policy Framework for Strengthening Oversight and Regulation of Shadow Banking Entities, 29 August, pp. 13. Overarching Principle 1 states "Authorities should define, and keep up to date, the regulatory perimeter" to address financial stability risks from NBFI entities. Also see FSB (2023) High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets, 17 July, Recommendation 2 in the case of crypto-asset activities and markets.

4 See BCBS (2024), Core Principles for effective banking supervision, 23 April, pp. 29. Principle 8, Essential Criterion 8 (states that "Where the supervisor becomes aware of bank-like activities being performed fully or partially outside the regulatory perimeter, the supervisor takes appropriate steps to draw the matter to the attention of the responsible authority to address regulatory arbitrage".

5 For example, see CPMI and IOSCO Technical Committee (2012), Principles for financial market infrastructures, 16 April, pp. 126-127 and IOSCO (2017) Objectives and Principles of Securities Regulation, May, Principle 7.

6 The IMF has also advocated an ongoing dialogue with industry stakeholders, the adaptation of regulatory frameworks to preserve financial stability and enhanced international cooperation and information-sharing. The effectiveness of regulatory perimeter monitoring is also evaluated as part of the IMF's Financial Sector Assessment Program.

this paper). The emergence of such groups, which do not typically include a bank, investment firm or insurance undertaking, but rather comprise large fintechs, platform-based financial ecosystems and mixed-activity groups (MAGs[7]), could challenge the effectiveness of the regulatory and supervisory frameworks by obscuring their aggregate risk profile. In the absence of prudential consolidation or conglomerate-level supervision, the group-wide risk profile of neo-conglomerates can be difficult to assess (ESA, 2024).[8] Apart from creating scope for certain risks to fall through regulatory and supervisory safety nets, the neo-conglomerate phenomenon may lead to regulatory arbitrage and promote unfair competition.

While the European Union's prudential rulebook for banks, investment firms and insurers is robust and takes a consolidated approach, gaps persist where financial activities are re-bundled by entities subject to lighter or fragmented regulatory regimes. In areas such as payments, crypto-asset services and non-bank lending, regulation tends to focus on rules of conduct, while prudential requirements are generally less stringent and apply only at individual entity level. The modularisation of financial services, through unbundling and re-bundling via digital platforms, is likely to complicate the task of allocating responsibility for their provision and obfuscate risk transmission channels.

White labelling arrangements[9], in which unlicensed entities control customer interfaces while regulated partners provide underlying services, also pose challenges. Such arrangements may enhance efficiency, but may also fragment compliance responsibilities, weaken consumer protection safeguards and create dependencies and single points of failure. Embedded finance and marketplaces intensify these dynamics by using financial services to drive platform activity and fee income, with "buy now, pay later" (BNPL) arrangements reshaping household consumption behaviour and borrowing, also raising transparency and prudential concerns. Although the revised Consumer Credit Directive[10] addresses consumer protection, it leaves out prudential requirements and related credit monitoring. The artificial intelligence (AI) and machine learning tools often deployed by neo-conglomerates may well deliver efficiency gains, but they also have the potential to introduce operational and governance risks.

In parallel, the evolution of the crypto-asset markets and decentralised finance continues to challenge the coherence of the regulatory perimeter, with multi-function intermediaries/groups (ESRB, 2025; FSI, 2024) and protocol-based lending concentrating risk outside prudential boundaries. Governance failures and cross-subsidisation could amplify contagion. For their part, third-country multi-issuer

7 MAGs engage in both financial and non-financial activities.

8 This observation was made in the context of the stocktaking of Big Tech direct financial services provision in the EU.

9 White labelling is a business model in which a financial institution (the provider) enters into an agreement with another entity (the partner, who may or may not be a financial institution) to distribute and offer one or more financial products and services under the partner's own brand only (EBA, 2025)

10 Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC (OJ L, 2023/2225, 30.10.2023).

stablecoin schemes risk undermining the existing safeguards under MiCAR[11] by enabling fungibility across jurisdictions without equivalent standards, reciprocity or enforceable asset transfer arrangements.[12] Crypto lending, borrowing and staking remain unregulated, despite their potential to transmit shocks across the financial system (EBA/ESMA, 2025).

Addressing the above vulnerabilities calls for enhanced supervisory cooperation and a forward-looking, proportionate policy response. This paper identifies four priority areas for further consideration:

1. Strengthening perimeter governance by harmonising definitions of bank and bank-like activities, bringing within the regulatory perimeter certain hitherto unregulated services (e.g. crypto lending), clarifying interest pass-through rules and empowering ESAs to intervene.

2. Enhancing consistency by holistically addressing white labelling arrangements and improving supervisory reach through: direct licensing for complex multi-partner distributors, complemented by harmonised disclosure requirements to break silos, reduce data aggregation loss and close reporting gaps; on-site inspection powers over agents/brokers; and systematic information-sharing on major infringements.

3. Establishing a regulatory framework for group-wide oversight by introducing a financial holding company regime for neo-conglomerates, featuring enhanced prudential requirements, recovery and resolution planning, dedicated supervisory colleges and ESA-led supervision for significant players.

4. Improving consolidation, cooperation and information-sharing, capturing regulated firms, those operating under exemptions and ancillary activities. EU-level sandboxes and forward-looking risk assessments will be key in detecting emerging models, recalibrating oversight and enabling coordinated action, while fostering responsible innovation that preserves EU sovereignty.

The structure of this paper is as follows: Chapter 2 outlines the EU regulatory context; Chapter 3 analyses key trends and resulting gaps; Chapter 4 sets out five illustrative case studies; Chapter 5 discusses policy options and supervisory approaches; Chapter 6 sets out EU-specific considerations; and Chapter 7 provides some concluding remarks.

11 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 9.6.2023, p. 40).

12 See European Central Bank (2025) and European Systemic Risk Board (2025).

3 EU legal and regulatory context

In the EU, traditional financial institutions such as banks, investment firms and insurance undertakings are subject to robust, risk-based regulation by a host of harmonised legal acts, such as the Capital Requirements Regulation/Directive (CRR III/CRD VI)[13], the Investment Firms Regulation/Directive (IFR/IFD)[14], the Markets in Financial Instruments Directive (MiFID2)[15] and the Solvency II Directive[16], and are also subject to supplementary, group-wide supervision under the Financial Conglomerates Directive (FiCOD)[17]. The relevant legal frameworks seek, among other things, to enable the CAs to assess these institutions' capital adequacy, risk exposures and governance at both the individual and the consolidated levels.

Systemic importance features across several (but not all) of the EU financial services regimes, serving as a determining factor for when to apply more stringent prudential requirements. This metric, which refers to the potential of an entity to disrupt the financial system upon failure, is typically assessed using a set of indicators: size, interconnectedness, substitutability, complexity and cross-border activity, as established in international regulatory standards (e.g. BCBS, 2013). Sector-specific requirements include the designation of Global Systemically Important Banks (G-SIBs) and Other Systemically Important Institutions (O-SIIs) under the Capital Requirements Directive (CRD IV)[18] frameworks and Single Supervisory Mechanism (SSM) Framework Regulation[19], the classification of investment firms under

---

13 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176 27.6.2013, p. 1) and Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

14 Regulation (EU) 2019/2033 of the European Parliament and of the Council of 27 November 2019 on the prudential requirements of investment firms and amending Regulations (EU) No 1093/2010, (EU) No 575/2013, (EU) No 600/2014 and (EU) No 806/2014 (OJ L 314, 5.12.2019, p. 1) and Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms and amending Directives 2002/87/EC, 2009/65/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU and 2014/65/EU (OJ L 314, 5.12.2019, p. 64).

15 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

16 Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

17 Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate and amending Council Directives 73/239/EEC, 79/267/EEC, 92/49/EEC, 92/96/EEC, 93/6/EEC and 93/22/EEC, and Directives 98/78/EC and 2000/12/EC of the European Parliament and of the Council (OJ L 35, 11.2.2003, p. 1).

18 Regulation (EU) No 468/2014 of the European Central Bank of 16 April 2014 establishing the framework for cooperation within the European banking supervision between the European Central Bank and national competent authorities and with national designated authorities (OJ L 141, 14.5.2014, p. 1).

19 See Articles 39 to 42 of Regulation (EU) No 468/2014 of the European Central Bank of 16 April 2014 establishing the framework for cooperation within European banking supervision between the European Central Bank and national competent authorities and with national designated authorities (SSM Framework Regulation) (ECB/2014/17) (OJ L 141, 14.5.2014, p. 1).

IFR/IFD[20], the FiCOD[21] regime for financial conglomerates and the ECB's oversight of the payment system through its systemically important payment systems (SIPS) Regulation[22] and PISA framework. MiCAR[23], the Digital Operational Resilience Act (DORA)[24], the Digital Markets Act[25], the Digital Services Act[26] and the European Market Infrastructure Regulation (EMIR)[27] also aim to capture systemic importance in crypto-asset markets, information and communications technology (ICT) infrastructure, platform-based ecosystems and central counter parties, respectively.

Investment firms that engage in activities akin to the business of credit institutions (i.e. dealing on own account or underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis)[28] are required to apply for authorisation as credit institutions, provided their total assets, at individual or EU group level, equal or exceed €30 billion[29]. This status is maintained unless the threshold is not met for five consecutive years, although CAs may waive this requirement[30] based on systemic risk, group structure and counterparty credit risk considerations.[31] Under Article 1(2) IFR, investment firms with total consolidated assets at individual or group level of between €15 billion and below EUR 30 billion, or that are designated under Article 5 IFD, become subject to supervision under the CRD[32], and to its capital buffer requirements, but do not require authorisation as credit institutions unless they meet the additional conditions of Article 8a CRD. This

---

20 The classification of investment firms under the EU prudential framework is governed by (i) the IFR, in which Article 1(2) defines the scope of investment firms excluded from the IFR and instead subject to the CRR/CRD framework (i.e. Class 1 firms), Article 4(1) sets out the classification of investment firms and the application of prudential requirements and Article 55(5) introduces size monitoring obligations relevant for threshold assessments and potential reclassification, (ii) the IFD, in which Article 5 establishes initial capital requirements for different classes of investment firms, Article 8 provides the basis for supervisory powers and classification criteria and Article 62(6) amends the Capital Requirements Directive (CRD) by introducing Article 8a, which sets out the reclassification of certain investment firms as credit institutions based on asset thresholds, and (iii) the CRR/CRD, in which CRR Article 4(1)(1)(b) defines when an investment firm qualifies as a credit institution and CRD Article 8a establishes the framework for reclassifying certain investment firms as credit institutions.

21 See Articles 3(2) and (3).

22 Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (OJ L 217, 23.7.2014, p. 16).

23 See Article 56 (e-money tokens), Article 43 (asset reference tokens) and Article 85 (crypto-asset service providers).

24 See Article 31 (designation of critical ICT third-party service providers) of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

25 See Article 3 (designation of gatekeepers) of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1).

26 See Article 33 (very large online platforms and very large online search engines) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

27 See Article 25 (central counterparties) of Regulation (EU) 2019/2099 of the European Parliament and of the Council of 23 October 2019 amending Regulation (EU) No 648/2012 as regards the procedures and authorities involved for the authorisation of CCPs and requirements for the recognition of third-country CCPs (OJ L 322, 12.12.2019, p. 1).

28 See Article 4(1)(1)b of the CRR.

29 ibid., read in conjunction with CRD, Article 8a.

30 See Article 8a(3a) of the CRD.

31 As further detailed in RTS under Article 8a (7).

32 CRD, Titles VII and VIII.

tiered approach illustrates how systemic importance[33] and cross-sectoral activity can trigger the application of stricter requirements.

Market players that engage in other financial activities, such as providing payment services (regulated under the second Payment Services Directive – PSD2)[34], the issuance of e-money (regulated under the second E-Money Directive – EMD2[35]), and non-bank lending are typically subject to lighter regulatory requirements.[36] Although it includes a tiered structure, the prudential regime for entities authorised under MiCAR remains comparatively less demanding than that imposed on banks and investment firms.

Harmonised rules apply in specific areas – such as anti-money laundering and counter-terrorist financing (AML/CFT), DORA and market conduct – providing a baseline of protections in these areas. The revised Consumer Credit Directive (CCD2)[37], applicable from November 2026, will expand its precursor's scope of protections to also encompass credit agreements below €200, interest-free credit (with fees), short-term credit repayable within three months, BNPL products and credit offered via digital platforms and mobile applications. It also covers crowdfunding and peer-to-peer lending platforms operating on a commercial basis. CCD2 introduces stricter obligations for lenders, e.g. with regard to creditworthiness assessment and pre-contractual information, as well as requirements for online interfaces, mobile applications and automated decision-making systems, to ensure processes are transparent, fair, and accountable. It also strengthens consumer rights by clarifying and harmonising provisions on withdrawal, early repayment and default charges.[38]

EU legislation is complemented by Level 2 measures developed by the European Banking Authority (EBA). The reference here is to Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS), which aim to provide technical details and which are, legally speaking, adopted by the European Commission, within the constraints of the (judicial) Meroni doctrine.[39] Additionally, the EBA can issue (and has issued, on the basis of legal mandates in EU legislation or at its own

---

33 Systemic importance refers to the potential of an entity to disrupt the financial system upon failure. This is typically assessed using a set of indicators – size, interconnectedness, substitutability, complexity and cross-border activity – as established in international regulatory standards (e.g. BCBS, 2013). For neo-conglomerates, additional dimensions, such as market capitalisation, cross-sectoral activity and the spillover effects of unregulated activities on regulated entities, become increasingly relevant.

34 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

35 See Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

36 Regulatory fragmentation may also be an issue for some of these activities, as in the case of entities active in the provision of non-bank lending, which are often regulated nationally (see EBA, 2022).

37 Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC (OJ L, 2023/2225, 30.10.2023).

38 These changes are aligned with the Mortgage Credit Directive.

39 Judgement of the Court of 13 June 1958, Case 9/56 Meroni & Co., Industrie Metallurgiche, SpA v. High Authority of the European Coal and Steel Community [1957-1958] ECR 133. In a nutshell, and on its narrowest reading, Meroni precludes the attribution to the ESAs of discretionary powers.

initiative) guidelines that legal entities and supervisory authorities are required to make every effort to comply with, unless they can justify deviations. RTS, ITS and guidelines frequently embed risk-based adjustments, particularly in areas such as AML/CFT, operational risk and governance. Moreover, supervisors are expected to exercise risk-based judgement to ensure appropriate and proportionate responses to identified risks. Additionally, the EBA is required to prevent regulatory arbitrage and to ensure the appropriate regulation of credit and other risks, and has a specific mandate to monitor and assess new and innovative financial activities.[40] Pursuant to these mandates, the EBA has issued multiple reports, accompanied by opinions addressed to the European Commission as appropriate, on matters pertaining to the regulatory perimeter, including the definition of credit institutions, other financial intermediaries (OFIs), non-bank lenders and crypto-asset-related and cloud services activities.

The European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) perform analogous functions in the financial market/securities and insurance/pensions sectors, respectively, including the development of Level 2 measures and supervisory guidelines. Where appropriate, they cooperate with the EBA on cross-sectoral mandates, particularly in areas such as digital operational resilience, crypto-assets, AML/CFT and governance.

[40] See Articles 8(1)(f) and 9(2) of Regulation (EU) No 1093/2010 of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

4 Trends, gaps and developments at the boundary of the regulatory perimeter

4.1 Unbundling and re-bundling of financial activities

Technological innovation has facilitated the disaggregation (unbundling) of traditional financial services (in the case of banking, lending and deposit-taking, payment services and investment services) and operational processes (such as customer acquisition and onboarding, product development and support, transaction processing and execution and risk management and compliance) and their re-integration (re-bundling) into separate components, allowing consumers to pick and choose specific features from different providers for a more personalised and cost-effective experience. This process of unbundling and re-bundling financial activities[41] allows new and, typically, less regulated or unregulated market entrants (covered by the term "fintechs") to develop business models that target specific parts of the value chain and often transcend conventional sectoral boundaries, allowing them to compete with incumbents by embedding financial services into non-financial platforms[42] and while operating as pure online providers (EBA, 2021). According to McCaul (2024) payments and e-commerce have become frequent entry points for such firms, which often expand, over time, into retail credit (mortgage lending and consumer loans) or crypto services. The World Economic Forum (2025) identifies digital payments as the largest business segment for retail-facing fintechs, followed by digital lending (see **Figure 1**).[43] In Europe, most digital lending firms provide balance sheet business lending services. The growth trend of peer-to-peer lending[44] has slowed somewhat[45], but other, less regulated (or unregulated) forms of retail lending, such as crypto lending (EBA/ESMA, 2025) or, according to Cornelli et al. (2023) and Ehrentraud, et al. (2024), BNPL, are becoming more popular. Wallets, multi-function apps and other central platforms are becoming mainstream, reflecting a broader trend toward embedded finance and application programming interface (API) driven ecosystems.[46] Innovations in investment advice and wealth management often include robo-advisers and personal financial management

41 See also European Banking Authority (2019b), FSB (2019a) and Himino (2019).

42 Embedded finance refers to the integration of financial services – such as payments, lending, insurance, deposits or investments – directly into non-financial applications or digital platforms, allowing users to access these functions seamlessly within the non-financial interface, rather than through the interface of a traditional financial institution (e.g. online banking).

43 World Economic Forum (2025), p. 7.

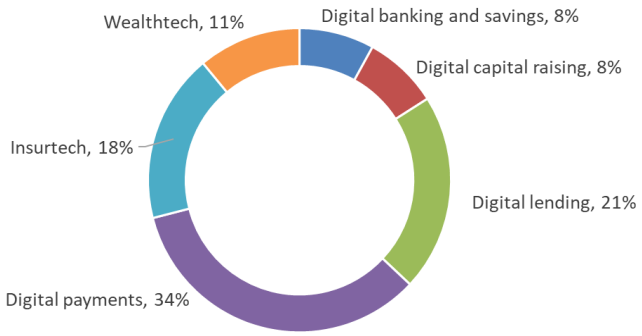
44 Digital finance refers to credit activity facilitated by platforms that match borrowers with lenders (investors). Depending on the jurisdiction, these platforms are referred to as "peer-to-peer (P2P) lenders", "loan-based crowdfunders" or "marketplace lenders". See BIS (2018).

