MASTER THESIS | MASTER'S THESIS

Titel | Title

The Regulatory Framework for EU Fintech: Insights from the U.S. and Singapore

verfasst von | submitted by

Rrita Rexhepi

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 999 082
Universitätslehrgang lt. Studienblatt | Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht [Vollzeit Englisch]
Betreut von | Supervisor:	Univ.-Prof. Dr.iur. Matthias Lehmann LL.M.

Abstract

Fintech innovation, largely driven by non-bank entities, has undergone significant development over the past few years. As global financial centres, the U.S., the U.K., Singapore, and (broadly) the EU host most of the fintech firms operating today. The EU has adopted a regulation-heavy approach, with different instruments governing different aspects of fintech operations. This thesis examines some of these key regulations, specifically the Payment Services Directive II, the Electronic Money Directive II, the GDPR, the AML Framework, and the recently adopted Digital Operational Resilience Act ("DORA"). It aims to assess the combined impact of these instruments on payment service fintech firms, including how they affect innovation incentives, and determine whether the level of stringency in their scope imposes a significant burden on their operation.

To contextualise these findings, the thesis includes a comparative analysis of approaches adopted in the United States as well as Singapore. It ultimately aims to use this information to provide recommendations on improving the regulatory framework to optimally balance innovation with security and privacy.

Zusammenfassung

Finanztechnologische Innovationen (Fintech), die größtenteils von Nichtbank-Unternehmen vorangetrieben werden, haben in den vergangenen Jahren eine erhebliche Entwicklung erfahren.

Als globale Finanzzentren beherbergen die USA, das Vereinigte Königreich, Singapur und (im weiteren Sinne) die Europäische Union den Großteil der heute tätigen Fintech-Unternehmen. Die EU hat einen stark regulierungsorienti erten Ansatz gewählt, bei dem verschiedene Rechtsinstrumente unterschiedliche Aspekte der Fintech-Tätigkeit regeln.

Diese Arbeit untersucht einige dieser zentralen Regelwerke, insbesondere die Zweite Zahlungsdiensterichtlinie (Payment Services Directive II), die Zweite E-Geld-Richtlinie (Electronic Money Directive II), die Datenschutz-Grundverordnung (DSGVO), das Rahmenwerk zur Geldwäschebekämpfung (AML) sowie die kürzlich verabschiedete Verordnung über die digitale operationelle Resilienz („DORA“). Ziel ist es, die kombinierte Wirkung dieser Instrumente auf Fintech-Unternehmen im Zahlungsdienstleistungssektor zu bewerten, einschließlich der Frage, wie sie die Innovationsanreize beeinflussen, und festzustellen, ob das bestehende Regulierungsniveau den Geschäftsbetrieb spürbar erschwert.

Zur Kontextualisierung dieser Ergebnisse enthält die Arbeit eine vergleichende Analyse der Ansätze, die in den Vereinigten Staaten sowie in Singapur verfolgt werden. Letztlich soll diese Analyse dazu beitragen, Empfehlungen zur Verbesserung des regulatorischen Rahmens zu formulieren, um ein optimales Gleichgewicht zwischen Innovation, Sicherheit und Datenschutz zu erreichen.

Table of Contents

Figures

Table of Abbreviations

AIS	Account Information Services
AISPs	Account Information Service Providers
AML	Anti-Money Laundering
AMLD	Anti-Money Laundering Directive (The numbering, e.g., 3AMLD, refers to the subsequent amending directives)
AMLR	Anti-Money Laundering Regulation
API	Application Programming Interface
ASPSPs	Account Servicing Payment Service Providers
BSA	Bank Secrecy Act
CDD	Customer Due Diligence
CFPB	Consumer Financial Protection Bureau
CFT/TF	Countering the Financing of Terrorism / Terrorist Financing
DORA	Digital Operational Resilience Act
DPT	Digital Payment Token
EBA	European Banking Authority
ECB	European Central Bank
EDPB	European Data Protection Board
EMD2	Second e-Money Directive
EMIs	Electronic Money Institution
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
KYC	Know-Your-Customer
MAS	Monetary Authority of Singapore
MFA	Multi-Factor Authentication
MPI	Major Payment Institutions
MSBs	Money Services Businesses

NBPSPs	Non-Bank Payment Service Providers
PDPA	Personal Data Protection Act
PIS	Payment Initiation Services
PIs	Payment Institutions
PISPs	Payment Initiation Service Providers
PSA	Payment Services Act
PSD2	Second Payments Services Directive
PSPs	Payment Service Providers
PSR	Payment Services Regulation
SCA	Strong Customer Authentication
SPI	Standard Payment Institution
TPPs	Third Party Providers
TRM	Technology Risk Management
XS2A	Access to Accounts

Chapter I: Introduction

1.1. Financial Technologies and Their Rise in Contemporary Finance

The financial crisis of 2008 resulted in major disruptions to the financial services industry. It served as a turning point in traditional finance, previously provided quasi-exclusively by licensed banks and other institutions. The decrease of public confidence in these institutions, as well as advancements in digital infrastructure, such as machine learning and cloud computing, opened the door for new players in the sector: "digital-first" firms, which began offering financial services catered to user-experience and efficiency, often at a lower cost than traditional banks.[1]

While fintechs had always, to an extent, encroached on the finance industry, the financial crisis led these established companies to begin delivering financial products directly to both businesses and customers, and allowed them to circumvent pre-existing legacy systems and the regulatory burdens that traditional banks were subject to.[2] These included the Dodd-Frank Act in the U.S. and Basel III internationally, both adopted in response to the systemic problems of "too big to fail" culture, which imposed stricter obligations for banks, making it more difficult for them to provide riskier services.[3] Fintech firms had the opportunity to exploit this gap, and, by 2015, they had acquired significant market share in the finance sector, especially in peer-to-peer payments, retail payments, and money transfers, with public surveys by this point showing that technology companies such as Amazon and Google were perceived as more trustworthy by customers than established banks like Citibank.[4]

In developing markets, the shift was even more exacerbated. Fintech platforms had the ability to provide certain services to regions that the traditional bank system was largely unresponsive or inaccessible to. This led to a noticeable democratisation of financial services. For instance, in Kenya, transactions through payment service platform M-Pesa amounted to almost half of the country's GDP in 2017.[5] A similar occurrence was made out in Zimbabwe, where transactions through the platform EcoCash reportedly exceeded 50% of the country's GDP.[6] These developments raised regulatory concerns, especially with regard to consumer protection and financial stability.

The EU addressed some of these concerns in a series of regulatory measures, most notably the Second Payments Services Directive (PSD2), the Second e-Money Directive (EMD2), and the Anti-Money Laundering Directives.[7] Similarly, in the U.S., regulatory bodies such as the Securities and Exchange

---

[1] Douglas W Arner, Janos Nathan Barberis and Ross P Buckley, 'The Evolution of Fintech: A New Post-Crisis Paradigm?' (2015) University of Hong Kong Faculty of Law Research Paper 2015/047, UNSW Law Research Paper 2016-62 <www.ssrn.com/abstract=2676553> accessed 18 July 2025.
[2] ibid.
[3] In Lee and Yong Jae Shin, 'Fintech: Ecosystem, Business Models, Investment Decisions, and Challenges' (2018) 61 Business Horizons 35.
[4] Arner, Barberis and Buckley (n 1).
[5] Bitange Ndemo and Ben Mkalama, 'Digitalisation and Financial Data Governance in Africa: Challenges and Opportunities' in Bitange Ndemo and others (eds), *Data Governance and Policy in Africa* (Springer International Publishing 2023) <https://link.springer.com/10.1007/978-3-031-24498-8_6> accessed 13 August 2025.
[6] ibid.
[7] 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 (Text with EEA relevance) [2015] OJ L337/35 (PSD2); 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 (Text with EEA relevance) [2009] OJ L267/7 (EMD2); Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money

Commission and the Consumer Financial Protection Bureau ("CFPB") began to issue guidance papers in an effort to prompt a harmonised framework for both bank and non-bank financial service providers.[8] Gaps in these regulations created uncertainty for market entrants and, to a degree, created a tension between encouraging further innovation and ensuring supervisory control.

Fintech products and services have been subject to varying degrees of regulation, both across jurisdictions and within them. Additionally, both the products and the regulatory approaches directed at them are still evolving and attempting to adapt to rapid technological developments. In many cases, the regulatory response has lagged behind evolving technology, resulting in it being fragmented or insufficiently reflective of market realities. Moreover, regulators are facing increasing pressure to find solutions that are both innovation-friendly and preserve operational resilience.

1.2. Purpose of Study

The objective of this thesis is to examine how the European Union has handled this tension more closely. Specifically, it aims to look into how the EU governs fintech providers in the payment services and e-money space and assess how this framework impacts innovation in these areas. It considers key regulatory measures fintechs have to follow, such as licensing, AML/KYC obligations, operational resilience, and data protection. It describes these measures, then analyses their collective effect on innovation in the industry. By adopting a comparative approach, using the U.S. and Singapore as reference models, the thesis aims to assess whether the regulatory instruments in place that govern fintech in the EU are efficient in finding the balance between enabling innovation and maintaining financial stability and security.

1.3. Research Questions

For the purpose of this study, this thesis explores the following questions:

1. Which regulatory instruments in the EU govern payment service and e-money fintech firms, and how do they interact with one another?
2. In what ways do these compliance requirements both enable and constrain innovation within EU fintech firms?
3. How does the EU's regulatory approach compare with those in the U.S. and Singapore, and what lessons can be drawn from these regimes in achieving a balance between fostering innovation and maintaining market integrity?

1.4. Scope and Delimitation

This thesis focuses on the regulatory frameworks governing non-bank financial technology firms ("fintechs") that provide payment services and/or issue electronic money ("e-money"). It does not cover investment-based fintech services (such as robotic financial advisory or wealth management technologies). Similarly, it excludes crypto-currency service providers and blockchain technologies, which, in the EU, are primarily covered by the Markets in Crypto-Assets Regulation (MiCA), and P2P lending platforms, which are covered by the Consumer Credit Directive.[9] Additionally, the thesis does

laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L156/43 (5AMLD).

[8] Bureau of Consumer Financial Protection, 'Compliance Bulletin and Policy Guidance; 2016-02, Service Providers' (4810-AM-P, 2016).

[9] Nofie Iman, 'The Rise and Rise of Financial Technology: The Good, the Bad, and the Verdict' (2020) 7 Cogent Business & Management 1725309.

not address banking regulations applicable to credit institutions, except insofar as they relate to partnerships with non-bank fintech firms.

The analysis centres on how these entities are regulated within the EU and compliance mechanisms applicable under EU law. Particularly, it will explore the following: a) licensing and registration requirements; b) anti-money laundering and know-your-customer obligations; c) data protection rules; and d) risk management and digital operational resilience. The primary focus is on the EU framework, with the U.S. and Singapore serving as comparative reference points, considering their status as large fintech innovation hubs.

1.4. Methodology

The thesis will consist of a qualitative evaluation of the EU legal framework, drawing from EU legal sources including legislation and proposals. It will apply a comparative approach when discussing the contrasting environments in the U.S. and Singapore. It will also use secondary sources, including academic literature and specific case studies with firms operating in each jurisdiction.

Chapter II: Conceptual Framework

The term 'fintech' is a neologism derived from "financial technology", describing modern technologies that manage core financial activities.[10] While there is no uniformly accepted definition of the term as of now, most definitions emphasize the use of technology in improving financial services.[11] Fintech is representative of a recent shift in the financial sector wherein the primary driver of innovation has become information technology. This shift has allowed institutions to introduce more agile, data-driven, and user-friendly approaches outside of the confines of traditional finance structures.[12] As such, it has also caused disruptions to existing business models, products, and regulatory measures of protection.