45 According to Allied Market Research, the global peer-to-peer lending market was valued at USD 153 billion in 2022 and is projected to reach USD 1.7 trillion by 2032. Developments vary by region, with corporate lending exceeding consumer lending. North America dominated the market share in 2022, driven by higher interest rates in traditional banking and increased loan rejection rates for small and medium-sized enterprises. Asia-Pacific is expected to be the fastest-growing region, due to developments in financial institutions, minimal lending regulations and the rise of crowdlending platforms in India and Japan. https://www.alliedmarketresearch.com/peer-to-peer-lending-market

46 World Economic Forum (2025), p. 46.

tools.[47] Insurtech has also experienced remarkable customer growth, especially in emerging markets, and is increasingly serving underserved segments such as micro-enterprises and small and medium-sized enterprises, low-income populations and rural communities.[48]

Figure 1
Distribution of fintechs worldwide by business model



Sources: World Economic Forum & Cambridge Centre for Alternative Finance (2025).

The above trends are largely driven by the demand for customer convenience, service efficiency and financial inclusion.[49] They may also allow for more accurate assessment of customer risk profiles and behaviours. Open banking – defined as the corpus of laws and regulations that grant consumers greater control over their financial data and enable the sharing of information with non-bank entities[50] – often benefits fintech firms and thus increases competition (Babina et al., 2022, Doerr et al., 2023). However, they also create new risks for, and interdependencies among, financial institutions.

Given these developments, authorities face challenges in supervising firms that lie on the fringes of the regulatory perimeter, straddling the divide between the regulated and the unregulated. Depending on their business models or how they unbundle and re-bundle, fintech firms can fall within or outside different components of the applicable regulatory and supervisory frameworks, in the latter case bypassing requirements for traditionally highly regulated financial activities (such as banking). The wider the range of financial services offered without appropriate regulation, supervision and oversight, and the wider the network of jurisdictions across which their providers operate, the greater their potential to threaten financial stability.

47 ibid., p. 7.

48 ibid., pp 30-31.

49 World Economic Forum (2025), p. 4.

50 The proposed EU Financial Data Access (FIDA) framework builds on the already existing open banking access to customer data held by account-servicing payment service providers and takes a customer-centric approach. It aims to ensure that all consumers and firms have effective control tools over their financial data. It provides additional tools to ensure personal data protection in line with the General Data Protection Regulation (GDPR) and applying the general principles of business-to-business data sharing in line with the data act proposal.

4.2 Partnerships between financial and non-financial entities

Many unlicensed or lightly regulated firms partner with financial institutions: according to the World Economic Forum (2025), 84% of surveyed fintechs partner with incumbents, mainly via API integrations (52%), collaborations with technology providers (41%) and funding agreements (36%). The main drivers are access to advanced technology solutions and infrastructure, enhanced credibility and trust, and opportunities for innovation.[51] **Back-end partnerships** typically involve tech firms supporting financial entities' back-office and middle-office functions by supplying software, infrastructure or compliance tools, to improve cost efficiency, service delivery, client reach and risk management. However, these partnerships may also create dependencies, especially when financial institutions face limited visibility on the risks of outsourced solutions, or lead to high switching costs, resulting in potential "lock-in" effects.

In **white labelling** (also called **front-end partnerships)**, financial products and services are offered under the brand of a firm – that may or may not be regulated – while the licensed provider remains legally responsible for compliance but may not have a direct client relationship. In such arrangements, the white label partner controls the customer interface and acts as the primary point of contact, while the financial institution (**white label provider**) operates in the background. As outlined by the EBA (2025), this set-up may complicate the financial institutions' oversight of customer onboarding and marketing, risk assessment and compliance. However, it can enable financial institutions to leverage technological capabilities so as to achieve cost efficiencies, improve service delivery, expand their client base or offer ancillary services. This set-up may also strengthen their risk control capabilities and enhance customer value (Wang et al., 2021). Unlike traditional cobranded card issuance partnerships, some unlicensed white label partners have established complex arrangements involving multiple financial service providers.

These complex partnerships may magnify the licensed entities' exposure to common risks, including liquidity, operational (e.g. legal and conduct) and reputational risks.[52] According to the FSB (2024), complex partnerships may also give rise to resolvability risks, agency problems, adverse selection and step-in risk.[53] In white label arrangements, licensed financial services risk being reduced to generic, non-branded utilities on broader platforms, while still bearing the regulatory and risk burden. This form of commoditisation can erode customer loyalty, limit access to customer insights and destabilise deposit-based funding. Moreover, it may hamper differentiation and innovation, weakening the scope for competition on value-added services. Meanwhile, unlicensed partners, typically rewarded for client acquisition, may be incentivised to expand business without any risk consideration, shifting costs

---

51 World Economic Forum (2025), p. 4.

52 For instance, the US Consumer Financial Protection Bureau (October 2024) ordered Apple and Goldman Sachs to pay USD 89 million for mishandling transaction disputes and misleading customers about interest-free payment options. https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-apple-and-goldman-sachs-to-pay-over-89-million-for-apple-card-failures/.

53 Compare Box 3.

and risks onto the licensed entities delivering the regulated services. As highlighted by McCaul (2024), such partners often lack robust risk management capabilities, increasing the need for banks to retain control over critical functions such as onboarding, resilience and legal risk.

In addition, while unbundling can contribute to diversity and innovation, the growing dominance of certain players may give rise to concentration risks in specific activities (e.g. payment gateways and acquiring services). Providers acting as both the back-end infrastructure partners and the financial service provider (as in 5.3) illustrate how this dual role can have amplifying effects on their market footprint. Disruptions, whether technical or regulatory, could cascade across the financial system. Big Tech could similarly exert pressure by offering critical infrastructure services while embedding financial products into their consumer-facing ecosystems. Although their current focus in the EU seems to be mainly on payments and retail lending, their business models may evolve.

4.3 Market places

Neo-conglomerates operating large marketplaces, which maintain dual relationships with both vendors and buyers, have strong incentives to engage in lending, either directly or as intermediaries. This can stimulate buyer spending and support vendor growth, particularly among small and medium-sized enterprises (SMEs). As a result, overall transaction volumes increase, boosting platform revenues through higher fees and greater activity. Marketplace lending can help vendors finance inventory, product development and marketing, while buyers may benefit from more flexible purchasing options. Leveraging their scale and data access, these platforms may also negotiate favourable terms with financial institutions or offer white-labelled financial products under their own brand. However, this model could also lead to overspending, rising non-performing loans and cross-subsidisation, where one side of the market receives preferential loan terms while the other bears higher costs.[54]

4.4 Buy now, pay later arrangements

BNPL arrangements are another rapidly expanding area of financial intermediation. These arrangements – frequently embedded within mobile apps, e-commerce platforms or marketplaces – enable customers to defer payment, with merchants shouldering elevated transaction fees in exchange for greater sales volumes and higher conversion rates. BNPL providers frequently extend facilities without traditional credit checks, such as basic income verification, and repayment behaviour is often not reported to credit bureaus, although some jurisdictions are imposing requirements to facilitate responsible lending (Ehrentraud et al., 2024). While it promotes financial inclusion and supports platform growth, the BNPL model gives rise to concerns around transparency, responsible lending and consumer protection. Users of BNPL are generally described as higher risk, being typically younger

[54] Compare Gambacorta et al. (2023b).

individuals who have lower credit scores and education levels and are more indebted, with higher delinquency rates (Corneli et al., 2023)[55]

According to Statista, BNPL is projected to reach 7.4% of global e-commerce by 2028[56], with transaction volumes expected to more than double to USD 733 billion. Initially concentrated in sectors such as retail and health, BNPL has expanded into broader consumer segments and geographies, including Europe, the United Kingdom, the United States, the Middle East and Latin America. The product lifecycle shows a shift from buyer protection and simple point-of-sale credit towards layered instalment lending structures. These newer structures are frequently perceived by consumers as offering lower apparent cost and greater manageability compared with credit cards and personal loans.

Some BNPL providers are evolving into full-service lenders and payment service providers. Leveraging their extensive data access and customer reach, they increasingly compete by offering fully integrated service suites for SMEs, including fraud prevention, tax, inventory, risk and cash management (Capgemini, 2024).[57]

4.5 AI and data access

Some neo-conglomerates are also at the forefront of AI development and/or deploy it to optimise credit scoring, fraud detection, customer engagement and operational efficiency. In China, Big Tech firms have leveraged AI and alternative data to extend unsecured, short-term loans to millions of small businesses and individuals. These loans are often extended without collateral, reducing exposure to real estate cycles and enabling more dynamic credit allocation (Gambacorta et al., 2023a). While critics argue this may be due to the offering of smaller, higher-rate loans addressing short-term liquidity needs rather than long-term financing, they nonetheless expand access for underserved clients (Liu et al., 2022).

This duality underscores the need for balanced oversight, to preserve innovation while mitigating emerging risks by ensuring appropriate customer protection, robust security standards and reciprocal data-sharing obligations. As AI enables more granular customer profiling through the integration of diverse data sources, regulation must evolve to safeguard fairness, transparency and accountability, while avoiding data and technological asymmetries that could amplify competitive imbalances (Jeng et al., 2025) and financial exclusion.

Agentic AI – autonomous AI systems capable of executing tasks, learning and adapting with minimal human input – represents a further evolution of AI, with applications in financial services. According to BCG (2025), such AI agents act

---

55 However, BNPL providers Affirm and Klarna report that their delinquency rates are far lower than those of traditional credit cards in the United States (see https://investors.affirm.com/news-releases/news-release-details/affirms-underwriting-approach-and-advantage/, https://investors.klarna.com/News--Events/news/news-details/2025/Klarna-delinquency-rates-drop-as-consumer-health-improves/default.aspx).

56 Statista BNPL Market Forecast.

57 Compare pp. 25-27.

proactively, often coordinating with other agents to deliver complex, multi-step outcomes across domains such as lending, payments and wealth management. Fintechs also use them to accelerate software development and automate compliance processes. BCG highlights that agentic AI could erode traditional banking profit pools by continuously reallocating customer funds to higher-yield accounts, thereby undermining inertia-based revenue models.[58] The convergence of agentic AI with open banking may enable autonomous financial agents to manage entire customer lifecycles, from onboarding to investment. With regard to payment services, international card networks have begun equipping AI agents to autonomously execute transactions and deliver personalised shopping experiences.[59] Using tokenised credentials, authentication protocols and behavioural controls, financial institutions can enable these agents to act on users' instructions by, for instance, purchasing tickets, while maintaining oversight and compliance.

While agentic AI systems may operate autonomously, legal and supervisory responsibility remains vested in the financial institution(s) deploying that technology. In the EU, the Artificial Intelligence Act (AI Act)[60] applies to a wide range of actors involved in the development, deployment and use of AI systems, regardless of whether they are regulated financial institutions or unlicensed firms. Particular attention is required where systems fall into the high-risk category, such as credit scoring. Key obligations include embedding mechanisms to enable human oversight (e.g. to monitor, intervene in, and override AI decisions) as well as registering high-risk AI systems and complying with post-market monitoring and incident reporting obligations. Thus, agentic AI must also be subject to robust governance frameworks, including internal controls and redress mechanisms. Institutions must be able to explain how agentic AI systems reach decisions, especially in contexts with a legal, financial or reputational impact. This includes maintaining audit trails and documenting decision logic. Agentic AI systems often require access to sensitive financial data across silos, heightening data protection and cybersecurity risks.[61]

Supervisory challenges may arise where AI agents (i) initiate financial transactions, adjust credit terms or rebalance portfolios without direct human oversight; (ii) interact with multiple regulated and unregulated entities, creating opaque decision chains; (iii) operate across jurisdictions; and/or (iv) leverage open banking and fragmented data infrastructures. To address these challenges, supervisors will need to develop tools to verify decision logic, risk thresholds and behavioural patterns across ecosystems. Stress testing and scenario analysis should consider such autonomous systems and their potential systemic impact. Supervisory guidance may need updating, alongside capacity building and enhanced cooperation among CAs to monitor spillovers and consistent enforcement.

---

58 See BCG, p.15.

59 Examples include Visa's Intelligent Commerce initiative and Mastercard's Agent Pay.

60 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024).

61 See Visa (2025), Agentic Commerce: The Threat Landscape.

4.6 Decentralisation and DeFi

Crypto-asset services and the rails they operate on – distributed ledger technology (DLT) – have received significant regulatory attention in recent years. The CPMI/IOSCO (2022) issued guidance on applying its Principles for Financial Market Infrastructures to stablecoin arrangements. The FSB (2023a) released "High-level recommendations for the regulation, supervision and oversight of crypto-asset activities and markets", as well as "Revised high-level recommendations for the regulation, supervision and oversight of 'global stablecoin'", and analysed the Financial Stability Risks of Decentralised Finance (FSB, 2023c) as well as the Financial Stability Implications of Multifunction Crypto-asset Intermediaries (FSB, 2023d). For its part, the BCBS (2022) released a standard for the prudential treatment of banks' crypto-asset exposures. The IOSCO (2022) issued Policy Recommendations for Crypto and Digital Asset Markets to address concerns related to market integrity and investor protection arising from crypto-asset activities. In the EU, MiCAR became fully applicable at the end of 2024, and the BCBS crypto standard has been already partially implemented through CRR3 and CRD VI.

Despite the SSB and legislative efforts, the continued expansion of crypto markets outside the regulatory perimeter remains a fact that is likely to pose growing financial stability concerns. This is particularly relevant, given the increasing interlinkages with the traditional financial sector, as evidenced by the US banking turmoil in March 2023, which had its roots, at least in part, in the collapse of the Terra-Luna ecosystem. Notably, the failure of FTX, a vertically integrated multi-function crypto-asset intermediary (MCI), played a catalytic role in the 2023 turmoil, underscoring the systemic implications of such entities (FSI, 2024). MCIs – entities that combine multiple functions, such as proprietary trading, custody, lending and issuance[62] – have gained significant market share and, in some jurisdictions, may already enjoy oligopolistic positions in the crypto market. Their dominance is often reinforced by network effects, data advantages and cross-subsidisation across business lines. Several high-profile cases have revealed serious governance failures, deficient risk management and misconduct within crypto firms. Such events – which had spillover effects within the sector and beyond – highlight the urgent need for transparency, regulatory clarity and supervisory oversight. The operating model of MCIs (off-chain recording of crypto-asset transactions) may facilitate malicious actors' money laundering efforts and aggravate the problem of insufficient data on crypto-assets. Various enforcement actions undertaken by supervisory authorities around the globe in recent years prove the vulnerability of MCIs to financial crime, likely aggravated by inadequately managed conflicts of interest. Garcia Ocampo et al. (2026) highlight that many of the largest MCIs engage in bank-like intermediation, borrowing from customers to fund lending and leveraged transactions, thereby taking material credit, market and liquidity risks. These observations align with the authors' assessment that, in the case of these entities, comprehensive consolidated supervision and proportionate but risk-sensitive prudential requirements (capital and liquidity) are warranted, for the sake of robust governance and risk management arrangements.

[62] The ESRB refers to MCIs as multi-function groups active in crypto-asset markets (ESRB, 2025).

In the European Union, some large third-country stablecoin issuers have established or acquired multiple, smaller e-money institutions (EMIs), which are only supervised, on an individual basis, exclusively for their EU operations. In parallel, concerns are growing around "third-country multi-issuer schemes"[63], where a particular stablecoin is jointly issued by entities based in different jurisdictions, with the tokens marketed as "fully fungible", thereby allowing stablecoins issued in a third country to be treated as "interchangeable" with those issued within the EU, for example. As highlighted by the ECB (2025), this represents a "material deviation from traditional risk management and supervisory standards". For the first time, an EU entity and, by extension, its prudential supervisor, would effectively become accountable for both EU and third-country issuers alike, and for their respective liabilities, in circumstances where issuer A could not realistically be expected to fulfil issuer B's obligations. Such schemes risk undermining MiCAR's prudential safeguards, weaken the EU's strategic autonomy, facilitate regulatory arbitrage and incentivise non-EU holders to redeem tokens with EU entities – potentially draining EU reserves and amplifying contagion risks (e.g. a "run" on EU issuers, resulting in spillovers to EU banks where issuers' deposits are placed). Third-country multi-issuer schemes also create a structural mismatch between local supervisory reach and global risk exposure, as they do not countenance the need for (i) third-country issuers to be subject to equivalent regulatory standards, (ii) reciprocity agreements, and/or (iii) legally enforceable asset transfer mechanisms, especially in crisis situations. The multi-issuer scheme's inherent risks are compounded by the fact that crypto-lending, borrowing and staking are often unregulated, facilitating further regulatory arbitrage and the unchecked growth of multifunction crypto-asset intermediaries. It follows that third-country multi-issuer schemes could become sources of systemic risk, which policy makers will need to analyse and guard against.[64]

Another phenomenon on the rise is that of decentralised finance (DeFi), where financial services are offered through open-source protocols, on decentralised platforms, without the involvement of traditional intermediaries. DeFi platforms can be vulnerable to cyberattacks and fraud, and their lending activities are typically conducted anonymously, relying on collateral value rather than on borrower creditworthiness (EBA/ESMA, 2025). The DeFI ecosystem is heavily dependent on "smart contracts", which automate lending and borrowing but lack the relationship-based trust mechanisms of traditional finance.[65] DeFi lending is characterised by opacity, concentration of liquidity providers, and re-hypothecation practices, often resulting in high leverage. Over-collateralisation is the primary risk mitigation tool, but this model may prove fragile under stress because of the uncertainty about the backing of certain stablecoins and the high volatility of other crypto-assets. Born et al. (2022) argue that if DeFi continues to grow, it could become a source of systemic risk (e.g. via tokenised assets, custody services or investment products). In addition, many decentralised platforms are, in practice, controlled or significantly influenced by

63 Referred to as multi-jurisdictional stablecoin in BCBS and FSB publications.

64 For ways in which these risks can be addressed, see ESRB (2025).

65 The reference is to contractual arrangements embedded in computer software, which the latter can validate, execute and record automatically, on a DLT platform, as soon as certain pre-programmed/pre-defined conditions are met, based on information fed into the distributed ledger or received from a pre-defined source.

identifiable entities and, therefore, fall into the category of "decentralised in name only" – DINO (Sims, 2024). Thus, some jurisdictions have recognised Decentralised Autonomous Organisations as legal entities, issued guidance for DAOs or otherwise included them in the regulatory framework.[66]

Box 1

Crypto-based staking, lending and borrowing

This box summarises key findings on crypto-based staking, lending and borrowing from the ESMA and EBA Joint Report (January 2025). Any interpretations are those of the authors.

Crypto-based staking, lending and borrowing activities currently remain largely outside the scope of EU and national regulation, except when conducted by professional lenders (e.g. banks). MiCAR[67] excludes these activities from its scope, but mandates the European Commission[68] to assess the need for regulating them based on a consultation of the EBA and ESMA, and to report to the European Parliament and the Council[69], together with a legislative proposal where appropriate.

Crypto lending involves a user (lender) transferring crypto-assets or funds to another user (borrower) against the commitment to return the equivalent value plus an interest payment on a future date or upon a trigger event. In **crypto borrowing,** the roles are inverted. **Crypto staking** is a contract where one party confers to a protocol certain crypto-assets with the goal of receiving a return. The crypto-assets are used by the protocol in the context of proof-of-stake blockchains. Improper staking may result in slashing, where staked tokens are used to pay compensation to parties damaged by the underperformance of the validator.

Crypto lending, either offered by legal entities (centralised) or through smart contracts (decentralised), relies on a very high level of collateralisation, given the absence of borrower creditworthiness. Centralised services are typically structured around over-collateralisation, with loan-to-value ratios commonly ranging between 20% and 80%, depending on collateral asset volatility. Accepted collateral mainly comprises highly liquid crypto-assets, such as Bitcoin and Ether, with some platforms accepting utility tokens under stricter conditions. Interest rates generally range from 8% to 15%, though EBA/ESMA identified instances exceeding conventional usury thresholds. Liquidation is generally triggered at a loan-to-value ratio of around 85%, with limited grace periods and additional fees, further exacerbating borrower losses in volatile market conditions.

EBA/ESMA stress that crypto lenders may be highly leveraged and exposed to credit and liquidity risk[70]. Annunziata et al. (2025) warn that the materialisation of these risks could trigger the failure of these entities and jeopardise the provision and repayment of credit in crypto-assets. The 2022 market downturn, which coincided with the collapse of several major market players, illustrates this.

DeFi lending operates through smart contracts and algorithmically managed liquidity pools, without the involvement of intermediaries or creditworthiness assessments. Key models include (i)

66 The reference is to certain US jurisdictions (such as Wyoming and Vermont), as well as to Switzerland, Malta, Singapore, Estonia and Gibraltar.

67 See MiCAR, Recital 94.

68 ibid., Article 142.

69 MiCAR provided for this to take place by 30 December 2024, but the report was delayed. The EBA/ESMA Joint Report was published in January 2025.

70 EBA/ESMA (2025), pp. 50 ff.

collateralised debt positions, where users lock collateral to mint stablecoins, and (ii) collateralised debt markets, facilitating lending through peer-to-peer matching or pooled liquidity. These protocols are highly composable, enabling user engagement in complex leveraged strategies and collateral chains. While this can enhance market efficiency, it also amplifies systemic risk due to interconnectedness, the absence of circuit breakers and procyclicality during periods of market stress.

Crypto borrowing services are typically offered by platforms aiming to generate yield on user-held crypto-assets. They may be structured either as direct counterparties or through intermediaries matching lenders and borrowers, sometimes via DeFi protocols. The investment returns paid generally range from 4% to 16%, with intermediaries charging commissions of 15% to 30%. Routing through DeFi protocols adds layers of complexity and risk, particularly in terms of transparency, adequacy of custody and exposure to smart contract vulnerabilities.

Staking refers to the immobilisation of crypto-assets to support the consensus mechanisms of proof-of-stake blockchains. Staking models comprise solo, pooled, validator-as-a-service and liquid staking. Liquid staking protocols issue tokens representing claims on staked assets, which can be reused as collateral in DeFi, enabling leveraged staking and re-staking strategies. These introduce multi-layered systemic risks, especially during de-pegging or liquidity shocks. Staking rewards may vary significantly across networks and providers, with annual investment yields ranging from 2.3% to 7.7%. The associated risks, which include slashing penalties, custody vulnerabilities and the loss of access to staked assets during unbonding periods[71], are high.

EBA/ESMA identified consistent risks across all models, with consumer protection as a primary concern. Users often receive insufficient or misleading information on fees, yields, collateral terms and dispute resolution. Market risk is elevated due to the inherent volatility of crypto-assets, which can trigger forced liquidations and procyclical feedback loops. Operational and ICT risks are acute in DeFi, where smart contract vulnerabilities, oracle manipulation and private key compromise are prevalent. ML/TF risks are exacerbated by the absence of gatekeepers and the anonymity or pseudonymity of operators, which hinders traceability. Systemic risk is amplified by leverage, rehypothecation and market concentration, especially in liquid staking protocols, which introduce multi-layered exposures and potential contagion channels.

Despite significant data limitations, EBA/ESMA found that crypto lending, borrowing and staking attract a niche of digitally literate, investment yield-seeking EU retail clients, but remain largely inaccessible or unattractive to the broader public due to complexity, risks and regulatory gaps.

At the time of the report, EU banks had minimal exposure, with only about 5% of significant, SSM directly supervised institutions actively exploring such services. One US bank announced that it was considering accepting crypto-asset-related exchange-traded funds as collateral[72], something that is feasible in the United States, where the Basel Committee's standard on the prudential treatment of crypto-assets has not yet been implemented. In the EU, this would be capital-intensive. Nevertheless, some EU financial institutions partner with or outsource to unregulated entities to offer crypto lending, borrowing or staking. While such collaborations may provide access to technical infrastructure and liquidity, they pose risks related to transparency, accountability and

71 Staked crypto-assets are subject to a "bonding period", which is a length of time set by the protocol after which the owner of the crypto-assets becomes eligible to earn rewards. The "unbonding period" is a length of time (hours, days or weeks) set by the protocol to "unstake" a crypto-asset.

72 See https://cointelegraph.com/news/jpmorgan-accept-crypto-etfs-collateral-loans-report.

consumer protection, particularly when users are unaware of third-party involvement, and may, in the absence of harmonised standards and supervisory oversight, facilitate regulatory arbitrage and create systemic vulnerabilities.

4.7 Data and information-sharing gaps

Current supervisory practices involve significant frictions in the collection, sharing and utilisation of data across institutional and jurisdictional boundaries. For example, while some information is available through national or EU-level data collections focused on specific financial activities, access is often limited to home authorities. Access is also limited to specific authorities, such as prudential supervisors, payment system overseers, consumer protection bodies, CAs under MiCAR, securities or insurance supervisors or those operating under national frameworks. While the Commission's proposal to facilitate data-sharing and reduce redundant reporting in EU financial services[73] is expected to remove barriers to information exchange among EU-level authorities and reduce duplicative data requests to financial institutions and other market participants, it excludes relevant national CAs (NCAs) from its scope. This is a significant shortcoming, as some NCAs may be reluctant to share supervisory data, driven by the desire to safeguard jurisdictional autonomy, protect domestic financial actors or markets or, in certain cases, avoid external scrutiny of potential regulatory shortcomings. Consequently, EU-level institutions risk being left without access to the bulk of supervisory data, thereby undermining the overall effectiveness of the system.

For passported activities, EU supervisors collect information at the time of authorisation and share it with other Member State authorities via notification procedures. However, the initial business plans of firms can evolve rapidly. The activities notified as part of the passporting process frequently encompass a broad range of services, of which only a subset are actually offered in some, at least, of the Member State jurisdictions. Firms often test, introduce and drop services, or pivot their business models, without necessarily informing their supervisors. Even when updates are reported, onward sharing with host authorities is not systematically ensured. Registers and data collections may also lack harmonised company identifiers, making it difficult to consolidate group information. Overall, this leads to incomplete, inaccurate and often delayed communication between firms and their home and host authorities (ESAs 2019, 2022).

Neo-conglomerates may further complicate supervisory oversight by carrying out financial services-related business through unlicensed entities within the group, using brokerage arrangements, agent networks or white label partnerships. Although attempts have been made to evaluate these practices through ad hoc data collections, the resulting information remains incomplete. These groups may also hold multiple licences across different EU jurisdictions, leaving individual supervisors

[73] See Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 1092/2010, (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2021/523 as regards certain reporting requirements in the fields of financial services and investment support.

with only a partial view of activities that may appear monoline but are, in fact, more complex.

Ongoing risk reporting is also not standardised (ECB, 2024). For instance, while some Eurosystem central banks require detailed reporting, other authorities impose minimal or no requirements. Moreover, the underlying data are not consistently shared among the CAs. As a consequence, for firms engaged in multiple activities, such as payments, crypto-assets or non-bank lending, there is no assurance that own funds will appropriately mitigate consolidated risk exposures.

Another example of data fragmentation is that firm-specific information is often lost in submissions to EU institutions. Supervisors typically aggregate data across all licences before submission, eliminating the granularity needed for firm-level risk assessments. This is evident in the reporting of fraud statistics under PSD2.

The ESAs' European Forum for Innovation Facilitators (EFIF)[74] developed a matrix to take stock of financial services carried out in the EU by Big Tech and other selected mixed-activity groups (which both form part of neo-conglomerates), building on previous data collections: however, these efforts only resulted in the publication of a fact sheet (ESAs, 2024, 2025) containing information on licences and an announcement of next steps to enhance transparency and data-sharing.

The European Commission's study on mixed-activity groups, which approached firms directly, also faced significant data limitations.[75] Many firms declined to participate or did not identify themselves as MAGs, reflecting ambiguity around the concept and raising possible regulatory concerns. Even among the respondents, key data, such as information on risk management and capital structures, were often unavailable or depended on voluntary disclosure. Publicly available data were also insufficient, due to materiality thresholds and the blending of EU and non-EU activities. Together, these limitations undermined generalisable conclusions.

The above examples reflect a serious institutional shortcoming in data reporting and information-sharing that should be urgently addressed, both generally and specifically for neo-conglomerates. The continued dependence on public sources, anecdotal accounts and fragmented registers negates analytical rigour and creates scope for systemically relevant blind spots, being clearly inadequate for identifying and managing emerging systemic risks in a complex and evolving financial landscape. A holistic response would entail addressing reporting gaps on unregulated activities that are intertwined with financial services, such as crypto borrowing, lending and staking, as well as in the ancillary services of financial service providers. The resulting challenge is compounded by the general absence of internationally accepted, harmonised, definitional solutions for innovative products, services and processes in the financial industry, whether for statistical or other classification purposes. The status quo hampers consistent data collection and comparability across jurisdictions, further exacerbating the opacity of emerging financial activities (Kalckreuth et al., 2022).

---

74 See https://www.eba.europa.eu/european-forum-innovation-facilitators.

75 See European Commission (2024).

5 Case studies

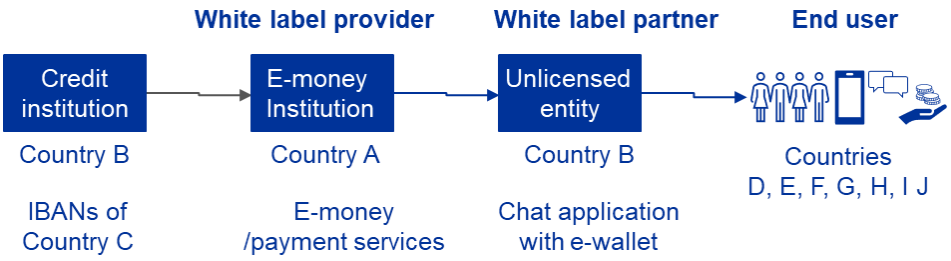
The case studies below are included for illustrative purposes only, to highlight potential gaps in the EU regulatory perimeter. They should not be interpreted as implying any judgement at all of the soundness or governance of the firms concerned or of the effectiveness or adequacy of the actions taken by the relevant supervisory authorities. The cases are, thus, intended to be indicative of broader categories and of similar arrangements amongst market participants that currently exist or may exist in the future.

5.1 Cross-border white label arrangement

Business model and licensing

Case Study 1 concerns a digital wallet embedded within a messaging platform to enable peer-to-peer money transfers, e-wallet functionalities and bank transfers directly within the chat interface. At the time of writing, this service was available in seven EU Member States, with plans for expansion to at least one non-EU country. The arrangement holds a dominant position in one Member State, with over 90% smartphone penetration.

Figure 2: White label/fintech partnership, Case Study 1



Source: ECB.

The service is offered via a white label arrangement with an EMI authorised in another Member State, which passports its services to all EU Member States, covering the issuance and redemption of e-money, the execution of payment transactions (including those covered by credit lines), money remittances and the provision of payment initiation and account information services (AIS). This EMI is positioned as a global financial infrastructure provider, offering APIs, hosted checkout, virtual terminals and embedded fintech solutions. It supports card acquiring, cross-border payments and multi-currency virtual accounts.

A credit institution licensed in Country B issues Country C international bank account numbers (IBANs) to support the white label partner's bank transfer functionality.

Although the operator of the messaging app owns a credit institution, it does not appear to be involved in the white label services: it only has a narrow operational scope, focusing on merchant services and loyalty programmes.

The white label partner does not hold a financial licence and is not subject to direct prudential supervision. Nevertheless, it acts as the customer-facing interface, controlling the user experience and brand. The EMI acts as the white label service provider. It is legally responsible for the regulated services and manages the payment transfers, but appears to have outsourced the issuing of IBANs to the bank in Country B (that previously held a payment institution (PI) licence in Country C, and still maintains Country C virtual IBANs for some of its clients).

From a functional perspective, the wallet offers a seamless user experience. The account can be set up in under two minutes by verifying the user's identity, linking a payment method (e.g. a card or local bank transfer) and activating security features such as personal identification number (PIN) codes or biometric authentication. Small-value transactions require only basic personal information, while higher-value transactions trigger enhanced identity verification. Users can instantly send money to messaging app contacts, and the transaction appears directly in the app. Recipients without a wallet are prompted to create one within seven days to redeem funds transferred to them. Bank transfers are also supported, although these may take several days to settle. Card details are not shared with recipients, and transaction records are stored within the app, as well as in the white label provider's infrastructure.

Potential regulatory gaps and risks

The above white label arrangement allows an unlicensed entity to offer financial (fund transfer) services without being directly supervised. The arrangement creates ambiguity around accountability, particularly for host supervisors, in cases of fraud, service disruption or data breaches. The management of core compliance processes, such as customer onboarding and transaction monitoring, may give rise to concerns, and the same is true of outsourcing to an unregulated entity, for example with regard to the effectiveness of anti-money laundering measures and consumer protection safeguards.

Moreover, the cross-border nature of the arrangement complicates supervisory oversight. By virtue of the EMI's licence in Country A, the wallet is available in multiple EU jurisdictions (through passporting). Despite the service's significant presence in Member State D, the supervisor of Country D reported that, when approaching the white label partner as host supervisor, the firm declined to share information on the payment service offered through its platform. The host also engaged with the home supervisor of the EMI, which indicated that it only had limited insights into the white label partner and its relationship with the white label provider. Home and host cooperation appears to be reactive, which may constrain the host's ability to monitor risks, enforce compliance or respond effectively to incidents. The scale of the wallet's operations in Country D and its international expansion have prompted questions about systemic importance, which the host supervisors cannot assess as they only have access to public information on the use of the messaging

app but no insights on the payment service itself. White label services may not yet have received attention from all home authorities.

Supervisory implications and policy considerations

Case Study 1 underscores the need for a more robust and harmonised regulatory response to white labelling and embedded finance. The EBA considers enhancing disclosure practices to be one of the follow-up actions to their 2025 report, to ensure that consumers are clearly informed of the identity of their financial service provider(s) and the applicable regulatory protections, particularly where the unlicensed partner is the user's primary point of contact. As a general proposition, direct licensing of white label partners should enhance transparency, accountability and supervisory effectiveness.

Case Study 1 also highlights the fact that white label activities are not necessarily included in group-wide supervision, even though a bank is part of the group. Home/host cooperation should be strengthened, and consideration could be given to how best to enable host supervisors to engage voluntarily with, and support, home supervisors, as well as receive information, particularly where the service demonstrates material importance in the host country.

Having examined the evolving value chain in the distribution of financial services, with a focus on white labelling in banking and payments, the EBA reports that at least 35% of banks engage in such arrangements.[76] The EBA also confirms a lack of transparency for consumers on the contracting entity, exposure to fraud and mis-selling and difficulties in complaint-handling procedures. For providers and partners, business model, operational and reputational risks, as well as potential step-in risk, predominated, alongside, in some cases, compliance issues related to onboarding, credit assessment, transaction monitoring, limited insight into product suitability and a heightened risk of losing customers if the partnership ends. Challenges for supervisors related to the opacity of the structure, inconsistent visibility and regulatory qualification of different parts of the distribution arrangements and divergent supervisory expectations. Additional concerns arise due to the potential for overlapping responsibilities for customer due diligence in the context of AML/CFT, as well as the lack of direct supervision over partners – especially when they are unregistered or unauthorised entities or are located in other jurisdictions – and deficiencies in home/host notification practices. The EBA notes that the growing role of digital platforms, marketplaces and Big Tech as white label partners adds further complexity and needs to be proactively assessed, identifying a need for supervisory convergence and observing that supervisors rarely focus on white labelling business models in the context of line supervision.