The evolution of fintech has been driven by a range of advanced (and often, interrelated) technologies, namely artificial intelligence, big data analytics, cloud computing, and distributed ledger technology.[13] These technologies are used to support efficiency and security, but also to reduce operational costs for firms and allow them more space to gain competitive advantages over traditional institutions.[14] Fintechs touch on several market segments, including retail/investment banking, wealth management, insurance, and regulatory compliance.[15] Considering this range, they have triggered structural changes in various sections within the financial ecosystem.[16] Different players (including fintech startups, BigTech, and decentralised networks) increasingly operate in collaborative environments, relying on each other for shared resources.[17] In this context, the boundaries between technology and finance are becoming blurred. Reliance on third-party service providers has increased, as has convergence between sectors (worth mentioning are social media companies which have begun to additionally offer financial services, e.g. Facebook's Meta Pay).[18] In addition to this, it has also led to a wave of new regulatory and supervisory challenges. Regulators have to face an interdependent financial system in which innovation is distributed across a network of actors with diverse functions.[19]

From a regulatory perspective, fintech firms in the payment and e-money sector are broadly categorised into two regulatory groups: bank and non-bank providers.[20] This distinction is fundamental to understanding the regulatory frameworks that govern financial services in the EU. Traditional banks, regulated partly by the Capital Requirements Directive IV (CRD IV), are subject to more extensive oversight and are growingly collaborating with (and competing against) non-bank entities.[21]

---

[10] ibid.
[11] Arner, Barberis and Buckley (n 1).
[12] Iman (n 9); Oskar Kowalewski and Paweł Pisany, 'The Rise of Fintech: A Cross-Country Perspective' (2023) 122 Technovation 102642.
[13] Dirk Andreas Zetzsche and others, 'Fintech Toolkit: Smart Regulatory and Market Approaches to Financial Technology Innovation' (2020) University of Hong Kong Faculty of Law Research Paper No 2020/027.
[14] Shahriar Akter and others, 'Transforming Business Using Digital Innovations: The Application of AI, Blockchain, Cloud and Data Analytics' (2022) 308 Annals of Operations Research 7.
[15] Arner, Barberis and Buckley (n 1).
[16] Iman (n 9).
[17] Bengt Larsson and others, 'Digital Disruption Diversified—FinTechs and the Emergence of a Coopetitive Market Ecosystem' (2024) 22 Socio-Economic Review 655.
[18] Arner, Barberis and Buckley (n 1).
[19] Zetzsche and others (n 13).
[20] Johannes Ehrentraud and others, 'Fintech and Payments: Regulating Digital Payment Services and e-Money' (Bank for International Settlements (BIS), Financial Stability Institute, FSI Insights on policy implementation, No 33, 2021).
[21] Lee and Shin (n 3); See also 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 and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance [2013] OJ L176/338.

Non-Bank Payment Service Providers (NBPSPs) serve as a core regulatory category under the current framework.[22] These are legal entities authorised to provide payment services, including executing transfers, initiating payments, and issuing payment instruments.[23] These non-bank fintechs, operating under licenses for Payment Institutions or Electronic Money Institutions, are the focus of innovation in the EU's digital finance market. Their licensing is conditional on satisfying certain requirements depending on what services they offer. For instance, fintechs that offer payment initiation have to meet a EUR 50,000 initial capital requirement.[24] This is meant to ensure operational resilience without imposing the full regulatory requirements that are applicable to banks.[25]

While Payment Institutions are not allowed to issue e-money, Non-Bank Electronic Money Institutions (EMIs) are permitted to do so.[26] These institutions are regulated primarily under the Electronic Money Directive (EMD2) and must comply with additional safeguarding rules not applicable to PIs.[27] EMIs also face licensing and minimum capital requirements; however, unlike PIs, they are specifically authorised to issue stored value (e-money), making them particularly relevant in the mobile payment space.

A new phenomenon manifests itself in "hybrid" models. Such models may include partnerships between banks and fintechs (e.g. Banking-as-a-Service arrangements), wherein a fintech uses a licensed bank's infrastructure and provides technical services in exchange.[28] Banks may outsource technological innovation while covering regulatory responsibilities on behalf of fintechs. This dynamic has contributed to a diversified financial services ecosystem, in which banks and fintechs are both cooperators and competitors of each other.[29] Studies show that banks often partner with fintechs to adapt to shifting market expectations, particularly with user experience and speed of service execution.[30]

Payment institutions, e-money issuers, and hybrids together shape the structure of non-bank fintech regulation in the EU. Fintechs operating under these categories often incorporate high-end technological infrastructures that regularly introduce new regulatory concerns.[31] For example, cloud-native fintechs have raised concerns under the EU's Digital Operational Resilience Act due to the amplified risk and potential vulnerabilities of the interconnectedness inherent in their structures.[32] Overall, these business models are indicative of a need to adopt an adaptable and coherent regulatory framework that can address and keep up with the evolving realities of the digital finance sector.

[22] Ehrentraud and others (n 20).
[23] ibid.
[24] PSD2 art 7(b).
[25] Lee and Shin (n 3).
[26] See PSD2 art 18(3); EMD2 art 2(1).
[27] EMD2 art 7.
[28] Larsson and others (n 17).
[29] ibid.
[30] ibid.
[31] Wolf-Georg Ringe and Christopher Ruof, 'Regulating Fintech in the EU: The Case for a Guided Sandbox' (2020) 11 European Journal of Risk Regulation 604.
[32] Zetzsche and others (n 13).

Chapter III: The Core EU Legal Framework: PSD2 and EMD2

3.1. Introduction to Fintech Regulation in the EU

The European Union's regulatory approach to fintech is built on several principles which cumulatively aim to reconcile exponential technological development with systemic safeguards to protect investors and consumers.[33] It is also built on an intent to foster innovation and competitive practices.[34] Through its policies, the EU has emphasised reducing regulatory uncertainty and embracing a unified digital market, and thus has made efforts to implement clear and uniform rules.[35]

Fintech regulation in the EU was initially characterised by regulatory fragmentation across Member States and a lack of technology-neutral rules, which placed firms in uncertain legal territory.[36] Most innovative fintechs found themselves in a regulatory "grey zone" due to overly broad legal categories or non-neutral policies.[37] In addition, information asymmetries, driven largely by the rise of AI, data-driven services, as well as the mass concentration of main actors outside of the EU, have hindered its ability to shape appropriate regulatory measures, albeit initiatives like the AI Act illustrate its rapid response to such developments.[38]

In 2018, the EU launched its Fintech Action Plan and was soon followed by rollouts of national-level regulatory sandboxes in some Member States under its guidance, as well as "hard" regulatory measures in domains like AML, cybersecurity, and digital banking.[39] The Action Plan has three main objectives: supporting innovative business models, encouraging new technologies in the finance sector, and increasing the security and integrity of the financial system.[40] The introduced regulatory sandboxes allowed for controlled environments where firms can test new financial products under supervision from competent authorities. Under the sandbox model followed by states such as Denmark and Lithuania, national competent authorities utilise the European Banking Authority's Fintech Knowledge Hub to establish a 'feedback loop' in which they can continuously share information under regulatory guidance.[41]

Although some fintech sub-sectors are regulated more loosely (e.g. certain cryptocurrency activities), others, particularly payment services and e-money issuers, are governed by a robust legal framework. This framework is primarily composed of the following instruments:

- The Second Payment Services Directive (PSD2);[42]
- The Second Electronic Money Directive (EMD2);[43]

---

[33] Uniwersytet Ekonomiczny w Krakowie and others, 'FinTech Regulation and the Development of the FinTech Sector in the European Union' (2023) 2023 Journal of Banking and Financial Economics 44.
[34] Kowalewski and Pisany (n 12).
[35] Uniwersytet Ekonomiczny w Krakowie and others (n 33).
[36] Ringe and Ruof (n 31).
[37] ibid.
[38] Giovanni Briganti Dini, 'The EU's Response to the Fragmented Emergence of Artificial Intelligence' in Oriol Costa, Eduard Soler and Martijn Vlaskamp (eds), *EU foreign policy in a fragmenting international order* (Palgrave Macmillan 2025).
[39] Directorate-General for Financial Stability, Financial Services and Capital Markets Union, 'Fintech Action Plan' (2018) Communication; Uniwersytet Ekonomiczny w Krakowie and others (n 33).
[40] European Commission, 'EU Blockchain Observatory and Forum' (*Shaping Europe's digital future*, 24 July 2017).
[41] Ringe and Ruof (n 31).
[42] PSD2.
[43] EMD2.

- The Anti-Money Laundering Directives (AMLDs), as well as the Anti-Money Laundering Regulation (AMLR) adopted in 2024most;[44]
- The General Data Protection Regulation (GDPR);[45]
- The Digital Operational Resilience Act (DORA)[46]

These instruments collectively establish the operational conditions, licensing requirements, risk management standards, and compliance obligations for non-bank fintechs[47]. They form the legal foundation for most fintech firms engaged in payment processing, e-money services, and digital banking across the EU[48]. Among these, PSD2 and EMD2 serve as the two core instruments specifically governing non-bank actors offering payment services and issuing e-money, respectively[49]. While their exact scopes are different, they are tightly interlinked, and many providers operate under both regimes[50]. Together, PSD2 and EMD2 cover the legal and operational structure of the most prevalent fintech business models in Europe.

This chapter will examine both of these instruments in detail. It will explore the rationale and design of each directive before analysing the core requirements and their implications for fintechs, with specific attention paid to authorisation, conduct obligations, and operational safeguards.

3.2. The Revised Payment Services Directive

3.2.1. Purpose and Scope of the PSD2

The Second Payment Services Directive has intensely shaped the fintech and payments landscape in the EU. It is a foundational instrument which opened up digital financial services within the internal market[51]. Its predecessor, the first Payment Services Directive, was adopted in December 2007 and aimed to harmonise and integrate electronic retail payments in Europe by considering non-bank providers such as electronic money institutions and payment institutions.[52] It established rules for market

[44] See Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (Text with EEA relevance) [2024] OJ L 2024/1640 (6AMLD); Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance) [2024] OJ L2024/1624 (AMLR).
[45] 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) (Text with EEA relevance) [2016] OJ L119/1 (GDPR).
[46] 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 (Text with EEA relevance) [2022] OJ L333/1 (DORA).
[47] Uniwersytet Ekonomiczny w Krakowie and others (n 33).
[48] ibid.
[49] European Commission, Directorate General for Financial Stability, Financial Services and Capital Markets Union, VVA, and CEPS, *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*. (Publications Office 2023) <https://data.europa.eu/doi/10.2874/996945> accessed 28 August 2025.
[50] ibid.
[51] Michał Polasik and others, 'The Impact of Payment Services Directive 2 on the PayTech Sector Development in Europe' (2020) 178 Journal of Economic Behavior & Organization 385.
[52] Dermot Turing and Simon Crown, '21st Century Payments in Europe: The Payment Services Directive' (2006) 2 Journal of Payment Systems Law 639.

participants and business conduct, including exchange rates, information provision on charges, as well as detailed rights and obligations for both providers and users.[53]

However, PSD1 was unable to adequately confront challenges arising from technological advancements of the years following, in particular, the rise of mobile payments, digital financial services, and fintech startups[54]. These led to security, privacy, and supervision concerns, especially arising from the use of peer-to-peer cash systems and cryptocurrency, which hindered consumer confidence and, in turn, the growth of payment services[55]. In response to limitations and regulatory gaps, the European Parliament adopted the Revised Payment Services Directive in 2015, with a transposition timeline for Member States that lasted until January 2018. A second phase of implementation began in 2019, focusing largely on additional Strong Customer Authentication (SCA) requirements.[56]

PSD2 has several objectives, including enhancing consumer protection, increasing security for payment services, boosting competition, driving innovation through Open Banking, improving market efficiency, and closing regulatory gaps.[57] Open Banking is a core principle driving PSD2, allowing third-party providers (TPPs), including non-bank entities, to access bank accounts and offer payment services. This provision enables a new business model where services like personal finance management and direct-to-account payments can be offered independently of banks, inducing these banks to compete on user experience, innovation, and pricing.[58]

The scope of PSD2 is outlined in Article 2 and encompasses a geographic and a material dimension. Geographically, PSD2 applies to payment services provided within the Union, including services offered by entities registered in third countries to the extent that they operate within the EU[59]. The directive primarily governs transactions in EU and EEA currencies where both the payer and the payee's payment service providers (PSPs) are located within the Union (so-called "two-leg" transactions)[60]. However, certain provisions of PSD2 may also apply in cases involving one PSP within the Union and one outside, particularly regarding transparency and information requirements[61].