5.2 Complex multi-partner white label arrangement

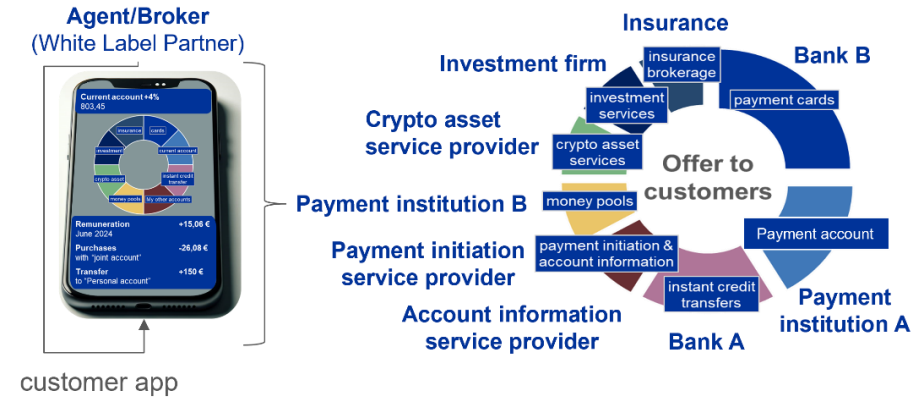
Case Study 2 explores an even more intricate and multi-layered variant: an **unlicensed firm offering a bundle of financial services** – payments, retail lending,

[76] EBA 2025 Spring Risk Assessment Questionnaire.

insurance, investment products and crypto-asset transactions – via **partnerships with over ten licensed institutions**, all integrated into a single mobile app. This business model reflects risks commonly associated with white labelling, such as: (i) operational risks stemming from IT complexity and interdependencies among institutions connected via API platforms; (ii) liquidity, solvency and capital planning risks for depository institutions, particularly where activities are large in scale or highly concentrated; (iii) step-in and compliance risks for licensed partners; and (iv) consumer protection concerns, including the potential for misleading information and unclear accountability. However, in Case Study 2, the complexity of the unlicensed partner's business model exceeds the control of the white label providers. Each institution remains responsible for its specific service, with none having an overview of the broader interdependencies created by the platform. The individual arrangements are typically not classified as critical outsourcing from the perspective of the white label provider, and thus face limited third-party risk scrutiny. Yet, when re-bundled through a single interface, they may constitute a synthetic form of regulated activity and, in extreme cases, may reach the threshold of systemic importance.

Figure 3

Complex white label arrangement, illustration of the initial set-up



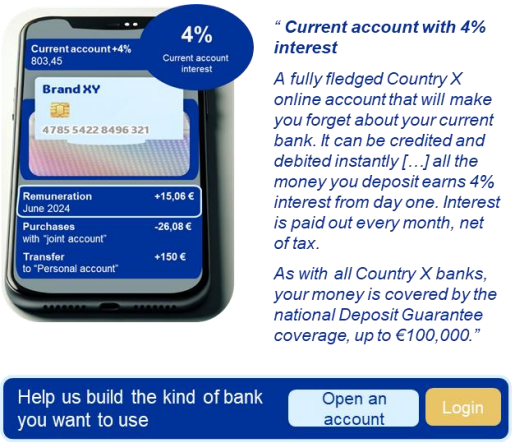
Source: ECB.

Supervisory response and remaining gaps

The initial supervisory response relied on moral suasion, which ultimately led to the licensing of the firm as an EMI and non-bank lender under a national regime. The firm has continued to operate under agent registrations and has expanded into eight countries, serving over eight million users under two brands. Several regulatory challenges remain, many also relevant for other EU-based firms with similar models. The absence of a comprehensive regulatory and supervisory framework for re-bundled financial activities is a key problem, leading to (i) fragmented oversight and inadequate monitoring of the full range of financial and ancillary services provided; (ii) entity-level capital requirements, which may not reflect group-wide risk; (iii) the absence of liquidity requirements; and (iv) less stringent financial resilience requirements.

While the firm has, in the meantime, applied for a banking licence, other firms may continue designing models and marketing strategies to remain outside the regulatory perimeter.

Figure 4
Example of misleading advertising



Source: ECB.
Note: This image reproduces the advertising to illustrate the offering without identifying the firm.

In addition, certain practices in selected EU Member States allow **EMIs and PIs to pass on interest** earned from customer funds held with banks. While EMD2 prohibits EMIs from paying interest on e-money balances, a workaround has emerged: EMIs may place customer funds with a licensed bank that pays interest on these funds, and then pass it on to customers, provided they act solely as a conduit. Some NCAs, including Germany, Austria and the Netherlands, accept this practice, as long as the EMI gains no economic benefit from the interest and the arrangement does not resemble deposit-taking. Such market practices have also emerged in other countries, while in others such practices are either explicitly prohibited or decisions have yet to be taken on their permissibility. Another workaround involves the white label partner acting as a broker for the bank. In this model, although it may appear to the customer that the funds are held in the wallet, the funds are in fact deposited with the bank, which maintains a direct contractual relationship with the wallet holder. However, risks for the depositor may arise if, at any time, the white label partner comes into possession of the funds or has the ability to instruct fund transfers (e.g. from one bank to another, because the latter offers better rewards to the broker, although it may be less creditworthy) or is involved in executing any of the transactions. Moreover, these funds are likely to be more volatile than traditional deposits, resulting in higher liquidity risks for the depository bank. Banks may not in all cases be able to form an accurate view of the depositors' behavioural patterns, which could, in turn, compromise their capacity to assess the liquidity risk inherent in this type of funding source.

Box 2

Examples from the United States of white labelling risks and enforcement

The Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Federal Reserve Board enforcement actions against Patriot Bank (January 2025), Evolve Bank & Trust (14 June 2024), Cross River Bank (8 March 2023) and Blue Ridge Bank (August 2022) illustrate how risks related to white labelling materialise in practice.[77] In particular, the bankruptcy in April 2024 of Synapse Financial Technologies, a middleware provider for numerous fintech companies, highlighted the complexities and dependencies created by the involvement of multiple third parties.[78] Synapse offered application programming interfaces and technological infrastructure to integrate banking services into fintech applications. This event revealed the challenges licensed partners face in managing and overseeing custodial deposit accounts, showcasing the limitations of indirect supervision.

5.3 Large neo-conglomerate

Case Study 3 examines a large, interconnected financial group that has reached systemic importance within the EU by accumulating monoline licences, primarily through mergers and acquisitions. Structured as a listed, EU-based company, it holds multiple authorisations, including an EMI and several PI licences, a reinsurance licence and other national authorisations for critical financial service infrastructures.[79] It operates through subsidiaries and branches across more than ten Member States. Most of the group's licensed entities have exercised their passporting rights, establishing branches or appointing agents in other Member States. The group also maintains seven other interconnected financial service infrastructure locations which, while not subject to local licensing requirements, can be considered essential nodes of the EU payments ecosystem. In principle, one EMI licence, the reinsurance licence and the national licences for critical infrastructures would be sufficient. The group also acts as white label partner in several jurisdictions.

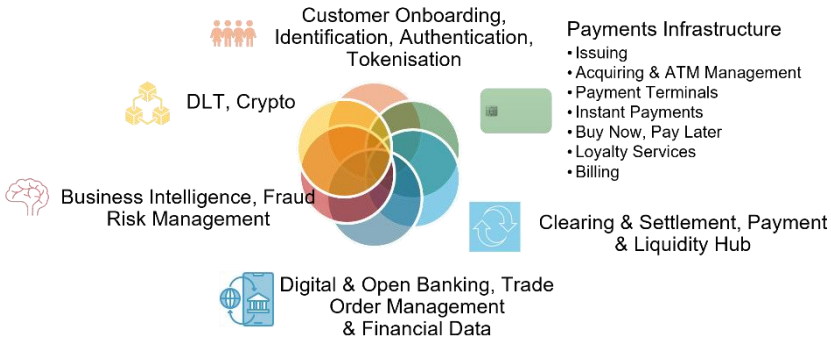
The group offers a broad suite of services spanning digital banking, payments and crypto-related activities, including transaction processing, business intelligence, fraud prevention, compliance, customer onboarding, infrastructure provision and multi-channel transaction management. Operating under multiple brands, the group serves corporate and financial sector clients within the EU and beyond.

77 The reference is to operational risks (e.g. control, security, resilience), financial risks (e.g. inadequate credit underwriting practices, weak internal controls over financial transactions), compliance (e.g. BSA/AML, consumer protection) and reputational risks. The crucial role of third parties in ensuring that all transactions and account activities comply with regulatory requirements, protecting consumers from potential fraud and ensuring the integrity of the financial system, was identified.

78 See FDIC (2024).

79 Such licensing is not harmonised in the EU. This could be envisaged under a review of DORA.

Figure 5
Overview of group services, Case Study 3



Source: ECB.
Note: The group offers services across digital banking, payments and crypto, including processing, business intelligence, fraud prevention, compliance, customer onboarding, infrastructure and multi-channel transaction management.

Systemic footprint

The group's scale and reach are considerable: its reported revenues are substantial, and in 2025 it ranked among the largest payment service providers in Europe and globally. Within the EU, the group holds a dominant market position in card issuing services and processing of account-based payments, serving more than one million corporates and hundreds of financial institutions, including a material share of the EU's significant banks. Many banks describe the group's services as difficult or even impossible to replace, underscoring its critical role in the financial infrastructure.

The group operates multiple, interconnected data centres in Europe, where it processes most of its global transaction volumes. These facilities, certified under multiple standards, constitute core infrastructures for the EU payments ecosystem. As financial institutions, the licensed entities are required to comply with DORA. However, in the authors' view, the group's scale and centrality may warrant reflection on whether it should be designated as a critical ICT third-party service provider, triggering joint oversight by the ESAs for DORA compliance purposes.[80] However, due to the combination of thresholds and criteria established in the designation framework, the group has not, so far, been classified as such.

Potential regulatory gaps

Despite its systemic relevance, the group is subject to fragmented monoline supervision, with no consolidated supervisory framework or college of prudential supervisors (due to the absence of a bank in the group). As a result, no single authority has an overview of the group's risk profile and governance, with cross-border operations remaining largely beyond the prudential perspective.

The group's designation under DORA would help to address any operational resilience concerns but may not mitigate other risks (e.g. prudential or systemic). Moreover, the group's extensive operations in third countries underscore the need

[80] See Article 31(2) of the DORA. The designation of an ICT third-party service provider is based on its potential systemic impact on financial services, the importance of the financial entities it serves, their reliance on its critical services and the difficulty of substituting or migrating away from it.

for structured supervisory cooperation beyond the EU-level, e.g. through joint supervisory colleges, data-sharing agreements and mutual recognition frameworks, in order to ensure effective oversight of cross-border systemic actors.

Supervisory implications

It follows from the foregoing that neo-conglomerates can replicate the systemic footprint of traditional financial institutions, but without the benefit of consolidated supervision.[81] Operating through exemptions[82] and monoline authorisations (e.g. as a PI[83], a non-bank lender[84] or a crypto-asset service provider[85]), combined with brokerage or agency arrangements and front-end/back-end partnerships with licensed firms, neo-conglomerates often remain below regulatory thresholds. This architecture may obscure the risk profile of their group-wide activities. Although it can enable scalability, innovation and competition, it can hinder the authorities' ability to assess the adequacy of capital, governance and risk management practices and hamper the detection of critical interconnections and dependencies, potentially masking emerging systemic risks.

This phenomenon is not new. The limitations of sector-specific supervision in capturing the full scope and the systemic risks of financial conglomerates were evident during the Global Financial Crisis and formally recognised in the BCBS Joint Forum's 2012 principles by Noble (2020) in the context of discussions about the role of Big Tech in finance. Today's neo-conglomerates have prompted similar concerns. Operating across both regulated and unregulated domains, they embed financial services within broader business models and often adopt opaque corporate structures. Leveraging digital infrastructure, data-driven strategies and cross-border platforms, they scale rapidly through innovation, acquisitions and strong market capitalisation, potentially attaining systemic relevance before supervisory frameworks can adapt. This underscores the need to reassess the adequacy of existing supervisory frameworks. Traditional, siloed and sector-specific approaches may no longer suffice. New tools and approaches may be needed to address the risks posed by neo-conglomerates, such as enhanced cross-sectoral coordination, increased transparency requirements and expansion of the regulatory perimeter to ensure timely identification and mitigation of systemic risks. However, the absence of international standards or supervisory college arrangements tailored to neo-conglomerates make effective cross-border oversight challenging.

Several other large firms have adopted similar business models in the EU and have likewise reached substantial scale. According to the Nilson Report (2025), the largest merchant acquirers in Europe in 2024 (measured by number of transactions) were predominantly non-bank entities (see Figure 6).

---

81 As defined under FiCOD.

82 For example, under PSD2 and EMD2, entities may benefit from the limited network exemption or the small EMI waiver or the exclusion for certain low-value transactions for providers of telecommunication services.

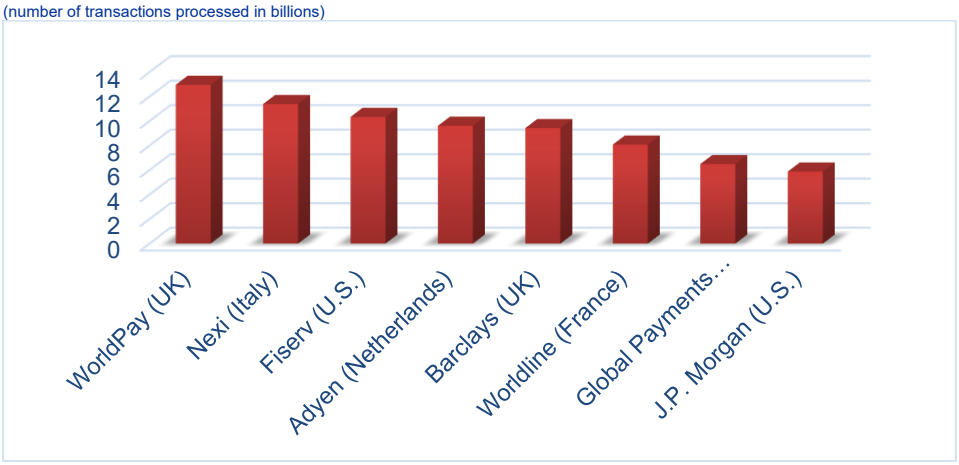
83 Under PSD2.

84 Under national regimes.

85 Under MiCAR.

Figure 6

Biggest merchant acquirers in Europe 2024, based on number of transactions



Sources: Statista, "Europe's leading payment card processors for merchants" – Merchant acquirers based on number of transactions processed (in billions) in 2024. Data retrieved from the "Nilson Report", June 2025.
Notes: The figures include credit, debit and prepaid card transactions across global brands (Visa, Mastercard, American Express, Diners Club, UnionPay and JCB) and domestic-only brands (e.g. Russia's MIR, Türkiye's Troy). The countries covered are Denmark, France, Ireland, Italy, the Netherlands, Russia, Sweden, the United Kingdom and the United States, and are thus not consistent with the EU. Moreover, data may be rounded or estimated and thus should be interpreted with caution regarding EU-wide coverage.

Only three banks ranked among the top eight. While the exact figures should be interpreted with caution, given that the data include some non-EU countries and do not cover all EU Member States, the trend appears settled: certain non-bank groups have outpaced banks in specific segments of payment services.

Box 3

Limits of traditional conglomerate regulation

Neo-conglomerates are similar in some ways to traditional financial conglomerates: FiCOD may therefore offer useful reference points for addressing risks posed by these emerging structures. Introduced in 2002, FiCOD was designed to strengthen the supervision of financial groups operating across banking, insurance and investment services. It equips supervisors with tools for coordinated oversight, capital adequacy, enhanced transparency and reporting and consumer protection measures. After the financial crisis, FiCOD amendments addressed supervisory gaps by empowering authorities to oversee parent entities, such as holding companies, and enabling concurrent supervision of banking, insurance and supplementary activities. Subsequent updates through CRDs IV to VI expanded the Directive's scope, recognising crypto licences as financial institutions.

FiCOD is aligned with the BCBS Joint Forum's Principles for the Supervision of Financial Conglomerates (2012). Despite its enhancements, it does not encompass the risks posed by neo-conglomerates grouping the activities of lightly regulated institutions. FiCOD's applicability is constrained by several structural thresholds: the group must include a bank, insurance undertaking or investment firm; financial sector activities must exceed 40% of the group's total balance sheet; and both banking/investment and insurance activities must be present. Neo-conglomerates may circumvent FiCOD's applicability by adopting agent-based or broker-based models, providing non-financial activities or avoiding combining bank and insurance services. Given these limitations, FiCOD is generally inapplicable and arguably ill-suited for regulating such entities.

5.4 Borderless fintech with bank-like activities

Business model and licensing

Case Study 4 concerns a listed fintech firm headquartered outside the EU that has grown into a global provider of cross-border financial services. Its core offerings include international money transfers, multi-currency accounts, debit cards, interest-bearing balances and asset custody, serving individuals and SMEs. According to its annual financial report, the company processes a very large volume of cross-border transactions across a significant customer base, with customer holdings in the order of tens of billions. The firm operates globally and supports multiple currencies. In the EU, it operates through two distinct regulatory entities: a PI with European Economic Area (EEA) passporting rights, and an investment firm authorised to receive and transmit orders in relation to financial instruments, execute orders on behalf of clients, carry out safekeeping and administration of financial instruments and conduct foreign exchange services linked to investment services.

Systemic footprint

The firm's systemic importance is growing: it holds a very large number of licences worldwide and a substantial share of the cross-border retail payments market, managing billions in customer funds. The firm's expansion into QR-based payments, business invoicing and investment products has further broadened its global footprint. Through its infrastructure, the firm enables other institutions, including major banks, to offer cross-border services. It integrates AI into compliance, risk management and fraud management, and makes these capabilities available to partners via APIs. As licensed financial institutions, the firm's EU entities are required to comply with DORA; however, the firm itself has not been designated as a critical service provider.

Potential regulatory gaps and risks

As the EU-based investment firm does not engage in proprietary trading, underwriting of financial instruments or placing on a firm commitment basis, it does not meet the criteria for classification as a CRD investment firm[86] and remains outside consolidated prudential supervision. The firm's global business model remains primarily focused on payment services: in financial year 2025, the company generated roughly two-thirds of its revenue from cross-border payments, around one-fifth from card-related services and the remainder from other activities, such as business accounts and investment products.

Although the firm is headquartered outside the EU, existing cooperation agreements and relatively aligned legal frameworks could facilitate supervisory engagement.

Potential supervisory response

Case Study 4 is another example of the need for a policy discussion on the introduction into payment services legislation of more robust, risk-based capital

[86] See Article 4(1)(1)(b) of the CRR.

requirements for large-scale providers. Where firms combine multiple regulated activities, such as payments, investment services, crypto-asset services and non-bank lending, it may be necessary to revisit the scope of the activities and thresholds that trigger the application of some of the CRD's requirements or the need for a bank licence. For large groups headquartered outside the EU, structured cooperation with non-EU authorities, through data-sharing arrangements, joint supervisory colleges or mutual recognition frameworks, is essential to ensure effective and coordinated oversight of firms operating extensively within the EU.

In the context of DORA, it is still too early to determine whether the operational dependencies created by the firm's platform have been adequately addressed. Nonetheless, the case demonstrates that even firms operating within the regulatory perimeter can pose systemic risks if their business model, scale and infrastructure roles are not adequately captured by existing frameworks. It underscores the need to adapt supervisory approaches to the realities of digital finance, cross-border activity and technological interdependence.

Another example of a large group accumulating multiple non-bank licences within the EU is an undertaking that holds an EMI licence, an investment firm licence and several crypto-asset service provider (CASP) authorisations. Under MiCAR, investment firms may provide crypto-asset services upon notifying the competent authority.[87] Thus, the question of why firms need or choose to accumulate such licences, and particularly whether this practice aligns with the objectives of a fully integrated EU financial market, the simplification of the regulatory framework and the appropriate supervision of group-wide risks, may warrant further analysis.

5.5 From fintech to banking and crypto-assets

Business model and licensing

Case Study 5 examines a European fintech group, founded years ago, that has evolved from an EMI into a global provider of financial services for retail and SME customers. Its core offerings include banking services spanning deposits and lending, investment and crypto-asset services and mobile phone/data services.

The group is headed by a holding company outside the EU, with no financial sector licences, that oversees numerous subsidiaries active in the EU and worldwide, including fintech firms abroad providing key technological services to financial sector sister companies in the EU. In its home country, it mainly operates via the original EMI authorisation – despite recently obtaining a fully-fledged bank licence.

In the EU, the group operates through (i) a mixed financial holding company (MFHC) which controls a bank, an insurance intermediary and an investment firm, as well as two legal entities established in a non-EU country, through which it offers some banking, payment and investment services; and (ii) a CASP established in another EU Member State that is directly controlled by the non-EU parent. Its EU clients

[87] See Articles 59 and 60 of the MiCAR.

access all group services via the bank's web/app platform, evidencing a high level of business and ICT integration among the sister companies. The group's EU financial institutions are required to comply with DORA.

Systemic footprint

Worldwide, the group serves several tens of millions of clients, handling over a trillion transactions in 2024. Its primary markets remain its home country and the EU, where it maintains double-digit penetration. In various EU Member States, the EU bank's branches serve tens of millions of customers and hold several tens of billions of retail deposits, based on the most recent public information.

Potential regulatory gaps and risks

The EU MFHC controls three financial sector subsidiaries, while crypto-asset services are provided by a CASP directly controlled by the non-EU parent. This set-up is possible because the requirement for an EU intermediate parent undertaking (IPU) applies solely to banks and investment firms. CASPs are not in the scope of Article 21b CRD. However, the integration of the CASP's activities with those of the bank could happen, giving rise to operational dependencies, as well as financial interconnections that, without the group requirement, cannot be properly identified and addressed by any supervisors. While CASPs are subject to non-risk-sensitive capital requirements[88], they may engage in activities that give rise to material (financial) risks, including leverage and asset/maturity transformation. Some activities in which a CASP may engage – crypto lending, borrowing and staking – are not governed by any piece of EU legislation. Under current regulations, a foreign group could ask the EU subsidiary bank to extend credit lines to the EU subsidiary CASP, which the latter could use to purchase crypto-assets other than electronic money tokens (EMTs) and asset-referenced tokens. The bank would risk weight its exposure to the CASP – under a standardised approach – by a factor of 20% to 150%, depending on the specific circumstances. However, if the CASP were within the MFHC, at consolidated level the crypto-asset exposure would instead be risk weighted by a factor of 1,250% and would be required to comply with the 1% exposure limit (see Article 501d.2(c) 3. CRR). There is a clear reduction in capital demand when the CASP remains outside the MFHC.

Based on media reports, the group intends to issue a "stablecoin" in other jurisdictions and potentially the EU. To the extent that such a token qualifies as an EMT, it could be issued either by the EU bank or by an EMI. In the latter case, if the non-EU ultimate parent company were to directly control the EMI (as it is currently the case for the CASP), neither EU nor Member States' supervisors would have a full view of group's operations in the European Union. The set-up also has implications from an AML/CFT stand-point. Because the CASP and the entities under the EU MFHC would not form part of the same EU group, they would not be

[88] Article 67 of MiCAR establishes that CASPs are subject to an own funds requirement equal to an amount of at least the higher of the following:

(a) the amount of permanent minimum capital requirements indicated in Annex IV, depending on the type of crypto-asset services provided (from €50,000 to €150,000);

(b) one-quarter of the fixed overheads of the preceding year.

required to have common AML/CFT policies and procedures, conduct a holistic business-wide risk assessment or be subject to consolidated supervision (including once the Anti-Money Laundering Authority (AMLA) assumes its direct supervisory responsibility). Furthermore, if both the CASP and the EMI operate as stand-alone entities in the EU, they will be less likely to meet the criteria for AMLA direct supervision. Given the greater frequency of AML compliance lapses by crypto-asset firms, the regulatory/supervisory gap has a concrete meaning.

Potential response

Case Study 5 offers the opportunity to reflect on the extension to CASPs and EMIs of the scope of application of the IPU requirement. EMI supervision is conducted at Member State level, while EU-level supervision applies only to the issuance of significant amounts of stablecoin and is limited to this business only, with the rest of the EMI's activities under the exclusive purview of national authorities. CASP supervision is solely a national competence, and MiCAR does not provide for any college of supervisors: thus, the coordination of bank/investment firm supervision and CASP supervision is not facilitated. The extension to CASPs of the IPU requirement would be beneficial from both a prudential and an AML/CFT supervision stand-point.

For large groups headquartered outside the EU, structured cooperation with non-EU authorities through data-sharing arrangements, joint supervisory colleges or mutual recognition frameworks is essential to ensure effective and coordinated oversight of firms operating extensively within the EU. The mechanism of the college of banking supervisors applies only once the group obtains a full banking licence in its home country. Nevertheless, some home authorities may engage in voluntary cooperation with the EU host authority while the parent entity holds a non-bank licence.

6 Policy options and supervisory approaches

This chapter outlines supervisory and regulatory approaches that could be used to address regulatory perimeter challenges.

6.1 Risk assessments and monitoring

To keep pace with the evolution of financial services, the FSB (2024) recommends, in the context of payments, that the CAs conduct risk assessments tailored to the specific characteristics of the relevant sector, including business models, operational resilience, services and products offered, target markets and third-party dependencies. Such assessments should consider the full flow of the process, covering instruments, transaction types, delivery channels, platforms, technologies, partnerships and intermediaries. The FSB also recommends continuous engagement with market participants, to ensure that the CAs stay abreast of developments and emerging risks and, where appropriate, adaptations to existing regimes. For its part, the IMF (Bains and Wu, 2023) highlights the importance of leveraging existing supervisory structures, where technology is mature or available resources are limited, and using innovation hubs, regulatory sandboxes and tech sprints to enhance supervisory awareness and responsiveness, where innovation is still at an embryonic stage or is poorly understood.

6.2 General regulatory approaches

Regulatory approaches entail trade-offs in managing risks and innovation, with the literature outlining various, non-mutually exclusive strategies for addressing regulatory perimeter challenges:

Laissez-faire: a wait-and-see approach for services that are not yet widespread and do not pose significant economic or systemic risks. Authorities monitor developments and may collaborate to pre-emptively address risks by issuing guidelines and warnings.[89] While it is suitable for early-stage developments, Borgogno & Manganelli (2021) argue that this approach may obscure risks, potentially leading to instability, market concentration and disruptive competition.[90]

Activity-based regulation: this approach is premised on the imposition of directly applicable regulatory requirements for specific activities, irrespective of the type of entity performing the activity and with no regard for any other activities in which that

[89] E.g. the EBA's January 2014 warning on crypto-assets ("virtual currencies"): https://www.eba.europa.eu/publications-and-media/press-releases/eba-warns-consumers-virtual-currencies.

[90] See p. 111.

entity may be engaged. Compliance is monitored and enforced – by means of appropriate tools, including sanctions – by supervisory authorities (FSB, 2024). This may not capture spillovers across, or interlinkages between, different financial and non-financial activities within a group.

Entity-based regulation: this approach aims to regulate activities at the level of the entities performing them. It may include governance, prudential and conduct requirements that are enforced through supervisory activities (FSB, 2024). Since an entity's resilience hinges on the mix of its activities, entity-based regulation may impose constraints on the combination of activities (Borio et al., 2022).

Hybrid approach: this combines elements of both activity- and entity-based regulation, depending on the nature of each jurisdiction's regulatory structure.

Principles-based approach: regulators aim to set broad, outcome-focused principles, rather than imposing detailed rules to keep pace with technological and market developments (Amstad, 2019; Black et al., 2007). Its flexibility and potential technology-neutrality may support innovation, but inconsistent application and regulatory gaps may give rise to level playing field concerns.

Regulatory experimentalism: this involves the use of innovation facilitators, such as innovation hubs, sandboxes and special licences, which enable regulators to assess new financial products or services at an early stage (Borgogno & Manganelli, 2021)[91], monitor developments and issue targeted guidance or intervene where necessary. It requires dedicated expertise, resources and, potentially, cross-sectoral cooperation. Key challenges include scalability, consistency, regulatory arbitrage and heterogenous legal standards for similar activities (Enriques & Ringe; 2020).[92]

6.3 Approaches for groups

Ehrentraud et al. (2022) identify three approaches that could be of particular relevance for neo-conglomerates: segregation, inclusion and bespoke frameworks.

The **segregation approach** assumes that key public policy objectives can be best achieved by mandating (for non-banks) a specific group structure for multi-activity companies offering financial services. It requires financial services to be legally separated from non-financial activities and consolidated under a financial holding company (FHC), which would be responsible for meeting prudential and other regulatory requirements on a consolidated basis for the resulting financial sub-group.

The **inclusion approach** adopts a "group-wide" perspective that encompasses both the parent company and all of its regulated and unregulated entities. It emphasises understanding and managing the risks of interdependencies inherent in the business models. As in the segregation approach, financial activities may be grouped into an FHC, subject to consolidated regulatory requirements at the sub-group level.

---

91 Compare pp. 112-122.

92 Compare fintech charters, p. 21.

However, interactions between financial and non-financial activities would be managed by group-wide requirements, rather than by isolating the financial sub-group. The aim is to adjust regulation to fit existing business models more comprehensively.

The **bespoke or holistic approach** assumes that unique risks, scale and ecosystem interdependencies, for example in the context of Big Tech, require a tailored regulatory framework. This should address not only individual entities and activities, but also their combined impact within digital ecosystems. Building on activity-based and entity-based rules, it proposes enhanced disclosure, systemic risk monitoring and potentially new institutional arrangements to ensure effective oversight.

6.4 Perimeter adjustment practices

Anticipating innovation and emerging risks

Scenario analysis is a tool for identifying emerging risks and informing mitigation strategies that is already applied in the context of stress testing exercises[93] and climate risk[94]. It typically explores plausible future states and helps to anticipate and adapt to structural shifts, as well as identifying transition pathways and critical dependencies.

Adaptive regulatory authority entails authorities having a mandate, processes and technical expertise that allow them to rapidly update regulatory categories and frameworks, enabling timely responses to emerging business models and technologies that may amplify existing risks or introduce new ones.

Enhanced dialogue with market participants such as innovation hubs, accelerators and regulatory sandboxes may offer authorities valuable insights into new developments and emerging risks and reduce the likelihood of market participants misinterpreting applicable laws, rules and regulations.

Capturing complex ecosystems

Mapping the full life cycle of financial services, **identifying all critical entities** (including third-party providers) and **assessing interdependencies** that could pose systemic risks (DNB, 2018; Bank of England, 2019), can help us understand the complexity of disintermediated financial ecosystems. As disruption to one entity can affect the entire ecosystem, the activities of agents and brokers should also be part of the mapping exercise. However, where entities operate outside the regulatory perimeter, legal and operational constraints may hinder data collections and risk assessments. While regulated institutions are often required to manage third-party

93 See EBA 2023 EU-wide Stress Test Results and ECB Macroprudential Stress Testing Framework.

94 Task Force on Climate-related Financial Disclosures (TCFD) (2020), Guidance on Scenario Analysis for Non-Financial Companies.

risks (FSB, 2019d), indirect supervision may be insufficient when unregulated providers play a critical role.[95]

The blurring of sectoral boundaries gives rise to complex questions as to when firms should be subject to **direct supervision** and which authority is best placed to oversee them. This requires a nuanced understanding of the individual firm's role within the ecosystem, the risks it introduces and the potential for cross-sectoral spillovers (Zetzsche et al., 2019). The EU's PSD2 (2015) extended the perimeter to previously unregulated services, such as payment initiation services (PIS) and AIS, enhancing consumer protection, operational resilience and market integrity. A similar approach may now be warranted for super apps and complex multi-partner financial platforms. In the crypto-assets space, financial intermediation, including crypto-asset issuance, staking, borrowing and lending, custody, trading and settlement, should fall within the regulatory perimeter.

Adapting to multi-activity models may include evaluating whether existing prudential safeguards are sufficiently resilient and adaptable to address risks arising from re-bundled activities, complex group structures and increasingly disintermediated, interdependent and blockchain-based business models. Neo-conglomerates may simultaneously deliver financial services to end-users and critical technology or infrastructure to regulated institutions, creating concentration risks and operational dependencies. Prudential frameworks should evolve to reflect the complex interdependencies of multi-activity financial firms, encompassing both commercial-financial linkages and cross-sectoral exposures.

Re-evaluating reporting and perimeter monitoring tools to capture new developments and activities may require revisiting quantitative and qualitative criteria for assessing systemic importance. In the context of digital platforms, metrics from market power assessments (e.g. revenue shares, user shares, mark-ups, Lerner index, profits, comparative advantage and evaluation of network effects) may offer useful insights (Frank & Peitz, 2023).

Assessing financial system impact and transmission risks

Evolving business models and interdependencies also require a reassessment of the resilience of traditional institutions and the broader system. Supervisory responses should reflect these shifts, and consider the implications of different business models for capital adequacy, governance structures and risk management frameworks. They should pay attention to customer onboarding procedures, ongoing monitoring practices, business continuity planning and the management of interdependencies, especially where services are outsourced or integrated via digital platforms. Addressing the financial linkages between traditional institutions and crypto markets includes mitigating contagion risks and applying appropriate capital and liquidity requirements to crypto-asset exposures.

In the area of crypto, regulatory arbitrage remains a concern, as large, unregulated groups may acquire lightly supervised entities (e.g. EMIs, CASPs) to create a façade

[95] This concern was one of the drivers behind the EU's adoption of DORA, which includes, among its objectives, enhanced oversight of ICT third-party risk.

of compliance while conducting substantial activities through unregulated affiliates, thereby obscuring risk and undermining the integrity of the regulatory framework.

In the DeFi space, particular attention may need to be paid to lending and borrowing protocols, which are prone to cyber threats, fraud and excessive leverage. Monitoring rehypothecation and leverage build-ups critical in preventing systemic spillovers (ESRB, 2023; EBA/ESMA, 2025).

Addressing these challenges is essential, in order to mitigate systemic risk and ensure a level playing field, applying comparable regulation to similar risks regardless of technology or structure.

Supervisory tools and powers

Precautionary measures, such as limiting market growth or delaying authorisation until risks are better understood, must be carefully balanced against competition concerns and consistency with legal frameworks.

Intervention powers enable competent regulatory bodies to prohibit or restrict financial products, services or practices that pose significant risks to investors, market integrity or financial stability. These are particularly important for addressing activities that lie outside the current regulatory perimeter but are closely linked to regulated services and may erode trust in the financial system. Their effective use requires strong institutional cooperation across regulatory and enforcement bodies, allowing authorities to respond swiftly and proportionately.

Enhancing national and international collaboration

Coordination among the various financial and non-financial authorities (e.g. those responsible for cyber risk, telecoms, competition and consumer and data protection) is essential in monitoring and addressing regulatory perimeter risks. This supports core regulatory objectives, such as ensuring the solvency of financial institutions, the soundness of payment systems and financial stability, while also balancing competition, consumer and investor protection and data protection goals. In the context of payments, the FSB (2024) recommends[96] establishing inter-agency task forces, and for actors operating across borders, groups similar to cooperative arrangements (CMPI/IOSCO, 2012)[97] or supervisory colleges (BCBS, 2014). In the context of crypto, the FSB (2023b)[98] recommends both domestic and international cooperation and coordination to support the authorities in fulfilling their mandates, while promoting regulatory and supervisory consistency.

---

96 See Recommendation 6.

97 See Responsibility E: Cooperation with other authorities, p. 133.

98 See Recommendation 3.

7 EU-specific considerations

The European Union has been a pioneer in developing comprehensive and forward-looking financial regulation, as illustrated by its initiatives in the areas of digital operational resilience (with DORA), crypto-asset regulation (with MiCAR), consumer and data protection in the context of retail payments (under PSD2), the CCD2, crowdfunding (with the ECSPR[99]), the Directive on access to basic payment accounts[100], data protection (with the GDPR[101]) and AI (with the AI Act). Such initiatives have not only harmonised rules across Member States, fostering supervisory convergence and deepening the financial integration, but have also positioned the EU as a global standard-setter. The EU has traditionally combined activity-based and entity-based regulatory approaches. For example, the CRR/CRD and MiFID2 impose requirements based on the type of institution at stake (a bank, an investment services firm or another type of regulated financial institution), while PSD2 includes both service-specific (hence, activity-based) rules and institution-specific prudential requirements (depending on the type of payment service provider at stake), making of it a hybrid framework.

As per the case studies, neo-conglomerates are increasingly challenging the boundaries of the EU's regulatory framework. Far from being isolated cases, the case studies exemplify a broader trend: large firms are replicating the economic and functional characteristics of regulated financial institutions while continuing to be supervised as niche service providers. Despite their scale and systemic importance, they are not subject to group-wide supervision, prudential consolidation or comprehensive risk assessments where there is no bank in the group. In many instances, even accounting consolidation fails to provide a complete view of their financial and operational exposures.