Materially, PSD2 primarily renders the following types of entities subject to regulation:

a) Payment Institutions (PIs): Non-bank firms authorised to provide one or more payment services.[62]
b) Credit Institutions: Traditional banks that offer payment services as part of their financial activities. Certain public institutions, such as the European Central Bank and national banks, are also covered by the Directive.[63]
c) Electronic Money Institutions (EMIs): Entities licensed under the Revised Electronic Money Directive that may also provide payment services, subject to PSD2 requirements.[64]

[53] ibid.
[54] Adebola Adeyemi, 'A New Phase of Payments in Europe: The Impact of PSD2 on the Payments Industry' (2019) 25 Computer and Telecommunications Law Review 47.
[55] ibid.
[56] PwC Austria, 'PSD2 – In a Nutshell' (2017) <www.pwc.at/de/publikationen/financial-services/psd2-nutshell-01-at.pdf> accessed 28 August 2025.
[57] PSD2 rec 4–8.
[58] Adeyemi (n 54).
[59] PSD2 art 2.
[60] ibid.
[61] Adeyemi (n 54).
[62] PSD2, art 1(1)(d).
[63] ibid art 1(1)(a).
[64] ibid art 1(1)(b).

A significant addition under PSD2 is the explicit introduction and regulation of Third-Party Providers (TPPs), allowing non-bank entities to access customer bank accounts, provided they have the user's consent, without necessarily having access to funds.[65] These entities normally fall into one of two categories:

a) Payment Initiation Services (PIS): services allowing third parties (Payment Initiation Service Providers or "PISPs") to initiate payment transactions at the payer's request from an account held by another payment service provider.[66] PISPs do not hold the payer's funds at any stage of the payment chain.[67]
b) Account Information Services (AIS): online services (provided by Account Information Service Providers or "AISPs") which provide consolidated information on one or more payment accounts held by a payment service user with one or more payment service providers.[68]

PSD2 established the regulatory elements governing the authorisation, operation, and oversight of PSPs within the EU. It represents an upgrade to regulation of the traditional banking system and drastically changed the regulatory environment under which payment service providers in the EU operate.[69] Furthermore, PSD2 served to foster innovation, and can be tied to a rapid surge in PayTech start-ups in Europe which primarily occurred after its adoption.[70] It was specifically designed to accelerate innovation in the payment services market and create new opportunities for start-ups at a pan-European level.[71] This was especially reflected in countries like Lithuania and Malta, which, despite their country size, have successfully attracted numerous PayTech entities by offering regulatory sandboxes and friendly regulatory environments.[72]

This chapter focuses on those compliance obligations under PSD2 that directly affect fintechs' operational capacity and innovative potential, particularly those that create frictions or incentives in how new business models are developed. These include registration and licensing procedures, Open Banking, Strong Customer Authentication, and risk management. Broader consumer protection or purely administrative requirements are addressed only where relevant.

3.2.2. Registration and Licensing Requirements

The Second Payments Services Directive introduced specific licensing, authorisation, and registration requirements for various fintech entities. It was built upon an existing prudential regime established by the first PSD, which introduced a single license for all payment service providers (PSPs) not involved in taking deposits or issuing electronic money.[73] PSD2 provides a comprehensive framework for non-bank financial entities using new technologies. In this context, it acts like a passport for payment companies and enables them to freely move within the EU and serve customers after they've met specific requirements.[74]

A fintech entity operating in the payment sector is generally required to obtain authorisation as a "payment institution" from the national competent authority in the Member State where it has its

[65] Polasik and others (n 51).
[66] PSD2 art 4(15).
[67] ibid rec 31.
[68] ibid art 4(16).
[69] Polasik and others (n 51).
[70] ibid.
[71] ibid.
[72] ibid.
[73] PSD2 rec 26.
[74] ibid art 11(9).

registered office, and where it carries out at least part of its payment service business.[75] Only after this authorisation can it commence the provision of payment services alongside traditional credit institutions, unless it falls into an exempt category.[76] The competent authority grants authorisation if the application complies with all requirements and if it classifies its overall assessment as favourable.[77] Conversely, they may refuse to authorise it if shareholders or members with qualifying holdings are deemed unsuitable.[78]

To obtain authorisation as a payment institution, applicants are required to submit detailed and comprehensive documentation, including a business plan, their corporate and organisational structure, as well as risk documentation.[79] Furthermore, the application must provide evidence of safeguarding measures for customer funds in accordance with Article 10 of the Directive, details of outsourcing arrangements, and any data collection methodologies they use.[80] Finally, the competent authority also assesses evidence of management fitness and ownership suitability.[81]

Payment institutions are required to hold initial capital requirements at the time of authorisations, although thresholds vary depending on the specific service being offered.[82] Money remittance services are subject to a minimum initial capital of EUR 20,000, payment initiative services are subject to a minimum initial capital of EUR 50,000, and other payment services, excluding account information services, are subject to a minimum capital requirement of EUR 125,000.[83] This includes placing/withdrawing cash from accounts, executing direct transfers, and issuing payment instruments. Beyond initial capital, PIs' own funds must not fall below the higher of the initial capital or an amount calculated using a prescribed method based as determined by national authorities.[84]

Firms must also demonstrate how they intend to safeguard customer funds.[85] Client funds received for transactions must not be lumped in with the firm's own funds.[86] They must either be deposited in a separate account or invested in secure, low-risk liquid assets by the end of the business day following receipt of the service.[87] Alternatively, funds may be covered by an insurance policy or comparable guarantee from an independent insurance or credit institution.[88] Payment institutions are not allowed to accept deposits from users, and user funds can only be used for rendering payment services.[89]

Outside of payment institutions, PSD2 also applies to Third Party Providers (TPPs), which can seek licensing as Payment Initiation Service Providers (PISPs) or Account Information Service Providers (AISPs), depending on their function. They are subject to distinct registration and authorisation

[75] ibid art 11(1-3).
[76] ibid art 11(1).
[77] ibid art 11(2).
[78] ibid art 11(6).
[79] ibid art 5(1).
[80] ibid.
[81] ibid.
[82] ibid art 7.
[83] ibid art 7(a-c).
[84] ibid art 8(1).
[85] ibid art 5(1)(d).
[86] ibid art 10(1)(a).
[87] ibid.
[88] ibid art 10(1)(b).
[89] ibid art 18(5).

requirements, depending on their function.[90] PISPs have to undergo a full authorisation procedure, where AISPs are subject to a simpler registration regime.[91]

Since these entities do not hold client funds, imposing full own funds requirements akin to those applicable to payment institutions is often deemed inappropriate.[92] Instead, PSD2 obliges undertakings applying for authorisation as PISPs, or for registration as AISPs, to hold professional indemnity insurance or a comparable guarantee which covers the territories in which they offer services to cover their liabilities.[93] The European Banking Authority has issued regulatory guidance on the criteria for setting the minimum amount of this insurance or guarantee, considering factors such as the undertaking's risk profile, activity size (value of initiated transactions for PISPs, number of clients for AISPs), and the characteristics of the guarantee.[94]

Member States are required to establish a public register where authorised payment institutions and their agents are entered.[95] Once authorised, the institution is listed in the national register as well as the central EBA register, which is kept up to date by Member States.[96] Under Articles 28-29, it may then "passport" its services across EU Member States, meaning it can operate in other states without needing a separate license[97]. This right of establishment or freedom to provide services is subject to a notification procedure between the home and host authorities.[98] Payment service providers have a general obligation to notify competent authorities of any changes affecting the accuracy of information provided, without undue delay[99].

PSD2 allows for exemptions from some or all authorisation conditions for small-scale payment service providers under Article 32, provided that the average total value of monthly transactions in the preceding 12 months does not exceed EUR 3 million.[100] They may be registered in a public register instead of being subject to the full authorization procedures.[101] However, these exempted firms do not benefit from passporting rights and cannot access EU-wide payment systems under the same terms as fully authorised institutions.[102]

Article 3 also provides several exclusions from the Directive altogether.[103] For fintechs whose services fall under one of the exclusions in Article 3 of PSD2, such as those operating in limited networks (e.g. store cards) or those processing payments related to charitable donations, there is no requirement for authorisation.[104] However, if the annual value of such transactions exceeds EUR 1 million, they must

[90] ibid art 5(2-3).
[91] ibid.
[92] ibid rec 35.
[93] ibid.
[94] European Banking Authority, 'Guidelines on the Criteria on How to Stipulate the Minimum Monetary Amount of the Professional Indemnity Insurance under PSD2' (EBA-GL-2017-08, 2017).
[95] PSD2 art 14(1).
[96] ibid art 15(1).
[97] ibid art 11(9).
[98] ibid art 28(1).
[99] ibid art 16.
[100] ibid art 32(1)(a).
[101] ibid art 14(2).
[102] Ibid art 32(3).
[103] Ibid art 3.
[104] ibid.

notify national authorities[105]. The authority will then assess whether the exemption still applies or whether full authorisation is required.[106]

3.2.3. Open Banking (Access to Accounts – XS2A)

A core regulatory pillar of PSD2 is its mandate for Open Banking, referred to also as Access to Accounts (XS2A). This principle compels banks to open up their customer payment account data and payment initiation capabilities to authorised Third-Party Providers, a mandate which broke the historical control banks had over customer transaction information, meant to enhance competition in the internal payments market.[107] As mentioned previously, PSD2 defines and regulates two new payment services to facilitate this openness: Account Information Services (AIS) and Payment Initiation Services (PIS). Under this framework, AIS Providers are able to access users' information, such as transaction history, with their explicit consent.[108] To operationalise this, PSD2 requires banks to open their Application Programming Interfaces (APIs) to Third-Party Providers[109]. This access should not be dependent on pre-existing contractual relationships between the TPP and the Account-Servicing or Payment Service Provider (e.g. the bank).[110] Furthermore, it must be granted on an objective, non-discriminatory, and proportionate basis, allowing any fintechs that use them to operate efficiently.[111]

Under PSD2, Open Banking relies on the Regulatory Technical Standards on Strong Customer Authentication (SCA) and Common and Secure Open Standards of Communication (CSC) to enable secure interaction between TPPs and account providers.[112] These standards ensure that AISPs and PISPs can securely and seamlessly access account information, with a particular focus on ensuring the protection of users' personal data. Data exchanges must be communicated through secure channels and be encrypted and mutually authenticated.[113] It should be noted, however, that despite its intent to facilitate secure and easy access, the lack of common standards for APIs has led to difficulties with EU-wide interoperability and has thus stalled cross-border development.[114]

The introduction of Open Banking has created some tension between existing credit institutions and new entrants. It was envisioned as a catalyst to disrupt the banks' control over customer transaction information and promote competition in the payments market.[115] Traditional banks, which previously had a monopoly over such information, now had to face the challenge of opening their core systems to fintechs offering potentially faster and cheaper services.[116] Many banks initially adopted a minimal compliance and less innovation-friendly approach, often due to the costs of updating their IT systems.[117] However, Open Banking prompted fintech start-ups to develop financial services ranging from payment