A similar pattern can be observed among the Big Tech firms, which currently operate within the EU under lighter regulatory regimes and exemptions. These firms are refining their strategies in emerging markets, particularly in Asia, South America and Africa, where regulatory environments tend to be more permissive and growth opportunities more pronounced. In the United States, they benefit from higher margins, although often at the expense of consumer protection. Collot et al. (2025) warn that Big Tech firms could rapidly scale, offer a broad suite of financial services and attain systemic importance without adequate oversight. The authors concur and

99 Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (OJ L 347, 20.10.2020, p. 1).

100 Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (OJ L 257, 28.8.2014, p. 214).

101 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

build on their analysis by proposing, below, concrete measures to close these gaps, extending the discussion to neo-conglomerates.

At the time of writing, the supervisory tools for addressing the risks posed by neo-conglomerates are limited to moral suasion, ad hoc data collection from licensed partners and the issuance of risk management guidelines to financial institutions. Enforcement is only possible when firms actually engage in regulated activities. Despite their merits, these measures do not allow for comprehensive oversight, with the absence of regulatory authority over unlicensed entities, combined with fragmented data flows, hampering effective risk assessment and mitigation and depriving the CAs of a consolidated view of the financial and non-financial activities of neo-conglomerates, including Big Tech (see ESAs, 2022 and 2024, McCaul, 2024 and Collot et al., 2025). Critical information on risk exposures, governance structures and potential conflicts of interest remains fragmented or is altogether inaccessible. Similar considerations apply to MCIs (see Garcia Ocampo et al., 2026). In principle, voluntary cooperation among supervisors could help illuminate some of the resulting blind spots, but practical barriers persist. Legal limitations, differing institutional mandates and jurisdictional frictions frequently impede the development of a coherent, cross-border supervisory approach.

The remainder of this chapter outlines concrete proposals to close these gaps, by enhancing supervisory coordination, improving data collection and sharing, harmonising definitions and licensing requirements and establishing a forward-looking framework for group-wide oversight. These considerations aim to ensure that the EU's regulatory architecture remains fit for purpose in a digital, cross-sectoral and increasingly platform-driven financial ecosystem, while also advancing the EU's broader objectives of innovation, competitiveness and financial inclusion.

7.1 Enhanced collaboration on regulatory perimeter monitoring and risk assessments

The ESAs have adopted collaborative approaches to enhance the oversight of emerging financial activities within the EU. These include cross-disciplinary exchanges and joint analyses aimed at fostering supervisory convergence and strengthening their collective capacity to identify and respond to new risks, including within the setting of the EFIF. The ESAs will occasionally coordinate their responses to European Commission calls for advice: examples include the joint EBA/ESMA review of the prudential framework for investment firms, which assessed the adequacy of the current requirements, methodology and unaddressed risks, and the ESAs' cross-sectoral mapping of Big Tech financial services activities and of their relevance to the financial sector (ESA, 2024), which examined the type and scale[102] of direct and indirect provision of financial services activities of such firms in the EU, their role as major technology providers[103] and their gatekeeping functions under the

[102] E.g. cross-border activity, number of subsidiaries active in providing the relevant financial services and other functions in the financial sector.

[103] For example, if designated as "critical third-party providers" under DORA.

Digital Markets Act. The ECB and, where applicable, the ESRB, also contribute to these risk assessments and monitoring efforts.

The EU could follow the example of the UK Financial Conduct Authority (FCA), which has developed proactive and structured regulatory perimeter monitoring, supported by advanced market intelligence and a regularly updated Regulatory Perimeter Report. The FCA systematically collaborates with key institutional partners – including HM Treasury, the Bank of England, the Prudential Regulation Authority and other regulatory, consumer protection and law enforcement bodies – to facilitate coordinated oversight and effective responses. Additionally, the FCA has launched the Global Financial Innovations (GFIN) network, to promote effective regulatory responses to the use of emerging and more traditional technologies in financial services, by sharing experiences, working jointly and facilitating responsible cross-border experimentation with new ideas. On the EU side, only the national authorities of Lithuania, Hungary, Malta, Luxembourg and Poland are participating. The Monetary Authority of Singapore (MAS) has also established strong cross-authority cooperation, launching the Global Finance & Technology Network (GFTN). Through the GFTN, the MAS aims to position Singapore as a global fintech hub by fostering dialogue between policymakers and industry, and by scaling innovation through strategic global partnerships in areas such as payments, asset tokenisation and AI.

To strengthen regulatory perimeter monitoring and align with international best practices, the EU and national authorities may want to consider further enhancing their cooperation. Efforts in that direction could be complemented by cooperation between prudential, oversight and conduct authorities, in order to reduce the risks of regulatory fragmentation and arbitrage, particularly from a micro-prudential perspective. In parallel, EU and national authorities may want to deepen their engagement with global standard setters and international organisations, fostering mutual learning and contributing to the development of globally coherent supervisory frameworks.

From a macroprudential stand-point, regular and structured collaboration with a broader set of stakeholders, including telecommunications regulators, data and consumer protection authorities, cybersecurity experts and competition bodies, is essential. Such multi-disciplinary engagement (e.g. via EFIF) is critical in capturing systemic risks arising from the convergence of financial services with digital infrastructure and platform-based business models.

Greater cross-activity collaboration is also advisable in the design and deployment of innovation facilitators, such as regulatory sandboxes, tech sprints and hackathons[104]. Rather than relying on fragmented, country-specific initiatives, the EU should promote the use of EU-own sandboxes capable of addressing cross-border and cross-sectoral activities. Inspiration could be drawn from the UK FCA's Early and High Growth Oversight initiative (FCA, 2024b), which complements its regulatory sandbox by proactive and enhanced supervision for up to 300 newly authorised or fast-growing firms. This helps the FCA to spot harm and misconduct early, ensuring

[104] For examples of hackathons, see European Central Bank / ESCB-SSM Hackathons / 2023 Climate Change Challenge - Beat the heat · GitLab.

that firms meet regulatory requirements, and to support firms in building robust systems and controls as they grow, while at the same time fostering responsible innovation and promoting competition. The FCA's Innovation Pathways initiative assists firms to launch innovative consumer products and services via automated advice and guidance platforms, explaining FCA rules in a clear and engaging way.

More broadly, authorities in the EU may want to establish robust metrics and feedback mechanisms to evaluate supervisory responses to financial innovation, and invest in more resources and capacity building to keep pace with the increasingly complex and dynamic financial ecosystems (something in which the EU Supervisory Digital Finance Academy could play a role).

7.2 Reviewing EU-wide reporting

Enhanced supervisory cooperation aside, effective regulatory perimeter monitoring also requires a forward-looking and harmonised reporting framework. Without consistent, granular and shareable data, even the most well-coordinated supervisory efforts could prove inadequate. Strengthening the EU's reporting architecture is, therefore, essential to support timely risk identification, ensure proportional supervision and enable coordinated responses across jurisdictions and sectors.

Basic indicators for all, enhanced reporting for systemically important entities

A more holistic framework should include a core set of basic indicators for all financial institutions, including a dedicated subset for entities benefiting from regulatory exemptions[82], to better capture developments (including potential changes in business models) and assess whether such exemptions remain proportionate. Enhancing supervisory information on ancillary services is another priority. In addition, stock-listed companies providing financial services in the EU could be required to disclose a separate breakdown of their direct and indirect (e.g. white labelling) involvement in financial services activities in their annual reports. This would improve transparency on the interplay between financial and non-financial activities, support supervisory risk assessments and help to identify their overall financial market relevance and their interdependencies, both within the group and with other financial market actors.

The EFIF matrix provides a useful starting point for basic indicators in the context of neo-conglomerates. However, it should continue to be refined, standardised and operationalised as part of a regular EU-wide data collection exercise, to ensure consistency, comparability, supervisory relevance and actual data-sharing.

Enhanced reporting requirements should ideally apply, on both a solo and consolidated basis, to firms or groups deemed systemically important[33]. Such requirements could include enhanced data on risk exposures, safeguarding arrangements, group-wide interdependencies and business model characteristics, with a clear distinction between regulated and unregulated activities. More granular and frequent reporting would allow deeper insights into counterparty and

concentration risks, while also ensuring that data are only submitted once, but reused for multiple supervisory and analytical purposes.

Market monitoring, data-sharing and consolidation

Effective supervision requires timely access to granular data on corporate structures, intergroup financial flows and market presence. Enhancing transparency requires the consistent identification of entities through the use of a common legal identifier for groups, such as the extant Legal Entity Identifier[105] (LEI), for both authorisation and reporting obligations. This would allow for improved mapping of group structures and interconnections, while also improving data traceability. Today's inconsistent use of identifiers – such as the concurrent use of alternatives to the LEI in the EBA's registers for payment institutions and EMIs – may undermine consistency and complicate the task of tracking group-wide activities. A similar issue arises in the ESAs' register of ICT third-party service providers under DORA, where the lack of a uniform identifier complicates the mapping of interdependencies and hampers the effective oversight of systemic risks.

Continued reliance on aggregated, anonymised, country-level reporting may also prove inadequate. The supervisory reporting architecture should ideally address data loss resulting from aggregation, which often removes firm-specific information when national authorities report to EU institutions – as seen in the reporting of fraud statistics under PSD2, where firm-level data are not retained.

There is also a growing need for near real-time market intelligence and market monitoring to ensure that supervisors are not caught off guard by new business models or cross-border expansions, and can respond to them in a timely and coordinated manner. In an era of AI-enabled tools, unstructured data and language barriers should no longer be considered valid constraints.

Finally, notification regimes should be expanded to cover material changes in ownership or control of critical infrastructure and data intermediaries. Supervisors should be granted timely access to structural and financial linkages within financial groups.[106] Ideally, notification templates should be harmonised, and information from various registers should be integrated to support supervisory coordination, avoid duplications of reporting requirements and reduce fragmentation.

Closing lending and crypto exposure data gaps

Data gaps related to lending, particularly in areas such as BNPL arrangements and retail lending conducted under national regulatory frameworks, should, in the authors' view, be addressed through systematic reporting obligations. Where

---

[105] The LEI is a 20-digit alphanumeric code based on the ISO 17442 standard that uniquely identifies legally distinct entities. It was developed to uniquely identify counterparties to financial transactions across borders, thereby improving and standardising financial data for a variety of purposes – for instance, to support a more accurate and timely aggregation of data on the same entity from different sources, especially on a cross-border basis – see FSB (2012), A Global Legal Entity Identifier for Financial Markets, June.

[106] Current notification thresholds under EU financial services legislation often do not capture changes of control involving APIs, data hubs or non-supervised entities. This is particularly relevant when such entities acquire financial firms, creating gaps in supervisory oversight and potentially allowing systemic risks to accumulate undetected.

national credit registers exist, coverage should be extended to non-bank lenders to enable a more comprehensive view of credit exposures across the financial system. The proposed reporting should also encompass crypto lending, borrowing and staking activities, which currently fall outside the scope of EU legislation. Moreover, as outlined by Aerts et al. (2025) and the ESRB (2025), data on exposures to crypto-assets of entities other than banks are absent or fragmented. This includes spot holdings of crypto-assets, leverage and interlinkages with the broader financial system, creating blind spots that mask potential contagion channels. Closing these gaps would be critical to ensure that all entities capable of posing systemic risks fall under supervisory scrutiny.

Cultural and structural shift towards collaborative oversight

Transforming the reporting architecture is essential, but without institutional cooperation, even the most advanced data framework will fall short of realising its full potential. Effective supervision demands not only technical upgrades, but also a cultural shift towards collaborative oversight.

Beyond prudential supervision, some neo-conglomerates are already subject to Eurosystem oversight under the ECB's PISA framework. PISA emphasises collaboration, with the Eurosystem lead overseer seeking to cooperate, as far as possible, with all relevant regulatory bodies with a legitimate interest. The PISA framework offers the possibility of fostering active contribution, coordination and the integration of findings from other authorities, and reduces the burden for both overseen entities and regulators.

Building a forward-looking, data-driven collaborative supervisory model calls for stronger institutional cooperation and the dismantling of barriers to information-sharing. Its prospects of success will depend heavily on a genuine commitment to collaboration, in which insights from other authorities are valued and risks are addressed jointly, rather than in isolation. Without a shift towards collaborative oversight, the regulatory perimeter will remain porous, and systemic vulnerabilities will continue to multiply unchecked.

7.3 Enhancing the EU regulatory framework

Intervention powers

The Markets in Financial Instruments Regulation (MiFIR)[107] gives ESMA the power to temporarily prohibit or restrict the marketing, distribution or sale of certain financial instruments in well-defined circumstances and the pursuit of certain types of financial activity within the European Union.[108] These powers can be exercised when there is a significant investor protection concern or threat to the orderly functioning and

[107] See Article 40 of Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

[108] Article 41 of the MiFIR also introduces similar powers for the European Banking Authority (EBA) in the case of structured deposits.

integrity of financial or commodity markets, or a risk to the stability of the financial system, particularly when these risks/threats are not adequately addressed by existing legislation. Such powers of intervention have also been established in MiCAR. In the authors' view, similar powers would merit being embedded, more systematically, across EU financial services regulations to ensure that supervisory authorities have the necessary tools to act swiftly and proportionately in the face of emerging, including cross-sectoral, risks/threats.

Publication of core findings from enforcement actions

To enhance transparency, accountability and supervisory convergence, the authors submit that EU authorities should be required to publish sanitised summaries of enforcement actions, similar to the practice followed in the United States. These summaries could include anonymised findings on key shortcomings – such as weaknesses in internal controls, third-party and fintech partnership oversight, credit underwriting and IT security – and outline the corrective measures imposed. These could involve requirements to strengthen governance, enhance risk management frameworks, improve consumer protection practices or address capital and liquidity planning. While detailed findings should be shared confidentially among the relevant supervisory authorities, public disclosure of key lessons learned would support market discipline, inform peer institutions and foster a compliance culture across the financial sector.

This principle should also apply to the assessments of supervisory authorities. For instance, the ESMA (2025) fast-track peer review on CASP authorisation and supervision in Malta demonstrates how publishing findings, even when directed at supervisory authorities, can promote convergence, transparency and mutual learning. Making such reviews a regular and public feature of the ESA's activities would help to strengthen trust in supervisory consistency across the EU.

Harmonising white labelling across sectors and borders, direct licensing for multi-partner arrangements.

As outlined in the EBA report on white labelling, a revision of the EBA Guidelines on Outsourcing could provide greater consistency on the regulatory qualification of white labelling arrangements. However, a regulatory change may be required to ensure that all entities engaging in agent or broker-type activities become subject to a minimum registration and disclosure regime, regardless of whether they hold a financial licence: this would further enhance consistency and transparency, particularly in cross-border contexts, and ensure that consumers are adequately informed of the parties responsible for service delivery and complaints handling.

While supervisors may already have enforcement tools at their disposal under existing EU law (including PSD2, MiFID2 and the Unfair Commercial Practices Directive), to address misleading advertising and unclear accountability, these tools are often applied indirectly, through licensed entities. In complex, cross-border or multi-partner arrangements, enforcement can become fragmented or delayed, particularly when the unlicensed partner controls the customer interface. Therefore, clearer and harmonised rules may be needed to ensure that disclosure and

marketing practices accurately reflect the nature of the financial service and the identity of the responsible entity. Consistent with the EBA white label report, enhanced supervisory coordination and guidance would help ensure consistent application of these rules and more effective oversight of consumer-facing risks.

Given the supervisory fragmentation and lack of visibility highlighted by the EBA, it is could be considered to grant CAs explicit powers to conduct on-site inspections of agents and to share information on major infringements – such as those related to fraud or IT security – with other CAs, the EBA and the AMLA. Enhanced cross-border cooperation is essential to ensure effective oversight of increasingly integrated and digitalised distribution models.

When white label partners engage with multiple licensed providers, it may be appropriate to bring such entities within the scope of direct licensing, particularly when they exert significant control over customer relationships or perform regulated functions. In these cases, the complexity of the business models may exceed the oversight capacity of the white label service provider. Furthermore, the nature and potential impact of such white label activities exceed the risks of comparable regulated services, such as payment initiation or AIS. Introducing a licensing regime would enhance transparency, accountability, and supervisory effectiveness and ensure a level playing field.

Harmonising definitions and requirements related to bank-like activities

Building on the above analysis of regulatory fragmentation, one key area requiring clarification is the legal and supervisory treatment of bank-like activities conducted by non-bank entities. This issue is closely linked to the absence of harmonised definitions for the activities subject to mutual recognition listed in Annex I of the CRD. It should be recalled that Article 4 1(1) of the CRR, which is directly applicable in national law, defines a bank as “an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account”. Credit balances are excluded if they fulfil the following conditions: (a) their existence can only be proven by a financial instrument; (b) their principal is not repayable at par; or (c) their principal is only repayable at par under a particular guarantee or agreement provided by the bank or a third party. The credit institution definition is aligned with the BCBS principles and has been in use in EU law since the First Banking Directive.[109] However, as stated in several EBA reports and

[109] First Council Directive 77/780/EEC of 12 December 1977 on the coordination of the laws, regulations and administrative provisions relating to the taking up and pursuit of the business of credit institutions (OJ L 322, 17.12.1977, p. 30).

opinions[110], core elements of the definition – including the concepts of "deposits"[111], "other repayable funds" and "from the public" – remain subject to different national interpretations, as also reflected in differing national supervisory practices. While other examples of EU law include definitions of some of the above concepts, direct cross-references to them are absent from the CRR.[112] At the same time, the definition of deposit-taking differs from one piece of EU legislation to another.[113] To improve legal clarity, future definitions could focus on the economic function of an activity, rather than relying solely on the type of underlying licence. As part of a recalibration effort, the regulatory treatment of emerging activities, such as crypto lending, borrowing and staking, could be addressed, for example by expanding the scope of MiFID2 or MiCAR (whose Title V is dedicated to crypto-asset services). Alternatively, as outlined by Annunziata et al. (2025), certain crypto-based services, particularly those involving risk-taking, yield expectations and third-party management, could be classified as investment-like products regulated under MiFID, with their providers subject to the applicable prudential regimes under the IFR/IFD or, where their scale, scope of activities, systemic importance or legal form warrants it, under the CRR/CRD.

Any ambiguity regarding the prohibition on EMIs and payment institutions passing on interest earned on customers' funds should also be removed. While this prohibition is largely applied across the European Union, there is anecdotal evidence that some supervisors allow interest to be passed on to customers, thereby blurring the distinction between e-money and deposits.

EU co-legislators could consider reviewing the perimeter of consolidated prudential and AML/CFT supervision by extending the scope of the IPU requirement under the CRD and corresponding CRR consolidated-supervision provisions to cover all financial institutions.

Harmonising minimum prudential requirements for non-bank lenders

In accordance with Article 9 of the CRD, the taking of deposits requires a bank licence in all Member States. In contrast, the EBA report on non-bank lending (2022) outlined that "where non-bank lenders are not subject to any entity-specific requirements, the only applicable [EU] provisions are the ones foreseen at activity

---

110 E.g. EBA opinion on the elements of the definition of credit institution, 18 September 2020, Report on OFIs and regulatory perimeter issues, 9 November, Opinion of the European Banking Authority on matters relating to other financial intermediaries and regulatory perimeter issues, 9 November 2017 and EBA Report and Opinion on matters relating to the perimeter of credit institutions, 27 November 2014.

111 Article 5a(4)(c) of the CRR introduces a cross-reference to the definition of deposits in Article 2(1)(3) of Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes (OJ L 173, 12.6.2014, p. 149) (the Deposit Guarantee Schemes Directive), including structured deposits, as part of the delineation of "traditional assets" for the purposes of the prudential treatment of crypto-asset exposures. However, that provision need not aim to define deposits for the purposes of the CRR but, rather, include them among a set of traditional asset classes, which, collectively, serve to delineate the scope of crypto-asset exposures.

112 For example, the term "deposit" is defined in Article 2(1)(3) of the Deposit Guarantee Schemes Directive, while the term "funds" is defined in Article 4(25) of PSD2.

113 Compare the definition of "deposit" in the annex to CRD6 with the definition in CRR3, which does not specify that deposits are taken "from the public": this could imply that deposits from other credit institutions are also covered.

level" such as the CCD2 and in the Mortgage Credit Directive (MCD)[114]". While the CCD2 foresees a need for supervision, it does not go into more detail.

Although some Member States apply additional national licensing regimes, there is a clear need for harmonised minimum prudential requirements for non-bank lenders, to ensure that all actors involved in credit origination and distribution are subject to appropriate safeguards (compare Collot et al., 2025). To ensure financial resilience and to prevent regulatory arbitrage between bank and non-bank lenders, the EU legislator may want to consider introducing harmonised own funds and liquidity requirements for all credit providers. These requirements should be calibrated based on the scale, complexity and risk profile of their target institution (in particular, asset and maturity transformation), and comply with the principle of proportionality. Introducing such a harmonised regime would reduce the risk of undercapitalised lenders contributing to credit market instability, particularly in periods of stress. Like the IFR, EU legislation on non-bank lending should establish thresholds that trigger the requirement for a banking licence. In this context, the regulatory response to MCIs engaged in financial intermediation with respect to market, credit and liquidity risks, prudential consolidation and cross-border collaboration should be considered (Garcia Ocampo et al., 2026).

Enhancing risk sensitivity in own funds requirements and prudential requirements for CASPs

To promote a more risk-sensitive approach to own funds requirements under PSD2, the removal of the current 20% cap on additional own funds requirements, as set out in Article 9(3) of PSD2, could be considered. Eliminating this cap would enable a more proportionate calibration of capital requirements in accordance with the actual risk profiles of payment institutions, thereby strengthening the prudential framework. In parallel, the EBA could develop guidelines specifying potential triggers that might justify the imposition of higher own funds requirements. These triggers could include the provision of licensing as a service, engagement in BNPL arrangements, exposure to chargeback risks, significant intragroup exposures and the undertaking of other activities that could elevate the institution's risk profile. Likewise, risk-sensitive own funds for CASPs could be introduced in MiCAR. This could be done in the context of the proposal on the development of capital market integration and supervision within the European Union[115] (Savings and Investments Union or SIU), which suggests strengthening the supervisory framework for CASPs by transferring authorisation, monitoring and enforcement powers for all CASPs from the NCAs to ESMA. At the same time, gaps in the statutory audit requirement could be closed for CASPs.

Moreover, the interaction between the PSD2 framework and MiCAR should be clarified. This clarification should reflect the considerations outlined in the EBA's no-

---

114 Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ L 60, 28.2.2014, p. 34).

115 European Commission (2025), Proposal for a Directive of the European Parliament and of the Council amending Directives 2009/65/EC, 2011/61/EU and 2014/65/EU as regards the further development of capital market integration and supervision within the Union (COM/2025/942 final).

action letter[116], with a view to ensuring regulatory coherence, avoiding supervisory gaps and mitigating the risk of arbitrage between overlapping regulatory regimes.

A holistic supervisory framework for neo-conglomerates

Chapters 2 to 4 describe how neo-conglomerates have evolved by replicating some of core functions of traditional financial institutions. Below, the authors propose the elements of a forward-looking supervisory framework tailored to their risks, building on the proposals of Ehrentraud et al. (2022), the ESAs (2023)[117] and Collot et al. (2025).

The basic indicators discussed in 6.2. should be applied to identify systemically important entities or neo-conglomerates. Once identified, enhanced reporting for these actors should apply. Thresholds for inclusion in the framework should be subject to dynamic reassessment, particularly for firms with fast-growing footprints or evolving business models. As discussed in 4.4, dual or multi-licensing structures may allow firms to remain below the quantitative thresholds, despite accumulating systemic importance. A dedicated framework for neo-conglomerates could complement efforts to revisit the scope and thresholds that trigger the partial application of the CRR or the requirement to obtain a bank licence. This could include consideration of additional qualitative criteria that reflect the group's consolidated risk profile, beyond the current activity-based triggers under Article 4(1)(1)(b) of the CRR. In addition, the direct placement of these systemic actors under the supervision of the ESAs could be considered (unless a bank licence is required in their case). Given the cross-sectoral nature and potential systemic footprint of such groups, placing them under ESA-led supervision could ensure their more consistent and coordinated oversight.

Large and complex groups should be required to consolidate their financial activities under a dedicated FHC. This would facilitate group-wide supervision, enable prudential consolidation and ensure clear accountability for governance, risk management and compliance. This approach mirrors the IPU requirement introduced under Article 21b of CRD V for third-country banking groups with significant operations in the EU. Alternatively, regulators could require such groups to integrate their financial activities under a single licence, for example by consolidating multiple payment service licences, to reduce regulatory fragmentation and improve oversight.

Box 4

Approaches of other jurisdictions to parent companies

From a global perspective, some jurisdictions require the parent entity of a financial institution to segregate its financial activities into a holding company structure for consolidated supervision, while others impose higher capital adequacy ratios due to unproven business models or higher risk profiles.[118] China requires the non-financial corporate parent of an FHC to be profitable for at least

[116] https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-no-action-letter-interplay-between-payment-services-directive-psd23-and-markets-crypto

[117] Recommendation 7c.

[118] See, for example, Zamil & Lawson (2022) for banks.

two or more years. The US FDIC requires the parent company of an industrial loan company to agree to maintain a certain level of capital and liquidity to support the bank. Additionally, the parent company is required to take steps, such as pledging assets or securing a line of credit, to show that they can financially support the bank if needed.[119]

Both approaches would capture group-wide risks, regardless of their legal form or licensing strategy, while allowing for the separation of commercial activities from financial and other, ancillary activities.

Moreover, large and complex groups should be subject to enhanced prudential and operational requirements, including capital and liquidity buffers calibrated to their risk profile, recovery and resolution planning and robust governance arrangements. With regard to operational resilience, complex white labelling partnerships and embedded service models would need to be considered. Besides the direct licensing of such multi-partner arrangements, the resulting interdependencies and concentration risks should be more effectively captured by a group-wide risk approach. Large and complex groups should be required to inform their (consolidated) supervisor in good time of any major change[120] to the group's business model, financial and ancillary services, structure, operations or strategic direction.

Moreover, the ECB (2026) recommended maintaining, in MiCAR, the category of significant CASPs, and expanding the existing criteria to include objective metrics of significance (e.g. size, cross-border activity, systemic importance, volume of trades for platforms, volume exchanged against funds, consideration of group-wide activities). In the same vein, the ECB recommends a regular review of the criteria for significant CASPs, drawing on experience with their application. To address risks and regulatory arbitrage opportunities arising from complex, unconsolidated group structures and close links, the ECB recommends that significant CASPs establish an IPU in the EU[121] and ensure that they have group-level recovery plans. Significant CASPs should also be expected to (i) apply enhanced internal controls and risk management arrangements, including for the management of conflicts of interest, (ii) adopt sound remuneration policy, (iii) require prior supervisory approval for management appointments and (iv) carry out enhanced disclosure and reporting at both entity and group level. As a second-best option, and conditional to the amendments suggested for Article 138a(2) of MiCAR below, significant CASPs could be required to apply for an investment firm licence. Finally, the ECB also recommends revising Annex VII of MiCAR to ensure comprehensive coverage of the activities of all CASPs, including custody, trading and settlement, and clarifying ESMA's powers to impose fines, periodic penalty payments and suspension of services.

Transfer of firms whose main activity is crypto-asset services to the supervision of ESMA

119 See Zamil & Lawson (2022).

120 Major changes may be driven by market developments, regulatory changes or internal strategic shifts, and may include the introduction of new business lines, entry into new jurisdictions or modifications to governance arrangements. Their unifying feature is that they could materially affect the group's risk profile and its ability to meet supervisory expectations.

121 Comparable to Article 21b of the CRD.

The ECB supports the proposal to transfer to ESMA the (direct) supervision of entities authorised under a licence other than that of a CASP, once the provision of crypto-asset services has become their main activity. However, the definition of the thresholds triggering such transfers could be clarified. First, in order to ensure that the rule also applies to firms combining financial and non-financial activities, the definition of the thresholds could take into account the total financial services activities of such entities in the European Union. Moreover, reliance on a single metric, such as 50% turnover, may not adequately capture business models where the key risk driver is the volume of operations rather than revenues (e.g. custody, trading venue, transfer service). Consideration could also be given to proprietary trading in crypto-assets and derivatives, as well as to borrowing and lending of crypto-assets, activities likely to give rise to material risks not captured by a turnover-based approach. Cooperation agreements between ESMA and other CAs should ensure smooth transition and effective oversight of residual activities. Finally, the ECB recommends clarifying that, for banks, the anti-market abuse monitoring requirements for CASP activities and the related enforcement could also be assigned to ESMA, as these activities are not covered by the SSM Regulation. At the same time, ESMA should inform the competent authority under the CRD before adopting any supervisory measures or initiating any enforcement actions, in view of potential implications for the institution's soundness, and so that actions can be coordinated under their respective mandates.

To support coordinated oversight, the establishment of dedicated supervisory colleges could be considered, to facilitate structured information-sharing, joint risk assessments and coordinated supervisory actions. The proposed colleges could include the ESAs and prudential and conduct authorities. For CASPs, the current SIU proposal suggests centralising supervision of CCPs, CSDs and CASPs.

Where relevant, memoranda of understanding with third-country authorities should be established to support supervisory cooperation; such cooperation could be further underpinned by the development of equivalence assessments and, ideally, by international standards to support cross-border supervision (which may, in the current political environment, only be possible in cooperation with willing jurisdictions). Risks, trends and patterns should be discussed with non-financial regulators, such as data protection and competition bodies.

Such a proportionate and forward-looking framework, buttressed by an early and high growth oversight approach (such as the one pursued in the United Kingdom), could foster responsible innovation, support sustainable scaling and promote fair competition, by ensuring that similar risks receive comparable regulatory treatment, regardless of legal form or licensing strategy. By providing regulatory clarity and consistency, such a framework could support market entry, reduce fragmentation and encourage investment in secure and compliant financial infrastructure. This would help to ensure that supervisory responses not only mitigate systemic risks, but also support the EU's broader objectives of innovation, competitiveness and financial inclusion.

Harmonising responsibilities across national authorities and re-integration of bespoke frameworks in wider regulatory concepts

The current multiplicity of regulations has led to a dispersed assignment of supervisory mandates to CAs across Member States, complicating cooperation and creating inefficiencies. A more integrated supervisory model could better address the risks posed by multi-activity groups. Although legal mandates often separate prudential and conduct supervision, these two areas are closely interlinked in practice: conduct-related deficiencies, such as poor disclosure or unfair practices, can signal broader governance lapses and poor compliance culture.

Simplifying the EU financial regulatory framework could involve reducing the current patchwork of legislative acts and consolidating them into a more coherent structure. Some Member States have explored this approach by attempting to introduce a consolidated financial services act. While achieving a fully unified financial services regime may be ambitious, organising legislation into a limited number of categories, such as payments, lending, investment services and insurance, could help to streamline the complex interplay of existing EU financial legislation. This should be complemented by an overarching regulation to ensure consistent treatment of cross-sector activities.

8 Conclusion

This paper has examined an evolving challenge to the EU regulatory perimeter: the rise of neo-conglomerates. By describing and analysing five case studies, it has illustrated how financial innovation has been reshaping the financial services landscape, and how neo-conglomerates are able to replicate the economic functions of traditional financial institutions while remaining outside the scope of prudential consolidated regulation and supervision. These developments have given rise to concerns about financial stability, market integrity and consumer protection.

Immediate actions (within existing mandates)

The ESAs could immediately deepen their perimeter monitoring by conducting scenario analyses, leveraging innovation hubs and regulatory sandboxes and producing regular publications of their results, including dedicated monitoring of developments in embedded finance, white labelling, non-bank lending, Big Tech and crypto. With regard to white labelling, the EBA plans to take forward actions in 2026 to facilitate supervisory dialogue, including the discussion of individual case studies, with a focus on the regulatory qualification of the arrangements between the provider and partner. This will be supported by a revision of the Outsourcing Guidelines to cover a broader range of third-party dependencies[122]. The EBA also envisages integrating white labelling into the 2026 Union Strategic Supervisory Priorities, and will continue monitoring such arrangements through its annual Risk Assessment Questionnaire. Similarly, the EBA has made known its intention to continue monitoring the importance of Big Tech for the EU financial sector, as providers of financial services, data and technology, and to strengthen cross-border and cross-disciplinary supervisory coordination. In the view of the authors, it is important to enlarge the scope to neo-conglomerates, particularly as their systemic footprint currently seems to exceed Big Tech activities. The review of the guidelines on the sound management of third-party risk could help to harmonise agent/broker classification and should also include guidance on the interpretation of conduct rules (e.g. disclosure, distribution responsibilities, fraud handling). They could promote cross-sectoral cooperation and collaborative oversight and publish sanitised peer reviews to encourage convergence. To close the data gaps, they should ensure that, when reviewing Level 2 and 3 texts, company information can be shared across Member States, the ESAs and the ECB.

The CAs could enhance the collection of data on non-bank lending and white labelling under existing powers. They could apply moral suasion and issue guidance to licensed partners on addressing emerging perimeter risks and simplifying their group structures. Findings could be shared with the ESAs and other authorities to improve the visibility of cross-border activities. They could proactively reach out to other authorities and participate in joint cross-authority cooperative initiatives, such

[122] See EBA (2025), Consultation on draft Guidelines on the sound management of third-party risk.

as GFIN and GFTN. The publication of sanitised supervisory findings on infringements could help to promote convergence.

The ECB could support the ESAs by contributing intelligence from both banking supervision and central bank activities, facilitate the integration of relevant data into EU-level collections and promote the consistent use of the LEI for group-wide mapping.

Adjustments requiring legislative changes

The European Commission could consider legislative amendments to clarify and harmonise definitions of bank-like activities, licensing thresholds and IPU requirements. It could mandate systematic use of the LEI in EU registers and reporting to reduce fragmentation and support a “report once, use many times” approach.

Proportionate and risk-sensitive requirements could be introduced for licensing complex MCIs and multi-partner platforms, to ensure accountability and consumer protection. Consistent with the Eurosystem’s view (ECB, 2026a), the European Commission could consider establishing a framework for neo-conglomerates, to foster comprehensive oversight of the full range of financial and ancillary services provided by these entities. This would entail a consolidated perspective on their activities, combined with capital and liquidity requirements reflecting both solo and group-level risks, to ensure that these entities can continue to operate without posing undue risks to financial stability. The framework could also incorporate enhanced prudential requirements, recovery and resolution planning, dedicated supervisory colleges and a stronger role for the ESAs, including, where appropriate, ESA-led supervision of systemically important non-bank entities. The aim would be to strengthen supervisory powers and obligations to address residual barriers to information, prevention, enforcement and cooperation. Moreover, the European Commission could review the requirements that trigger the need for a bank licence.

Strengthening supervisory cooperation and the role of the ESAs, including enhanced, direct supervision of multi-function crypto-asset intermediaries and multi-issuer schemes by ESMA, could be integrated into the European supervisory framework for capital markets. In particular, this could involve accounting for group-wide risks and enhancing ESMA’s role, while ensuring cooperation where these players engage in other financial or ancillary activities, for example through a dedicated supervisory college and joint supervisory teams. When reviewing the DLT pilot regime, lessons could be drawn from the United Kingdom, Hong Kong and Singapore to foster responsible innovation and growth, while limiting participation to entities whose business models, risk management practices and regulatory frameworks are sufficiently resilient and aligned with the services provided.

The ESAs could develop technical standards and guidelines to operationalise new legislative requirements. They could define criteria and indicators for systemic importance indicators for activities such as payments, crypto-asset service provision and non-bank lending.

The ECB, the European Commission and the ESAs could engage with global standard setters (such as the FSB, BCBS and IOSCO), as well as with third-country regulators, to ensure cooperation and consistency and prevent fragmentation.