[105] ibid art 37(2).
[106] ibid.
[107] Inna Romanova and others, 'The Payment Services Directive II and Competitiveness: The Perspective of European Fintech Companies' (2018) XXI European Research Studies Journal 3.
[108] PSD2 art 4(15)-(16), art 67(2)(a).
[109] ibid arts 66-67; Daniel Możdżyński, 'The Conceptions of New Payment Methods Based on Revised Payment Services Directive (PSD2)' (2017) 6 Information System in Management 50.
[110] PSD2 art 66(5); ibid 67(4).
[111] ibid art 36.
[112] ibid art 98(1).
[113] ibid.
[114] Rodrigo Zepeda, 'PSD2: Regulation, Strategy, and Innovation' (2024) SSRN Electronic Journal <www.ssrn.com/abstract=4998317> accessed 28 August 2025.
[115] Alan Brener, 'Payment Service Directive II and Its Implications' in Theo Lynn and others (eds), *Disrupting Finance* (Springer International Publishing 2019) <https://link.springer.com/10.1007/978-3-030-02330-0_7> accessed 28 August 2025.
[116] Adeyemi (n 54).
[117] Zepeda (n 114).

initiation to personalised management tools.[118] This heightened competition pushed traditional banks to modernise their systems and develop customer-facing innovations to retain market share.[119]

3.2.4. Strong Customer Authentication (SCA)

While its role within Open Banking ensures the security of customer data accessed by TPPs, Strong Customer Authentication (SCA) has a broader function within the PSD2 framework. The fundamental concept of SCA is to secure electronic transactions by requiring multi-factor authentication (MFA). The legal basis for this is outlined in Article 97, which states that a PSP must apply strong customer authentication when a payer accesses their account online, initiates an electronic payment transaction, or carries out any action through a remote channel that may give rise to fraud risks.[120]

For electronic remote payment transactions, Article 97(2) further specifies that SCA must include elements that link the transaction to a specific amount and a specific payee, in order to reduce risks from mistakes or fraudulent activity.[121] Moreover, PSPs are required by Article 97(3) to implement adequate security measures to protect the confidentiality of and integrity of users' personal credentials.[122] These requirements also extend to payments initiated through PISPs and information requests made via AISPs.[123]

The security requirements for SCA dictate that authentication must be based on the use of two or more elements categorised as knowledge, possession, and inherence, which must be independent of each other.[124] 'Knowledge' refers to something only the user knows, such as a password; 'possession' refers to something only the user has, such as a phone or a physical card; and 'inherence' refers to a unique characteristic of the user, such as a fingerprint or facial scan.[125] PSD2 acknowledges that it is not always necessary to or convenient to apply the same level of scrutiny for all transactions and allows for exemptions in certain low-risk scenarios.[126] For instance, transactions valued below EUR 30, or recurring transactions of the same amount to the same payee, are not subject to these requirements.[127]

SCA's introduction was intended to reduce online payment fraud and has successfully led to considerable drops in such incidents.[128] By mandating MFA, it ensures that both the payee and the payer are legitimate.[129] However, this implementation has also had its impact on user experience, with surveys showing that consumers often abandon complex payment processes.[130] Furthermore, not-so-user-friendly practices by banks often redirect customers to multiple pages or compel them to use multiple

[118] TrustBuilder, 'PSD2 and PSD3 Directive: How Are Payments Evolving in Europe?' <https://www.trustbuilder.com/en/psd2-psd3-directive-future-payments-europe/> accessed 28 August 2025.
[119] Amir Radnejad, Oleksiy Osiyevskyy and Olivia Scheibel, 'Learning from the Failure of the EU Payment Services Directive (PSD2): When Imposed Innovation Does Not Change the Status' (2021) 6 Rutgers Business Review 79.
[120] PSD2 art 97(1).
[121] ibid art 97(2).
[122] ibid art 97(3).
[123] ibid art 97(4).
[124] PSD2 art 4(30); Brener (n 115).
[125] Brener (n 115).
[126] ibid.
[127] ibid.
[128] 'PSD2 and PSD3 Directive: How Are Payments Evolving in Europe?' (n 118).
[129] Brener (n 115).
[130] Zepeda (n 114).

smartphones.[131] PSD3, the forthcoming updated directive, aims to address user experience concerns by promoting accessible processes and interfaces.[132]

In practice, SCA implementation has encountered some challenges. A primary issue was the significant burden placed on banks to meet technological implementation deadlines.[133] This has driven them to adopt a "patchwork" approach to their systems, instead of altering them at their core to adapt to the new industrial and regulatory realities.[134] Moreover, consumer awareness of, and trust in, Open Banking is low, with repeated concerns about data privacy breaches.[135] This has rendered the anticipated benefits of SCA, such as widespread user adoption of new payment services, unable to be fully realised.

3.2.5. Operational and Security Risk Management, and Incident Reporting

In addition to obligations related to open banking and authentication, PSD2 imposes operational and security requirements that affect the internal risk and compliance structures of payment fintechs. These include frameworks for operational and security risk management and comprehensive incident reporting. PSPs are mandated to proactively identify and respond to potential threats in order to protect transaction security and user data.[136]

Article 95(1) of PSD2 explicitly requires Member States to ensure that PSPs establish frameworks with appropriate mitigation measures and control mechanisms to manage potential risks.[137] This includes establishing and maintaining effective incident management procedures, especially for detecting and classifying major operational and security incidents.[138] Moreover, as part of their application for authorisation, payment institutions must submit a security policy document laying out their risk assessment mechanisms, including the security controls and mitigation measures taken to protect payment service users.[139] PSPs are also obliged to provide their national competent authority with an annual comprehensive assessment of potential risks, and the adequacy of the mitigation measures they have in place.[140] Under Article 95(3) and (4), the European Banking Authority (EBA), in cooperation with the European Central Bank, is tasked with issuing guidelines and developing regulatory technical standards (RTS) to specify these security measures.[141] The directive also promotes information sharing regarding operational and security risks among competent authorities, and between them and the ECB.[142]

A critical component of PSD2's security framework is its emphasis on incident reporting. Article 96(1) of PSD2 mandates that in the event of a major security incident, PSPs must notify their national competent authority without undue delay.[143] If the incident impacts, or may impact, the financial interests of users, the PSP is additionally required to inform its affected users directly, without delay, advising them on steps they can take to mitigate negative effects.[144] Once notified, the national authority

[131] ibid.
[132] 'PSD2 and PSD3 Directive: How Are Payments Evolving in Europe?' (n 118).
[133] Zepeda (n 114).
[134] Radnejad, Osiyevskyy and Scheibel (n 119).
[135] Zepeda (n 114).
[136] PSD2 art 95(1).
[137] ibid.
[138] ibid rec 91.
[139] ibid art 5(1)(j).
[140] ibid art 95(2).
[141] ibid art 95(3-4).
[142] ibid art 95(5).
[143] ibid art 96(1).
[144] ibid.

must then communicate the matter to the EBA and the ECB on payment-relevant issues.[145] This coordinated approach enables competent authorities to take the measures necessary to protect the immediate safety of the financial system. While these measures have been criticised for disproportionately burdening smaller or newer market entrants, they have also been credited with enhancing ecosystem resilience and strengthening fraud prevention.[146]

3.3. The Second Electronic Money Directive

3.3.1. Purpose and Scope of EMD2

The Electronic Money Directive 2009/110/EC (EMD2) replaced Directive 2000/46/EC, aiming to address issues that had hindered the development of a single market for electronic money services.[147] Similarly to PSD2, the Directive aims to develop the single market through a single passport for EMIs and the principle of home country control, which allows an EMI licensed in one Member State to operate across the EU.[148] Another key objective is to avoid the distortion of competition between traditional credit institutions and EMIs.[149] The ECB believed early regulations would promote innovation by providing legal certainty and preventing market fragmentation.[150]

EMD2 is particularly relevant because larger EU-based payment service fintechs typically opt to obtain EMI licensing to expand their operations.[151] This means that EMD2 and PSD2 work in parallel to form the core legal framework under which they operate, with EMD2 functioning as *lex specialis* vis-à-vis PSD2 for entities issuing stored electronic value.[152] In fact, many provisions of the PSD apply to EMIs by explicit cross-reference.

The territorial and material scope of application of EMD2 covers activities within the EU and the entities expressly permitted to issue electronic money.[153] As per Article 1(1), these entities include credit institutions, EMIs, post office giro institutions, the ECB and national central banks (when not acting as monetary authorities), and some public authorities.[154] Beyond issuing e-money, EMIs may provide payment services, grant credit related to payment services, operate payment systems, and conduct other business activities, but cannot issue e-money via agents.[155] The directive also excludes monetary value stored in limited-use instruments such as store or fuel cards and for digital goods/services with intrinsic value (i.e. digital media that is valuable in itself and not just a token for payment).[156] Unlike credit institutions, EMIs cannot take deposits or grant credit from e-money funds, nor can they pay interest on e-money holdings.[157] They operate under a lighter regime than banks, with a lower initial capital requirement of EUR 350,000 (Article 4 EMD2), compared to the EUR 1 million under the previous Directive of 2000.[158] However, they are generally subject to more restrictions on their business activities

[145] ibid art 96(2).
[146] Zepeda (n 114).
[147] EMD2 rec 2.
[148] ibid rec 4.
[149] ibid rec 14.
[150] Malte Krueger, 'E-money regulation in the EU' in Robert Pringle and Matthew Robinson (eds), *E-Money and Payment Systems Review* (Centralbanking 2002) 239–251.
[151] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[152] EMD2 rec 9.
[153] ibid art 1.
[154] ibid.
[155] ibid art 6; ibid art 3(5).
[156] ibid rec 5-6.
[157] ibid art 6(2); ibid art 12.
[158] ibid art 4; Rolf H. Weber, 'The European E-Money Directive: Background, Problems, and Prospects' (2000) 5 5 YB Int'l Fin & Econ L 293.

and required to invest funds in low-risk, highly liquid assets, with more stringent safeguarding standards.[159]

3.3.2. Regulatory Requirements for E-Money Institutions

Licensing rules under Article 3 of EMD2 mirror PSD2 prudential standards.[160] Specifically, Article 3(1) of EMD2 specifies that Articles 5 and 10 to 15 of the PSD shall apply to electronic money institutions mutatis mutandis.[161] In addition to capital requirements, EMD2 imposes strict rules on business plans, governance, and internal controls. EMIs must operate under principles of sound and prudent business management, including a requirement for two managers to approve legally binding activities (the 'four eyes principle').[162] They must also have robust internal control and accounting procedures to ensure a clear view of their financial situation at all times.[163] EMIs are prohibited from taking deposits or other repayable funds from the public and cannot grant credit from funds received for e-money issuance.[164]

By imposing a lower initial capital requirement and a balanced set of prudential rules, the directive allows EMIs to operate without the heavy regulatory burden of traditional banks. This is counterbalanced by significant restrictions on their activities, such as the prohibition on deposit-taking and credit-granting, and stringent safeguarding requirements for client funds.[165] This approach reflects a conscious effort to align the level of regulation with the specific risks associated with the issuance of electronic money.

Article 17(7), and Articles 18 to 25 of PSD2 also apply mutatis mutandis to EMIs.[166] EMIs are required to inform competent authorities in advance of any material changes to measures for safeguarding funds received in exchange for issuing e-money.[167] Rules for safeguarding user funds are similar in EM2 and PSD2. PIs and EMIs are mandated to safeguard user funds using one of two methods. They can either (i) segregate funds received by users in isolated accounts, protected even in the case of insolvency or creditor claims or (ii) cover the funds by using an insurance policy or comparable guarantee from an unrelated institution.[168]

EMIs are permitted to distribute and redeem electronic money through people acting on their behalf, although they are prohibited from using agents to do so.[169] They also face ongoing own fund requirements that are determined by the initial capital or a calculated amount based on their activities, whichever is higher.[170] For instance, the calculation used for e-money issuance requires own funds of at least 2% of the average outstanding electronic money.[171] In addition, competent authorities have the discretion to adjust these capital requirements by up to 20% based on the EMI's internal controls and risk management.[172]

---

[159] EMD2 art 7; Weber (n 158).
[160] EMD2 art 3.
[161] ibid art 3(1).
[162] Weber (n 158).
[163] ibid.
[164] EMD2 rec 4-9.
[165] Krueger, 'E-Money Regulation in the EU' (n 150).
[166] EMD2 art 3(1).
[167] ibid.
[168] International Monetary Fund, Monetary and Capital Markets Department and Legal Department, 'E-Money: Prudential Supervision, Oversight, and User Protection' (DP/2021/027, 2021).
[169] EMD2 art 3(4-5).
[170] ibid art 5.
[171] ibid.
[172] ibid art 5(5).

3.3.3. Rights, Obligations, and Consumer Protection

The legal framework under EMD2 establishes clear rights and obligations for EMIs and electronic money holders, fundamentally aiming to ensure consumer confidence and the integrity of electronic money services. A key focus of these obligations is the right to redeem e-money at par value.[173] Member States are mandated to ensure that EMIs issue electronic money at par value upon receipt of funds and, crucially, that upon an electronic money holder's request, the monetary value of the e-money held is redeemed at any moment and at par value.[174] This means there should be no possibility of agreeing to a minimum threshold for redemption. Instead, redemption should typically be granted free of charge.[175] However, the contract between the EMI and the electronic money holder may stipulate a redemption fee in specific circumstances: if redemption is requested before contract termination, if the contract has a termination date and the holder ends it prematurely, or if redemption is requested more than one year after contract termination.[176] These are some circumstances in which redemption fees may be acceptable. Any such fee, however, must be proportionate to the actual costs incurred by the EMI.[177] It is important to note that for non-consumer parties accepting e-money, their redemption rights are subject to their specific contractual agreement with the EMI.[178]

A distinct obligation imposed on EMIs by EMD2, as specifically articulated in Article 12, is the prohibition on interest-bearing balances.[179] Member States are required to prohibit the granting of interest or any other benefit that is directly related to the length of time an electronic money holder retains the electronic money.[180] This measure reinforces the distinction between electronic money and deposits, wherein electronic money is viewed as an electronic substitute for coins and banknotes, intended for payments rather than as a means of saving.[181]

Considering its focus on consumer protection and regulatory oversight, EMD2 integrates several recordkeeping and user transparency rules.[182] EMIs are required to maintain sound administrative and accounting procedures and internal control mechanisms to allow for a review of their financial situation.[183] Furthermore, they must report annually on their average outstanding electronic money.[184] For broader user transparency and consumer protection, EMD2 leverages the framework established by PSD2. It states that other relevant PSD provisions, specifically those related to out-of-court complaint and redress procedures, apply mutatis mutandis to EMIs.[185] It also requires that contracts clearly state redemption conditions and associated fees.[186] These transparency rules aim to provide consumers with the information necessary to make informed decisions and to have avenues for recourse.

3.4. The Upcoming Regulatory Shift: PSD III and the Payment Services Regulation

[173] Weber (n 158).
[174] EMD2 art 11.
[175] ibid rec 18.
[176] ibid art 11(4).
[177] ibid.
[178] ibid art 11(7).
[179] ibid art 12.
[180] ibid.
[181] ibid rec 13.
[182] Weber (n 158).
[183] ibid.
[184] EMD2 art 9(5)(b).
[185] ibid art 13.
[186] EMD2 art 11(3).

The European Union's new "Payment Services Package" was proposed by the European Commission in 2023 and was designed to further modernise and adapt legislative measures to the digital finance landscape.[187] It is comprised of two interrelated instruments: a Revised Payment Services Directive ("PSD III") and a new Payment Services Regulation ("PSR").[188] This updated framework aims to address issues raised with PSD2 after a comprehensive review of its impact undertaken in 2022.[189] This assessment identified four core issues: first, consumers remain at risk of fraud and lack confidence in digital payments; second, the open banking sector, covering account information and payment initiation services, functions imperfectly and providers face obstacles in offering services; third, supervisory powers and obligations are not harmonized across the EU, resulting in fragmented implementation and potentially forum shopping; and finally, there remains an unlevel playing field between traditional banks and non-bank PSPs (such as PIs and EMIs), notably regarding access to key payment systems and bank accounts.[190] Thus, this new approach aims both to strengthen security and user protection, and improve regulatory consistency, competition, and innovation across the EU payments market.[191]

One major structural change under PSD3 is its merger of EMD2 and PSD2, effectively repealing the former and placing both electronic money and payment institutions under the same regime.[192] Under this system, EMIs will be integrated and licensed as a sub-category of PIs, requiring them to comply with a single set of rules concerning licensing, prudential supervision, and market conduct.[193] A major element of PSD3 aims to address the unlevel playing field between banks and non-bank PSPs. As such, it grants PIs and EMIs the possibility of direct participation and access to all payment systems.[194]

While PSD3 focuses on simplifying the regulatory structure for PIs and EMIs, the Proposal for the Payment Services Regulation (PSR) contains the majority of conduct rules governing the day-to-day provision of payment and e-money services. In line with the objective of reducing fraud risks and enhancing SCA, the PSR improves SCA requirements and accessibility by mandating PSPs offer means of support for vulnerable users (e.g. persons with disabilities or older persons) in identifying threats.[195]

To further enhance the Open Banking framework, the PSR requires Account Servicing PSPs to implement a dedicated data access interface (API) for AISPs and PISPs while removing the obligation for most ASPSPs to maintain a permanent "fallback" interface.[196] ASPSPs must also provide permissions dashboards that allow users to monitor, manage, and withdraw previously granted data

[187] Issam Hallak, 'Payment Services Framework' (EPRS | European Parliamentary Research Service Briefing PE 775.891, 2025).
[188] ibid.
[189] Ciro Gennaro Corvese, 'Prudential Requirements for Payment Institutions: A European Union Perspective in View of PSD3' (2024) 13 Law and Economics Yearly Review 125.
[190] Hallak (n 187); European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010' (Proposal for a Regulation) COM(2023) 367 final (PSR Proposal).
[191] Jan Skrabka, 'Modernising Payment Services and Enhancing Open Banking: A Comparison of Recent EU Proposals of Payment Services Directive 3 (PSD3) and Payment Services Regulation (PSR) with Current PSD2 (2024)' (15th Law in Business of Selected Member States of the European Union conference, Prague, March 2024).
[192] Hallak (n 187).
[193] ibid.
[194] Skrabka (n 191).
[195] PSR Proposal (n 190) art 84.
[196] ibid art 35.

access permissions.[197] The proposal explicitly prohibits ASPSPs to create barriers to open banking services, providing a list of practices that may restrict fair access or hinder functionality.[198]

The legislative process for PSD3 and the PSR is still underway, with their adoption and implementation expected over the course of 2026.[199] As such, their full impact will only be observable after their entry into force and subsequent transpositions across Member States. Nevertheless, it is likely that this combined package will improve harmonisation in the EU payments market, as it directly tackles key discrepancies between the current legislative instruments. It is also expected to enhance customer protection through the stronger fraud prevention and open banking measures and in doing so, fostering further innovation, albeit it may simultaneously place additional regulatory burdens on existing market participants through the new licensing obligations.

[197] ibid art 43.
[198] ibid art 44.
[199] Skrabka (n 191).

Chapter IV: Compliance Environment: AMLD, GDPR, and DORA

4.1. Anti-Money Laundering and Know-Your-Customer requirements

The EU has developed a comprehensive legal framework for Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) to protect its financial system.[200] This framework is largely influenced by the recommendations of the Financial Action Task Force (FATF) and has evolved through a series of Anti-Money Laundering Directives (AMLDs), with the Fifth Anti-Money Laundering Directive (5AMLD), which serves as an amendment to the 4AMLD, specifically addressing potential threats from fintech.

The FATF has served as the global body setting the standards for AML/CFT since its establishment in 1989.[201] Its Forty Recommendations, first issued in 1990 but revised multiple times thereafter, cover AML/CFT policies, criminalisation of ML and TF, preventive measures, transparency and beneficial ownership, powers of competent authorities, and international cooperation.[202] Countries found to have strategic deficiencies risk inclusion on the FATF "grey" or "black" lists, which may trigger enhanced due diligence or restrictions on cross-border financial transactions.[203] Under the FATF mandated risk-based approach (RBA), countries and institutions must identify, assess, and mitigate ML/TF risks in a proportionate manner, allowing adaptation to local contexts and thus leaving some room for some national discretion.[204]

The EU has embedded this flexibility within its AMLDs, requiring Member States and obliged entities to apply enhanced due diligence in higher-risk cases and simplified measures where risks are demonstrably lower.[205] The EU's AMLDs largely operationalise FATF Recommendations within the EU legal order. Each successive directive has reflected FATF updates.[206] For instance, the adoption of the risk-based approach in 3AMLD and of beneficial ownership registries in the 4AMLD mirrored the 2003 and 2012 Recommendations, respectively. In some cases, the EU's AMLDs have preceded FATF standards, notably the inclusion of Virtual Asset Service Providers in the recently adopted 6AMLD and Anti-Money Laundering Regulation (AMLR) was then followed by the FATF update which clarified that its standards also apply to these providers.[207]

In 2024, the European Union introduced an updated AML/CFT Package which introduced the AMLR, moving away from the previous system under which rules were exclusively directive-based.[208] This package included 6AMLD, however, this Directive primarily sets out the necessary institutional framework and mechanisms to be put in place by Member States. The operational rules that were previously contained within the Fourth/Fifth AMLD (such as customer due diligence, internal controls, and reporting obligations) are now instead covered by the AMLR, which will begin to apply in July of 2027.[209] This means that the current 4AMLD/5AMLD framework in place will effectively be repealed

[200] 5AMLD rec 50.
[201] Gary W Sutton, 'The New FATF Standards' (2012) 4 Geo. Mason J. Int'l Com. L. 68.
[202] ibid; Kathryn Gardner, 'Fighting Terrorism the FATF Way' (2007) 13 Global Governance 325.
[203] Sutton (n 201).
[204] Financial Action Task Force (2012-2025), 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations)' (Financial Action Task Force 2012).
[205] 6AMLD art 8(4)(a).
[206] Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (2016) 23 Maastricht Journal of European and Comparative Law 261.
[207] Financial Action Task Force, 'Status of Implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity' (2024).
[208] 6AMLD rec 4.
[209] AMLR art 90.

by that date.[210] Additionally, the new framework establishes the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), a body tasked primarily with preventing ML/TF, assessing cross-border risks, and ensuring supervision and information-sharing between Financial Intelligence Units.[211]

The scope of entities obliged to comply with the AMLD has expanded considerably over time. The First AMLD initially was directed at banks, setting out Know-Your-Customer (KYC) and Customer Due Diligence (CDD) standards.[212] KYC refers to the mechanisms and processes designed to verify customer identity within the financial ecosystem, with the objective of preventing financial crimes such as identity theft, fraud, money laundering, and terrorist financing.[213] Over successive AMLDs, the scope expanded to include all financial firms, now also including fintechs as 'obliged entities' since 5AMLD.[214]

For fintechs, these obligations translate into a demanding set of operational requirements they must adhere to prevent financial crime.[215] These include CDD measures, including the identification and verification of customer identity using data, documents, or other information gathered from reliable and independent sources.[216] Such identification can be conducted electronically or through other secure identification processes approved by national authorities.[217] As mentioned above, obliged entities must also acquire and maintain accurate and adequate information on the beneficial owner (UBO) in a transaction.[218] The ultimate business owner is the natural person who ultimately controls or manages a customer, often through shareholding.[219] This is particularly relevant for customers registered as legal persons, such as corporations. Entities in charge of central registers must identify these owners to prevent potential illicit activity from hiding behind shell companies or other individuals.[220]