By preparing for adjustments and laying the foundations for structural reforms, the EU could preserve financial stability while fostering innovation and competition. This could involve reducing duplication, harmonising definitions and improving information-sharing, in line with the EU's simplification agenda, while maintaining core safeguards. A proportionate, risk-sensitive and forward-looking approach is key to ensuring that the benefits of digital finance do not come at the expense of resilience and trust. Early and high growth oversight can promote responsible innovation, support sustainable scaling and ensure fair competition through consistent regulatory treatment of similar risks. Regulatory clarity and coherence can facilitate market entry, reduce fragmentation and encourage investment in secure and compliant financial infrastructure. Taken together, these reforms would help ensure that supervisory responses not only mitigate systemic risks but also advance the EU's broader objectives of innovation, competitiveness and financial inclusion.

Bibliography

Aerts, S., Born, A., Gati, Z., Kochanska, U., Lambert, C., Reinhold, E. and van der Kraaij, A. (2025), "Just another crypto boom? Mind the blind spots", *Financial Stability Review*, ECB, Frankfurt am Main, May.

Amstad, M. (2019), "Regulating FinTech: Objectives, Principles and Practices", *Working Paper Series*, No 1016, Asian Development Bank Institute, October.

Annunziata, F., Perrone, A., Arrigoni, M., Girardi, I. and Di Gabriele, N. (2025), "Crypto Lending in the European Union. A position paper", *Bocconi Legal Studies Research Paper Series*, SSRN, February.

Babina, T., Buchak, G., De Marco, F., Foulis, A., Gornall, W., Mazzola F. and Yu, T. (2024), "Customer Data Access and Fintech Entry: Early Evidence from Open Banking", *Staff Working Paper*, No 1,059, Bank of England, February.

Barakova, I., Ehrentraud, J. and Leposke, L. (2024), "A two-sided affair: banks and tech firms in banking", *Financial Stability Institute (FSI) Insights on policy implementation*, No. 60, October.

Bank for International Settlements (2018), "Defining and measuring fintech credit", BIS Quarterly Review, September, p. 31.

Bank for International Settlements (2019), *Annual Economic Report*, Chapter 3, June.

Bank of England (2019), *Financial Stability Report*, December.

Basel Committee on Banking Supervision (BCBS) (2014), *Principles for effective supervisory colleges*, June.

Basel Committee on Banking Supervision (BCBS) (2022), *Prudential treatment of cryptoasset exposures*, 16 December.

Basel Committee on Banking Supervision (BCBS) (2024a), *Core Principles for effective banking supervision*, April.

Basel Committee on Banking Supervision (BCBS) (2024b) *Digitalisation of finance*, May.

Ben Naceur, S., Candelon, B., Elekdag, S. and Emrullahu, D. (2023), "Is FinTech Eating the Bank's Lunch?", *IMF Working Papers*, Institute for Capacity Development, November.

Bogaard, H., Doerr, S., Jonker, N., Kiefer, H., Koltukcu, O., Lopez, C., Ornelas, J.R. H., Rambharat, R., Röhrs, S., Teppa, F., van Bruggen, F. and Vansteenberghe, E. (2024), "Literature review on financial technology and competition for banking services", *Working Paper No 43*, June.

Boissay, F., Ehlers, T., Gambacorta, L. and Shin, H.S. (2021), Big techs in finance: on the new nexus between data privacy and competition, *BIS Working Papers*, No 970, October.

Borgogno, O. and Manganelli, A. (2021), "Financial technology and regulation: the competitive impact of open banking", *Market and Competition Law Review*, Vol. 5, No 1, p. 107.

Borio, C., Claessens, S. and Tarashev, N. (2022) "Entity-based vs activity-based regulation: a framework and applications to traditional firms and big techs", *FSI Occasional Papers*, No 19, August.

Born, A., Gschossmann, I., Hodbod, A., Lambert, C. and Pellicani, A. (2022), "Decentralised finance – a new unregulated non-bank system?", *Macroprudential Bulletin 18*, ECB, Frankfurt am Main, July.

Carstens, A. (2018) "Big tech in finance and new challenges for public policy", FT Banking Summit, 4 December.

Capgemini (2024), World Payments Report 2025, Capgemini Research Institute for Financial Services, September.

Collot, S., Machover, A. and Rocher, E. (2024), The growth of big techs in the financial sector: which risks, which regulatory responses?, the French Prudential Supervision and Resolution Authority, October.

Consumer Financial Protection Bureau (CFPB) (2024), CFPB Orders Apple and Goldman Sachs to Pay Over $89 Million for Apple Card Failures, October.

Cornelli, G., Gambacorta, L. and Pancotto, L. (2023), "Buy now, pay later: a cross-country analysis", *BIS Quarterly Review*, December.

Clifford Chance (2019), "Globalisation and Financial Regulation: Challenges and Trends", October.

CMPI/IOSCO (2012), "Principles for financial market infrastructures", April.

CMPI/IOSCO (2022), "Application of the Principles for Financial Market Infrastructures to stablecoin arrangements", July.

Crisanto, J. C., Ehrentraud, J. and Fabian, M. (2021) "Big Techs in Finance: Regulatory Approaches and Policy Options", *FSI Briefs*, March.

D'Acunto, F., Rossi, A.G., Zingales, L., Wardrop, R. and Rau, R. (2021), "Robo-Advising", *The Palgrave Handbook of Technological Finance*, pp. 725-749, September.

De Nederlandsche Bank (2018), DNB Payments Strategy 2018-2021.

Doerr, S., Gambacorta, L., Guiso, L. and Sanchez del Villar, M. (2023), "Privacy regulation and fintech lending", *BIS Working Papers*, No 1103, Monetary and Economic Department, June.

Doerr, S., Frost, J., Gambacorta, L. and Shreeti, V. (2023), "Big techs in finance", *BIS Working Papers*, No 1129, Monetary and Economic Department, October.

Ehrentraud, J., Mure, S., Noble, E. and Zamil, R. (2024), "Safeguarding the financial system's spare tyre: regulating non-bank retail lenders in the digital era", *FSI Insights*, No 56, March.

Ehrentraud, J., Lloyd Evans, J., Monteil, A. and Restoy, F. (2022), "Big tech regulation: in search of a new framework", *Occasional Paper No. 20*, Financial Stability Institute, October.

Enriques, L. and Ringe, W.-G. (2020), "Bank-Fintech Partnerships, Outsourcing Arrangements and the Case for a Mentorship Regime", *Law Working Paper No. 527/2020*, European Corporate Governance Institute.

European Banking Authority (2014), "EBA Report and Opinion on matters relating to the perimeter of credit institutions", November.

European Banking Authority (2017), "Opinion and Report on regulatory perimeter issues relating to the CRDIV/CRR", November.

European Banking Authority (2019a), "Guidelines on outsourcing arrangements", February.

European Banking Authority (2019b), "Report on Regulatory perimeter, regulatory status and authorisation approaches in relation to FinTech activities", July.

European Banking Authority (2020), "Opinion of the European Banking Authority on elements of the definition of credit institution under Article 4(1), point 1, letter (a) of Regulation (EU) No 575/2013 and on aspects of the scope of the authorisation", (EBA/OP/2020/15), September.

European Banking Authority (2021), "Report on the use of digital platforms in the EU banking and payments sector", (EBA/REP/2021/26), September.

European Banking Authority (2022), "Final report on response to the nonbank lending request from the CfA on digital finance", (EBA/Rep/2022), April.

European Banking Authority (2025), "EBA report on white labelling", (EBA/REP/2025/30), October.

European Banking Authority and European Securities and Markets Authority (2025), "Joint Report on recent developments in crypto-assets (Article 142 of MiCAR)", ESMA75-453128700-1391, EBA/Rep/2025/01, January.

European Central Bank (2018), "The revised Payment Services Directive (PSD2) and the transition to stronger payments security", March.

European Central Bank (2024), "Opinion of the European Central Bank on a proposed regulation and directive on payment and electronic money services", (CON/2024/13) 1.9 and 1.10, April.

European Central Bank (2025), "Non-paper on EU and third country stablecoin multi-issuance", Financial Services Committee (WK 4742/2025), April.

European Central Bank (2026), "Opinion of the European Central Bank on proposals as regards the further development of capital market integration and supervision within the Union", April.

European Central Bank (2026a), "Eurosystem Response to the European Commission's targeted consultation on the competitiveness of the EU banking sector", April.

European Securities and Markets Authority (2025), "Fast-track peer review on a CASP authorisation and supervision in Malta", (ESMA42-2004696504-8164), July.

European Supervisory Authorities (2019), "Report on cross-border supervision of retail financial services", (JC/2019-22), July.

European Supervisory Authorities (2022), "Joint European Supervisory Authority response: to the European Commission's February 2021 Call for Advice on digital finance and related issues: regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities", (ESA 2022 01), January.

European Supervisory Authorities (2024), "Joint-ESA Report on 2023 stocktaking of BigTech direct financial services provision in the EU", (JC 2024 02), February.

European Supervisory Authorities (2025), "Joint ESA stocktaking of BigTechs' direct financial services activities in the EU", October.

European Systemic Risk Board (2023), "Crypto-assets and decentralised finance. Systemic implications and policy options", ESRB Task Force on Crypto-Assets and Decentralised Finance, May.

European Systemic Risk Board (2025), "Crypto-assets and decentralised finance: Report on stablecoins, crypto-investment products and multi-function groups", October.

Expert Group on Regulatory Obstacles to Financial Innovation (2019), "30 Recommendations on Regulation, Innovation and Finance: Final Report to the European Commission", December.

Federal Reserve Board (2024), "Cease and Desist Order Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, as amended, against Evolve Bancorp, Inc. and Evolve Bank & Trust", Washington, D.C.: Federal Reserve Board, June.

Federal Deposit Insurance Corporation (FDIC) (2023), "Consent Order on Cross River Bank's Compliance Violations FDIC-22-0040b", March.

Federal Deposit Insurance Corporation (FDIC) (2024), "Recordkeeping for Custodial Accounts", Federal Register Vol. 89, No 191, 12 CFR Part 375, RIN 3064–AG07, October.

Financial Conduct Authority (2024a), "FS24/1 – Potential competition impacts from the data asymmetry between Big Tech firms and firms in financial services", Feedback statements, April.

Financial Conduct Authority (2024b), "Early and High Growth Oversight", July.

Financial Conduct Authority (2024c), "PSR and FCA launch joint call for information on big tech and digital wallets", press release, July.

Frank, J.-U. and Peitz, M. (2023), "Market power of digital platforms", *CRC TR 224 Discussion Paper Series, Oxford Review of Economic Policy*, Vol. 39, No 1, pp. 34-46.

FSB (2019a), "FinTech and market structure in financial services: Market developments and potential financial stability implications", February.

FSB (2019b), "Decentralised financial technologies: Report on financial stability, regulatory and governance implications", June.

FSB (2019c), "BigTech in finance: Market developments and potential financial stability implications", December.

FSB (2019d), "Third-party dependencies in cloud services: Considerations on financial stability implications", December.

FSB (2022), "Fintech and Market Structure in the Covid-19 Pandemic. Implications for Financial Stability", March.

FSB (2023a), "FSB Global Regulatory Framework for Crypto-asset Activities", July.

FSB (2023b), "High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements", July.

FSB (2023c), "The Financial Stability Risks of Decentralised Finance", February.

FSB (2023d), "The financial stability implications of multifunction crypto-asset intermediaries", November.

FSB (2024), "Recommendations for regulating and supervising bank and non-bank payment service providers offering cross-border payment services", Final report, December.

FSI (2024), "The financial stability implications of multifunction cryptoasset intermediaries - Executive Summary", FSI Executive Summaries, August.

Financial Stability Oversight Council (2019), "Authority to Require Supervision and Regulation of Certain Nonbank Financial Companies", December.

Fuster, A., Goldsmith Pinkham P., Ramadorai T. and Ansgar W. (2022), "Predictably Unequal? The Effects of Machine Learning on Credit Markets", *Journal of Finance*, Vol. 77, pp. 5-47.

Gambacorta, L., Huang, Y., Li, Z., Qiu, H. and Chen, S. (2023a), "Data versus Collateral", *Review of Finance*, Vol. 27, Issue 2, pp. 369-398, March.

Gambacorta, L., Madio, L. and Parigi, B. M. (2023b), Big Tech Lending and Business Expansion, SSRN.

Garcia Ocampo, D., P. Goodrich and G.-P. Lovicu (2026), "Cryptoasset service providers as financial intermediaries: risks and policy approaches", *FSI Occasional Papers*, No 27, April.

Himino, R. (2019), "Regulating ecosystem", October.

Hodges, B. (2023), "Banking-as-a-service: FinTechs Walking the Regulatory Perimeter", *Brooklyn Journal of Corporate, Financial & Commercial Law*, Vol. 17, Issue 2, p. 130.

Institute of International Finance (2018), "A New Kind of Conglomerate: BigTech in China", November.

IMF (2018), "The Bali Fintech Agenda: A Blueprint for Successfully Harnessing Fintech's Opportunities", *Policy Papers*, 11 October.

Jeng, L., Frost, J., Noble, E. and Brummer, C. (2025), "Consumer financial data and non-horizontal mergers", *BIS Working Papers*, No 1251, Bank for International Settlements, Monetary and Economic Department, March.

Jonker, N. (2019), "What drives the adoption of crypto-payments by online retailers?", Electronic Research and Applications, Vol. 35, 100848, May-June.

Koont, N., Santos, T. and Zingales, L. (2023), "Destabilizing digital 'bank walks'", *New Working Paper Series*, No 328, The University of Chicago Booth School of Business, George J. Stigler Center for the Study of the Economy and the State.

Kress, J., McCoy, P. and Schwarcz, D. (2019), "Regulating Entities and Activities: Complementary Approaches to Nonbank Systemic Risk", *Southern California Law Review*, Vol. 92.

Kshetri, N. (2016), "Big data's role in expanding access to financial services in China", *International Journal of Information Management*, June.

Liu, L., Lu, G. and Xiong, W. (2022), "The Big Tech Lending Model", *NBER Working Paper No. w30160*.

McCaul, E. (2024), "Adapting to technological shifts: supervision in the evolving financial landscape", *Eurofi Magazine*, September.

Monetary Authority of Singapore (2019), "Payment Services Act", January.

Noble, E. (2020), "The next generation of financial conglomerates: BigTech and beyond", *Butterworths Journal of International Banking and Financial Law*, September.

Office of the Comptroller of the Currency (August 2022), "Agreement by and between Blue Ridge Bank, National Association, Martinsville, Virginia and the Office of the Comptroller of the Currency", (AA-NE-2022-43), August.

Office of the Comptroller of the Currency, Federal Reserve System, & Federal Deposit Insurance Corporation (2024), "Request for information on bank-fintech arrangements involving banking products and services distributed to consumers and businesses", Notice, July.

Office of the Comptroller of the Currency (2025), "Agreement by and between Patriot Bank, National Association, Stamford, Connecticut and the Office of the Comptroller of the Currency", (AA-NE-2025-05), EX-10.1 2 ex_767430.htm EXHIBIT 10.1., January.

Paracampo, M., Annunziata, F., Di Gabriele, N. et al. (2025), "Beyond MICA – An overview of developments on crypto-assets", G. Giappichelli Editore, Turin, December.

Restoy, F. (2019), "Regulating fintech: what is going on, and where are the challenges?", Bank for International Settlements, 16 October.

Ruof, C. (2023), "Regulating Financial Innovation: Fintech and the Information Deficit", *EBI Studies in Banking and Capital Markets Law*, Chapter 7, Section 1.1., "The Information Problem Under Fintech", August.

Sims, A. (2024), "DAOs (Decentralised Autonomous Organisations) v DINOs (DAO in Name Only or Decentralised in Name Only)", SSRN, February.

Takanashi, Y., Matsuo, S., Burger, E., Sullivan C., Miller, J. and Sato, H. (2020), "Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem, Part 1 of 2, *Stanford Journal of Blockchain, Law & Policy*, Vol. 3, No 1.

US Department of the Treasury (2018), A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation, July.

Von Kalckreuth, U., Wilson, N., Giron, C., Kochanska, U., Buthiot, E., Wicky, Y., Maza, L.Á. and Santos, R. (2022), "Fintech in statistical classifications: suggestions and tentative figures in a central bank context", 11th Biennial IFC Conference on "Post-pandemic landscape for central bank statistics", Bank for International Settlements.

Wang, Y., Xiuping, S. and Zhang, Q. (2021), "Can fintech improve the efficiency of commercial banks? —An analysis based on big data", *Research in International Business and Finance*, Elsevier, Vol. 55(C), January.

World Economic Forum & Cambridge Centre for Alternative Finance (2025), "The future of global fintech: From rapid expansion to sustainable growth (Second edition)", World Economic Forum.

Zamil, R. and Lawson, A. (2022), "Gatekeeping the gatekeepers: When big techs and fintechs own banks – benefits, risks and policy options", *FSI Insights on policy implementation*, No. 39, Bank for International Settlements.

Zetzsche D.A., Buckley R.P., Arner D.W. and Barberis, J.N. (2017), "From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance", *EBI Working Paper Series*, No 6.

Zetzsche, D.A., Buckley, R.P., Arner, D.W. and Unterstell, M. (2024), "Study on mixed-activity groups (MAGs): an assessment of MAGs' financial services in the EU against the backdrop of international trends and regulation", European Commission Directorate-General for Financial Stability, Financial Services and Capital Markets Union, Publications Office of the European Union.

Acknowledgements
The authors are grateful, for their review and comments, to Samuel Collot, Alice Filippetta, Urszula Kochanska, Daniel Knapp, Maria Julve San Martin, Cyprien Milea, James Nugent, Elisabeth Noble, Yasushi Shiina, Georgios Tsiatouras, Anton Van der Kraaij, Esther Wehmeier.
The views expressed in this paper are the authors' and do not necessarily reflect those of the European Central Bank or the Eurosystem. The authors are not part of the ECB's digital euro project team and do not contribute to it.

Phoebus L. Athanassiou
European Central Bank, Frankfurt am Main, Germany; email: phoebus.athanassiou@ecb.europa.eu

Stephanie Czák-Ludwig
European Central Bank, Frankfurt am Main, Germany; email: stephanie.czak-ludwig@ecb.europa.eu

Nico Di Gabriele
European Central Bank, Frankfurt am Main, Germany; email: nico.di_gabriele@ecb.europa.eu

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

PDF ISBN 978-92-899-7913-9, ISSN 1725-6534, doi:10.2866/0612483, QB-01-26-158-EN-N