CDD is characterised as an ongoing process. Fintechs must continuously monitor transactions and customer behaviour to flag unusual patterns.[221] This involves both automated systems and manual reviews to detect suspicious activity.[222] Advanced technology or algorithms can be used during this process, in particular with identifying patterns indicative of money laundering, such as significantly large transactions, constant movement of funds, or transactions inconsistent with the customer's profile.[223]

Fintechs must apply the risk-based approach to their AML/CFT measures, as mandated initially by 3AMLD.[224] This means that the intensity of the CDD measures they have in place must be appropriate

[210] 6AMLD art 77.
[211] Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (Text with EEA relevance) [2024] OJ L2024/1620 (AMLA) art 1.
[212] ComplyAdvantage, 'Guide to EU Anti-Money Laundering Directives (AMLD)' (7 November 2024).
[213] Vineela Komandla, 'Overcoming Compliance Challenges in Fintech Online Account Opening' (2017) 1 International Journal of Multidisciplinary and CurrentEducational Research (IJMCER) 1.
[214] ComplyAdvantage (n 212).
[215] AMLR art 1(a).
[216] ibid art 22(6).
[217] Komandla (n 213).
[218] AMLR art 20, art 63.
[219] ibid art 51; Mitsilegas and Vavoula (n 206).
[220] 6AMLD rec 31.
[221] Komandla (n 213).
[222] ibid.
[223] ibid.
[224] ComplyAdvantage (n 212).

and proportionate to identified risks. Each customer has a risk profile, and risk variables taken into account include the jurisdiction the customer is based in, their beneficial owner, and the type and the delivery channels used.[225] For higher-risk situations, such as cash-intensive businesses, private banking, or complex ownership structures, they must apply enhanced customer due diligence measures which look at ownership structures, product/sector risk, as well as geographical risk.[226] The 5AMLD amendment introduced mandatory enhanced due diligence on customers from high-risk third countries as identified by the Commission.[227]

Fintechs are obliged to report suspicious transactions.[228] Suspicious Activity Reports (SARs) must be filed with Financial Intelligence Units, which can then request additional information.[229] Regarding record-keeping, 5AMLD also introduced an obligation for obliged entities to maintain records of customer due diligence documents and customer and transaction information for an extendable period of five years after the end of a business relationship or after the date of a particular transaction.[230] While this may raise data protection concerns under the GDPR, AML is treated as a public interest exception, which may justify the retention of sensitive data past the usual standards for compliance purposes.[231]

Fintech-specific challenges arise particularly in the area of identity verification.[232] Independent data from 2025 has shown that around 1 in 20 verification attempts for financial entities are fraudulent.[233] Digital finance heightens the risk of impersonation due to the lack of face-to-face checks, as well as the ease with which multiple accounts can be created quickly, facilitating the laundering of large sums of illicit funds.[234] The EU has addressed these issues through the Digital Identity Framework (eIDAS 2.0) and the planned EU Digital Identity Wallet, both of which aim to strengthen secure digital identity verification and streamline remote onboarding.[235] Furthermore, some Member States have also encouraged innovation by adopting sandbox models, allowing firms to test AI-based monitoring and biometric KYC solutions in controlled environments.[236]

While safeguarding of user funds is primarily governed by PSD2 and EMD2, it intersects with AML compliance. As mentioned earlier, fintechs classified as payment or e-money institutions are required to either separate customer funds from their own operational resources or to provide insurance

[225] AMLR art 20(2).
[226] ibid.
[227] 5AMLD art 1(10)(a).
[228] Mitsilegas and Vavoula (n 206).
[229] 6AMLD art 19.
[230] 5AMLD art 1(25).
[231] 6AMLD rec 124.
[232] Komandla (n 213).
[233] Chris Hooper, 'Top Fraud Trends in Digital Banking for 2025 – and How to Stay One Step Ahead' (*Veriff Insights*, 30 July 2025) <www.veriff.com/fraud/learn/top-fraud-trends-in-digital-banking-for-2025-and-how-to-stay-one-step-ahead> accessed 28 August 2025.
[234] Alexandre Pinot, 'Fintech: Friend or Foe to Anti-Financial Crime?' (ACAMS Today, 3 June 2019*)* <www.acamstoday.org/fintech-friend-or-foe-to-anti-financial-crime> accessed 28 August 2025.
[235] See Cyber Risk GmbH, 'eIDAS 2.0 | Updates, Compliance, Training <www.european-digital-identity-regulation.com> accessed 28 August 2025; European Commission, 'EU Digital Identity Wallet' <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487738/EU+Digital+Identity+Wallet+Home> accessed 28 August 2025.
[236] Komandla (n 213); Ringe and Ruof (n 31).

guarantees.[237] This also ensures traceability of money flows, which is important for reducing the risk of commingling illicit and legitimate funds.[238]

Because AML regulation in the EU is largely derived from FATF standards, and currently implemented through directives rather than directly applicable regulations, national transposition has resulted in some regulatory divergence among Member States.[239] Fintechs have to deal with a web of complex regional regulatory rules and additional costs and restrictions on operating across borders.[240] The passporting principle also complicates supervision because the main activity may be operated in a different Member State than the one responsible for oversight.[241] These variations can lead to regulatory arbitrage and create AML vulnerabilities, with similar services being offered by companies with differing obligations.[242] The recent AML package has significantly addressed these issues.[243] Unlike previous Directives, the AMLR is directly applicable, which gives Member States less flexibility when it comes to transposition, thereby increasing legal certainty for fintechs in the industry in the future.

The AMLR places strict limits on which AML/CFT activities can be outsourced. Tasks involving the establishment of a business relationship or assessment of customer risk are prohibited from outsourcing, which will likely compel fintechs to strengthen internal controls and invest in compliance systems.[244] Traditional banks that partner with fintechs may also deal with amplified AML vulnerabilities as they now may process transactions or hold funds for customers they have not directly onboarded, thereby increasing their exposure to high-risk profiles.[245] As such, banks may treat fintechs as high-risk clients by default and often push for them to meet more stringent AML requirements.[246]

Finally, it is important to note that the evolving nature of financial crime and its responding regulatory requirements render compliance a resource-intensive process. Fintechs must invest in ongoing training, technological updates, and consistent refinement of their internal compliance mechanisms.[247] These costs can be straining for smaller firms and their ability to remain competitive.

4.2. ICT and Operational Resilience under DORA

The Digital Operational Resilience Act (DORA) is a comprehensive regulation that introduced a harmonised framework for managing Information and Communication Technology (ICT) risk and

[237] EMD2 art 7(1); PSD2 art 10.
[238] 6AMLD rec 58.
[239] Stanisław Tosza and Olivier Voordeckers, 'An Anti-Money Laundering Authority for the European Union: A New Center of Gravity in AML Enforcement' (2024) 25 ERA Forum 405.
[240] Komandla (n 213).
[241] Pinot (n 234).
[242] ibid.
[243] Tosza and Voordeckers (n 239); See also Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance) [2024] OJ L2024/1624 (AMLR).
[244] AMLR art 18(3)(c-d).
[245] Noah Solowiejczyk, Ryan J Strauss and Kevin Kirby, 'Bank-Fintech Partnerships Under Scrutiny: What Fintechs Need to Know About BSA/AML Expectations' (Fenwick Insights, 29 May 2025) <www.fenwick.com/insights/publications/fintech-bank-partnerships-under-scrutiny-what-fintechs-need-to-know-about-bsa-aml-expectations> accessed 28 August 2025.
[246] ibid.
[247] Komandla (n 213).

enhancing digital operational resilience within the financial sector.[248] This regulation was viewed as a crucial step toward addressing increased risks from digitalisation and interconnectedness.[249]

DORA applies to a broad range of entities, including fintechs. It specifically applies to payment institutions, account information service providers and electronic money institutions, as well as investment firms, crypto-asset providers, and issuers of certain tokens.[250] DORA also applies to ICT third-party service providers that offer digital/data services through ICT systems, such as cloud computing or data analytics services.[251] Thus, it does not just regulate fintechs directly, but also their core dependencies, and serves as another acknowledgement of the co-dependence between the financial sector and ICT services.

Under DORA, there are a few key areas of obligations for financial entities:

a) ICT Risk Management: Financial entities must implement an ICT risk-management framework, although, under Articles 5-15, smaller fintechs may be subject to a simplified regime, especially with regard to governance structure requirements, as per the proportionality principle.[252]
b) ICT-Related Incident Reporting: Firms must report major ICT-related incidents to national authorities and continuously engage with them until the root cause has been identified and resolved.[253]
c) Digital Operational Resilience Testing: Financial entities must establish and maintain a regular testing program to assess their preparedness for dealing with ICT risks. Certain firms with systemic importance are required to perform advanced testing, whereas microenterprises are exempt from this specific requirement due to a lack of available resources, in line with the previously mentioned proportionality principle.[254]
d) Third-Party ICT Risk Management: Third-party ICT risk management must form part of financial entities' overall ICT risk management mechanism. This involves maintaining a register of all relationships with third-party providers and conducting sufficient due diligence on them before entering into agreements.[255]
e) Information-Sharing Arrangements: DORA encourages information sharing on cyber threats within trusted communities to enhance digital operational resilience and defence capabilities. Any such arrangement must adhere to existing data protection and competition law rules.[256]

While DORA aims for harmonisation, firms can be burdened by the volume of requirements they are obliged to meet within tight implementation deadlines.[257] This applies to early-stage startups in particular, as they may struggle to allocate sufficient technological and financial resources or develop the necessary expertise to meet DORA's technical and operational demands.[258] Furthermore, the principle-based nature of the regulation can lead to ambiguity in implementation, requiring national

[248] Christopher P Buttigieg and Beatriz Brunelli Zimmermann, 'The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision' (2024) 25 ERA Forum 11.
[249] DORA rec 1.
[250] ibid art 2(1).
[251] ibid art 2(1)(u).
[252] ibid art 4(1), art 6.
[253] ibid art 19.
[254] ibid arts 25-26.
[255] ibid art 28.
[256] ibid art 45.
[257] Buttigieg and Zimmermann (n 248).
[258] Georgios Pavlidis, 'Europe in the Digital Age: Regulating Digital Finance without Suffocating Innovation' (2021) 13 Law, Innovation and Technology 464.

competent authorities to exercise some degree of supervisory discretion leading to inconsistencies between differing Member States.[259]

It's worth also noting the emphasis DORA puts on concentration risk. The regulation acknowledges the financial sector's reliance on a limited number of ICT third-party service providers, which raises red flags for systemic vulnerabilities.[260] If one of these providers suffers an incident, the whole system could be affected.[261] While fintechs are required to assess this ICT concentration risk at their entity level, the regulation does not impose strict usage caps or limitations.[262] The implication is that firms will continue to face challenges in diversifying, especially since there are limited alternatives to major cloud providers (e.g. AWS and Microsoft Azure together own half of the total cloud market share)[263], which in turn are designated critical ICT third-party service providers under Article 31.[264]

Despite the compliance challenges, DORA effectively addressed inconsistencies concerning digital operational resilience within the EU's framework, as well as created a stable foundation for the EU's work in digital finance and for allowing fintechs to scale across borders.

4.3. Data Protection under the General Data Protection Regulation

The General Data Protection Regulation (GDPR), which became binding on May 25, 2018, significantly impacts fintechs in the payment and e-money sectors. It is also applicable to companies outside of the EU, with its scope extending to any firm that operates from within the EU or that provides to EU customers.[265]

For fintechs, any data processing activity is prohibited unless it has a legal basis set out in the GDPR.[266] Most fintechs rely on two primary legal bases under Article 6 for their core operations: contractual necessity and legal obligation.[267] According to these rules, data processing is lawful if it is necessary for the performance of a contract which the data subject has agreed to, or if it is necessary for compliance with the legal obligation to which the controller (i.e. the firm) is subject.[268] For instance, financial firms often adopt biometric authentication systems, and, in doing so, they must have separate controls to protect this data.

The GDPR emphasises data minimisation, mandating that data should be limited to what is absolutely necessary for processing purposes.[269] This provision may, at times, conflict with other regulatory requirements, in particular with existing obligations under AML or PSD2 frameworks.[270] Both of these directives mandate the collection and retention of certain categories of personal data, often for extended periods.[271] While the GDPR allows for such processing when based on legal obligations, the

[259] Buttigieg and Zimmermann (n 248).
[260] DORA rec 30.
[261] ibid rec 3.
[262] ibid rec 67.
[263] See HG Insights, 'AWS Market Share 2025: Insights into the Buyer Landscape' (*HG Insights*, 2025) <https://hginsights.com/blog/aws-market-report-buyer-landscape> accessed 3 December 2025.
[264] DORA art 31.
[265] GDPR art 3.
[266] ibid art 6.
[267] Phoenix Strategy Group, 'GDPR Checklist for Fintech Startups' (5 July 2025) <https://www.phoenixstrategy.group/blog/gdpr-checklist-for-fintech-startups> accessed 3 December 2025.
[268] GDPR art 6(1)(b-c).
[269] ibid 5(1)(c).
[270] Valeria Ferrari, 'Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy' (2020) 6 European Data Protection Law Review 522.
[271] PSD2 art 21; 6AMLD art 10(20).

simultaneous requirements create areas of overlap that financial entities must reconcile, especially as fintechs use practices typically involving large volumes of data crossing multiple IT systems.[272]

The complexity of these relationships creates compliance challenges, especially as the regulation also stresses individual rights. Data subjects may demand access, rectification, erasure, restriction, or portability of their data.[273] Meeting these obligations can be technically and operationally complex for automated fintechs that operate across borders.[274] The right to erasure (also known as the "right to be forgotten")[275] has been especially problematic: while firms must delete data when it is no longer necessary to be processed, fintechs must also consider legal retention duties, such as the aforementioned five-year minimum record-keeping for customer due diligence under 5AMLD.[276] Emerging technologies like blockchain, which are often used for personal data, also complicate matters, since data recorded on a distributed ledger cannot easily be deleted.[277]

In the context of open banking under PSD2, Third-Party Providers may rely on explicit consent as the basis for their processing activities, rather than the performance of a contract or legal obligation basis. Under the GDPR, consent must be freely given, specific, informed, and unambiguous, signified by a clear affirmative action from the data subject.[278] However, the use of consent for certain purposes, such as "screen scraping" (a practice in which a user's account is accessed by scraping information from their online banking interface), has been questioned.[279] The GDPR explicitly prohibits conditioning the performance of a contract on consent to process personal data that is not necessary for the contract, which has pushed companies to seek alternative legal bases.[280] Fintechs can process personal data based on their legitimate interest, provided these interests are not overridden by the data subject's fundamental rights.[281] This includes processing for purposes of IT security, direct marketing, or internal administrative purposes.[282] Thus, fintechs have to carefully structure their data processing systems and determine the most appropriate legal basis for each processing activity. The result is some companies defaulting to over-collecting consents or drafting long, unreadable privacy notes, which in turn effectively undermine the GDPR's aim of transparency.[283]

Security and breach management are another pillar of the GDPR. Articles 32–34 oblige firms to implement "appropriate technical and organisational measures" (TOMs) to ensure a level of security

[272] See Dilja Helgadottir, 'The Interaction Between Directive 2015/2366 (EU) on Payment Services (PSD2) and Regulation (EU) 2016/679 on General Data Protection (GDPR) Concerning Third Party Players' (2019) 23 Trinity CL Rev 199; Pankaj Pathak and others, 'Assessment of Compliance of GDPR in IT Industry and Fintech' in Pradeep Kumar Singh and others (eds), *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security*, vol 421 (Springer Nature Singapore 2023).
[273] GDPR arts 15–20.
[274] Gregor Dorfleitner, Lars Hornuf and Julia Kreppmeier, 'Promise Not Fulfilled: FinTech, Data Privacy, and the GDPR' (2023) 33 Electronic Markets 33.
[275] GDPR art 17.
[276] Magdalena Brewczyńska and Eleni Kosta, 'From the Fight Against Money Laundering and Financing of Terrorism Towards the Fight for Fundamental Rights: Role of Data Protection' (2023) 2 Tilburg Law School Research Paper.
[277] Bibitayo Ebunlomo Abikoye and others, 'Regulatory Compliance and Efficiency in Financial Technologies: Challenges and Innovations' (2024) 23 World Journal of Advanced Research and Reviews 1830.
[278] GDPR art 4(11).
[279] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[280] Paul Voigt and Axel Von Dem Bussche, 'Material Requirements' in Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer Nature Switzerland 2024).
[281] GDPR art 6(1)(f).
[282] ibid rec 47.
[283] Dorfleitner, Hornuf and Kreppmeier (n 274).

appropriate to the risks involved in data processing.[284] These may include measures such as pseudonymisation, encryption, and resilience testing.[285] There is a general reporting duty for personal data breaches, and controllers have to notify the competent Supervisory Authority without undue delay, no later than 72 hours after becoming aware of the breach.[286] Data subjects must also be informed if the breach is likely to adversely affect their rights and freedoms.[287] These obligations may overlap with requirements in other regimes, such as DORA, for instance, in cases where an ICT incident involves personal data.[288] Fintechs must integrate these obligations across their systems to avoid fragmentation and higher compliance costs.

Fintechs utilising US-based cloud services or operating across EU borders must adhere to GDPR rules on cross-border data transfers.[289] Any transfer of personal data outside the EU must meet specific safeguards to guarantee an adequate level of protection. This is a two-step process: first, the processing must have a legal justification (e.g. consent or legitimate purpose), and second, the transfer must comply with conditions under Articles 44 et seq.[290] Without meeting these requirements, the transfer cannot proceed. A significant number of personal data transfers by controllers occur to outside processors, especially the U.S.[291] A key mechanism for facilitating these transfers is adequacy decisions by the European Commission, which recognise some third countries as "adequate" in their level of data protection.[292] However, there has been great uncertainty regarding transatlantic data transfers. The ECJ rulings in *Schrems I* and *Schrems II* invalidated successive EU-U.S. regimes (Safe Harbor and Privacy Shield, respectively) in response to insufficient safeguards against U.S. surveillance programmes.[293] Ongoing uncertainties have created regulatory risks for fintechs, especially those that aim to scale globally, as reliance on contested transfer mechanisms can expose them to compliance failures.

The GDPR underlies these obligations with a strict enforcement regime.[294] Violations of fundamental provisions (such as lawful processing, data subject rights, or "privacy-by-design" obligations) can result in fines up to either EUR 20 million or 4% of the entity's global annual turnover, whichever is higher.[295] These penalties have been said to potentially lead to a chilling effect of legal uncertainty, especially with vaguely defined terms such as "privacy by design", which leaves courts discretion to fill in the gaps.[296] Furthermore, the rules on automated decision-making (Article 22) prohibit purely automated profiling if it significantly affects individuals.[297] This can deter fintechs from experimenting with more advanced data-driven tools, such as machine learning for fraud detection, despite their potential benefits.

---

[284] GDPR arts 32-34.
[285] ibid art 32(1).
[286] ibid art 33(1).
[287] ibid art 34.
[288] Banking Stakeholder Group (BSG), European Banking Authority, 'BSG Own Initiative Paper on DORA: Main Challenges and Recommendations' (European Banking Authority 2023).
[289] Paul Voigt and Axel Von Dem Bussche, 'Scope of Application of the GDPR' in Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer Nature Switzerland 2024).
[290] GDPR art 44.
[291] Voigt and Von Dem Bussche, 'Scope of Application of the GDPR' (n 289).
[292] GDPR art 45.
[293] See Case C–362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650 (Schrems I); Case C-311/18 *Data Protection Commissioner v Facebo*ok Irela*nd Ltd and Schrems* [2020] ECLI:EU:C:2020:559 (Schrems II).
[294] Paul Voigt and Axel Von Dem Bussche, 'Organisational Requirements' in Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer Nature Switzerland 2024).
[295] GDPR art 83.
[296] Voigt and Von Dem Bussche, 'Organisational Requirements' (n 294).
[297] GDPR art 22.

Ultimately, the fear of non-compliance, the high fines associated with it, and the burden of comprehensively demonstrating sufficient safeguards could deter firms from implementing innovative, data-intensive practices in their operations. In fact, research suggests that it may be very difficult for financial entities to operate in an industry that is data-driven without significantly restricting business activities for GDPR compliance.[298] The core challenge for fintechs here is exploiting data to deliver innovative financial solutions while avoiding non-compliance sanctions from the GDPR framework.

[298] Dorfleitner, Hornuf and Kreppmeier (n 274).

Chapter V: The Combined Legal Effects of the EU Fintech Framework on Payment Service Operations and Innovation

5.1 Purpose and Method

The instruments discussed above have meticulously built the landscape for payment services and e-money users in the fintech space. While they may often be considered individually, the real-world influence on fintech operations, particularly on their innovative capacities, is shaped less by isolated provisions and more by the way these provisions interact with each other, both through overlapping scopes and potential contradictions. This chapter analyses the combined impact of these instruments on innovative capacity for these fintechs.

In practice, the operational environment for many firms is shaped by a compliance matrix consisting of different sets of rules. PSD2 and EMD2 are tightly interlined, with EMD2 functioning as lex specialis to PSD2 in the area of electronic money.[299] AMLDs impose mandatory identity verification and customer and transaction monitoring, which may conflict with the GDPR's data minimisation rights.[300] DORA harmonises ICT resilience requirements, but provisionally, it sometimes duplicates or overlaps standards set out in other regulations which creates uncretainity.[301]

Different measures reinforcing each other can create benefits, such as increased consumer trust, market access, and harmonisation. It can also lead to positive innovative spillovers and increased long-term resilience. However, frictions are apparent in cases of duplicative compliance obligations and legal uncertainties. While support initiatives exist to help fintechs manage and take advantage of complex compliance systems, smaller fintechs may not have the resources necessary to fully benefit from such support which in turn may hinder them from achieving their full innovative capacity. This chapter first identifies the positive effects arising from this framework, then examines the compliance burdens that may have innovation-limiting effects. Ultimately, it aims to answer the question: how do PSD2/EMD2, AMLDs, GDPR, and DORA interact to affect operational choices and innovation for payment-service fintechs?

5.2. Positive Legal Effects: Compliance as a Tool for Growth

While companies operating in the fintech space often perceive regulatory compliance as a significant burden, it could also prove to be beneficial if used strategically. In fact, a strong internal compliance mechanism can serve as a driver of innovation, with companies often generating new capabilities or products to efficiently meet regulatory requirements.

5.2.1. Data Access Mandated by Law

PSD2's "access to account" obligation requires payment service providers to provide authorised TPPs with customer account data, subject to customer consent.[302] This is not by itself a permissive innovation channel but serves as a mandatory legal restructuring of competition. In other words, by legally mandating interoperability, the EU created space for new payment services to develop responsive infrastructure and valuable solutions.

[299] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[300] Ferrari (n 279).
[301] Banking Stakeholder Group (BSG), European Banking Authority (n 288).
[302] PSD2 art 66.

In the fields of data aggregation and personal finance management in particular, PSD2's Open Banking principle has interacted with the GDPR, and in doing so, has stimulated product innovation.[303] PSD2 obliges banks to open up their APIs to third-party providers, but it is the GDPR which ensures this access is only possible under user consent and strict data protection rules. This dual requirement is what prevents fintechs from freely collecting and aggregating data. Instead, they were compelled to build services that not only aggregate account and transaction data but also do so while maintaining security and a high level of user control over what is being shared and how it is being used.[304] Furthermore, to justify the user's consent, fintechs had to offer tangible value to them.[305] Therefore, the strict compliance regime ultimately led to innovation in tools that help users understand and optimise their performance.

An example is the evolution of Stockholm-based platform Tink. Launched in 2012, it initially focused on personal finance management (PFM) for end-users.[306] Its primary function was to aggregate users' accounts and provide spending insights through screen scraping methods which were often criticised for being unreliable and insecure.[307] After the adoption of the GDPR and PSD2, Tink shifted its model to one primarily B2B-focused.[308] It specifically leveraged PSD2's granting of API access and the GDPR's explicit consent requirements to transition into a scalable business model.[309] Considering that other organisations were facing similar challenges in obtaining financial data from banks, Tink rebuilt its infrastructure and developed a single API that allows other fintechs to access aggregated data and build personalised financial management tools.[310] In other words, mandatory compliance under PSD2 compelled it to replace its existing vulnerable technical model with more efficient and innovative infrastructure.

5.2.2. Compliance-Driven Technological Innovation

The effect of the AMLDs and DORA has been to raise compliance costs for fintechs, but also to stimulate compliance-driven innovation. The FATF Recommendations and the AMLDs require strict customer due diligence and ongoing transaction monitoring, whereas DORA, for its part, sets standards for incident reporting and operational resilience. In order to comply with both, fintechs have to embed strong monitoring and security mechanisms into their business models from the moment of foundation.[311]

A key positive spillover effect is the development of "RegTech" solutions.[312] These are technologies implemented to support businesses, including financial services, in meeting regulatory obligations.[313] Initially designed for in-house compliance (e.g. AI-driven KYC verification, automated incident reporting), they have now become standalone products.[314] For instance, UK company

[303] Federico Ferretti, 'Open Banking: Gordian Legal Knots in the Uncomfortable Cohabitation between the PSD2 and the GDPR' (2022) 30 European Review of Private Law 73.
[304] ibid.
[305] ibid.
[306] William Girling, 'Fintech Timeline: Tink's Acquisition by Payments Leader Visa' (FinTech Magazine, 24 June 2021) <https://fintechmagazine.com/digital-payments/fintech-timeline-tinks-acquisition-payments-leader-visa> accessed 1 September 2025.
[307] ibid.
[308] ibid.
[309] Tink, 'How Using Data Will Help You Win More Customers and Earn More Revenue' (3 July 2018) <https://tink.com/blog/open-banking/open-api/> accessed 1 September 2025.
[310] Girling (n 306).
[311] Aadit Sharma and others, 'Governance Challenges in Cross-Border Fintech Operations: Policy, Compliance, and Cyber Risk Management in the Digital Age' (2021) 4 Iconic Research and Engineering Journals 278.
[312] Bibitayo Ebunlomo Abikoye and others (n 277).
[313] ibid.
[314] ibid.

ComplyAdvantage developed AI-powered KYC and transaction monitoring to help fintechs comply with AMLD and now sells these tools globally.[315] DORA has also catalysed a new RegTech niche focused on ICT resilience and third-party risk. Netherlands-based 3rdRisk and Lithuania's CyberUpgrade both explicitly advertise compliance with DORA standards, offering vendor due diligence, monitoring, incident reporting and compliance self-assessment tools.[316]

Thus, the legal framework has not only constrained firms, but it has also led to the creation of new markets revolving around meeting its requirements. These developments have resulted in higher security for end-users/customers, as well as a scalable operational infrastructure that has inarguably improved trust and reliability across the sector.

5.2.3. Trust through Compliance

Under EMD2, e-money providers are required to safeguard customer funds by keeping them in segregated accounts or by covering them with insurance or with a comparable guarantee[317]. This protects customer funds even if the provider fails.[318] Alongside this, the AMLDs require customer due diligence and transaction monitoring. Taken together, these measures mean that fintechs must operate in a way that ensures both the security and integrity of financial flows. This compliance architecture has had an important impact: it has effectively reduced the perceived risk for customers using payment service and electronic money fintechs.[319] Service organisations, including financial institutions, have higher perceptions of predictability and trust from users if they demonstrate strong security mechanisms, leading to increased customer loyalty[320].

Trust is a precondition for numerous fintech activities: the adoption of digital wallets, cross-border payment platforms, as well as some aspects of "buy now, pay later" (BNPL) arrangements. If users know that their money is safeguarded and that the provider is subject to strict anti-money laundering and anti-fraud oversight, customers are more willing to use and adopt these products.[321] In other words, regulatory compliance serves as almost a substitute for (or a supplement to) brand reputation in emerging markets, allowing younger fintechs to compete with established credit institutions.[322]

This has served as another indirect channel for development. Providers such as Revolut expanded their cross-border services across Europe because of PSD2 passporting, but this growth was conditioned on compliance with strict safeguarding requirements.[323] These rules are meant to enhance consumer protection, but, in turn, they also build trust in digital finance services, making consumers more willing to use them when the risk is legally mitigated.[324]

---

[315] Lenar Valk, 'ComplyAdvantage Alternatives & Competitors' (Salv, 2023) <https://salv.com/blog/complyadvantage-alternatives-competitors/> accessed 1 September 2025.
[316] See 3rdRisk, 'DORA | Digital Operational Resilience Act' (3rdRisk) <www.3rdrisk.com/framework/dora> accessed 1 September 2025; CyberUpgrade, 'DORA Regulation' (CyberUpgrade) <https://cyberupgrade.net/dora-regulation/> accessed 1 September 2025.
[317] EMD2 art 7.
[318] International Monetary Fund, Monetary and Capital Markets Department and Legal Department (n 168).
[319] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[320] Carole Driver and Robert Johnston, 'Understanding Service Customers: The Value of Hard and Soft Attributes' (2001) 4 Journal of Service Research 130.
[321] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[322] Helgadottir (n 272).
[323] FinTech Review, 'Revolut Review: From Startup to Global Giant' (*FinTech Review*, 2 April 2025) <https://fintechreview.net/revolut-scaled-from-startup-to-global-fintech-giant/> accessed 1 September 2025.
[324] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).

5.2.4. Compliance-by-Design

The cumulative impact of EU regulatory policies has been particularly clear in the way fintechs now build their foundational technological infrastructure. In practice, a fintech registered as an EMI that also offers PSD2 services has to ensure at minimum the following: keep separate accounts for customer funds with daily automated reconciliation (EMD2), enforce Strong Customer Authentication (PSD2), operate data protection and retention services and document them through Impact Assessments (GDPR), run consistent KYC onboarding and real-time AML systems (AMLD), and maintain monitored infrastructure and vendor inventories (DORA). The only efficient response to the complexities presented is to build a unified framework, or "stack" of sorts, which is scalable, resilient, and comprehensive, into the architecture from the ground up, instead of treating them ad hoc.[325]

This compliance-by-design approach has also led to a positive ripple effect in some cases. Once a robust infrastructure exists, it can be reused and scaled to support new services.[326] In fact, by building such infrastructure, fintechs have inadvertently created a new business model, characterised by the provision of the infrastructure to others.[327] In particular, the Open Banking standard effectively led to the rise of Open Banking Platforms, such as the previously referenced Tink, as well as Truelayer, both of which provide the infrastructure necessary for fintechs to securely connect with banks' APIs, in virtue of PSD2.[328] Smaller fintechs can use these standardised connections without having to connect individually with each different bank, and without having to handle compliance with PSD2's security and consent rules.

This has created an environment where compliance pressures have indirectly supported future innovations, as these platforms, whether outsourced or created internally, allow fintechs to launch new services without having to re-engineer compliance from scratch. This is one of the reasons why European fintechs were able to proliferate after 2018, as they could build on top of a shared infrastructure layer created initially in response to regulation.[329]

5.3. Cumulative Compliance Burden

It is evident that PSD2, EMD2, DORA, and the GDPR and AMLDs pursue legitimate goals, and, at some level, facilitate innovative ecosystems among fintechs. However, challenges arise from their cumulative effects. While single regulations may be manageable, fintechs do not face them in isolation. Overlaps between different instruments create compound burdens for providers, which, together with high compliance costs, may restrict innovation in the sector. To analyse these burdens, three lenses are considered: a) overlapping and conflicting provisions; b) capital strains of compliance; and c) constraints on scaling and cross-border growth. The following sections will analyse these in more detail.

5.3.1. Overlapping and Conflicting Provisions

5.3.1.1. Data-access vs. Data-protection (PSD2 and the GDPR)

Fintechs operating in the EU face a structural challenge in reconciling certain elements of PSD2 with GDPR requirements. A fintech may be permitted to access data under PSD2, while inadvertently violating the GDPR if the scope of consent or subsequent data usage exceeds the GDPR's strict

[325] Sharma and others (n 311).
[326] ibid.
[327] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[328] ibid.
[329] ibid.

requirements.[330] PSD2 is explicitly designed to increase access to customer payment data by obliging banks to provide access to Third-Party Providers with the user's "explicit consent".[331] By contrast, the GDPR is designed to restrict access to personal data to protect users, mandating that any processing adheres to principles like data minimisation and purpose limitation. PSD2 stipulates that data processing should occur in accordance with the GDPR[332]. However, tension can arise if the "explicit consent" under PSD2 is not granular enough or if the fintech's subsequent retention or sharing of data goes beyond the original specified purpose without new consent compliant with the GDPR. In other words, even if a fintech accesses data under PSD2, its handling of that data must continuously meet the higher standards of the GDPR. The main points of conflict and compliance burdens for fintechs revolve around three key areas: consent, purpose limitation, and the handling of sensitive and third-party data.

As mentioned, PSD2 requires a user's "explicit consent" for a TPP to access transaction data. The European Data Protection Board (EDPB) interprets this as a form of contractual consent.[333] This is different from the GDPR's definition of consent as a legal basis for processing data that must be freely given, specific, informed, and unambiguous, while further differentiating between this general standard and "explicit consent", a higher standard required for specific categories of sensitive data (such as health information), that goes beyond a mere contractual agreement.[334] This discrepancy between PSD2's contractual "explicit consent" and the GDPR's legal basis "consent" (especially for sensitive data) is not very clear-cut in practice, which can lead to confusion for fintechs and require them to implement multiple layers of consent.[335]

Regarding purpose limitations, the GDPR mandates that data can only be collected for specified, explicit, and legitimate purposes.[336] The ambiguity lies in whether a fintech could reuse data collected under PSD2 for other services. For instance, PISPs are strictly limited under PSD2 and cannot use, access, or store data for any purpose other than providing a payment initiation service.[337] For AISPs, the rules are not as clear. PSD2 mandates that data use be in accordance with data protection rules, but it is unclear whether this allows AISPs to reuse data for other purposes, such as financial analytics or advice, even if they get new consent.[338] Since many TPPs rely on collected data for associated services, strict interpretations here could create an unfair competitive disadvantage.[339]

Even if financial status itself isn't considered sensitive, specific transactions within a payment account may reveal sensitive personal data, such as medical expenses.[340] If this data is processed, the GDPR's stricter explicit consent is required, and a simple contractual agreement is insufficient. Since it's often difficult to separate sensitive from non-sensitive data within one account, this poses another potential challenge.[341] Furthermore, fintechs accessing payment accounts also acquire data on "silent parties" (e.g., payees or payers in a user's transaction history) who have no direct relationship with the fintech.[342] Banks are legally obliged to provide this data under PSD2 and the Regulatory Technical Standards on

[330] Helgadottir (n 272).
[331] PSD2 art 65.
[332] ibid 94.
[333] Fiona Maclean and others, 'Consent under PSD2 and the GDPR: Squaring the Circle' [2021] Butterworths Journal of International Banking and Financial Law.
[334] GDPR art 4(11), art 9.
[335] Helgadottir (n 272).
[336] GDPR art 5(1)(b).
[337] PSD2 art 66(3)(g).
[338] Maclean and others (n 333).
[339] ibid.
[340] Ferretti (n 303).
[341] ibid.
[342] ibid.

SCA, but the legal basis to process it is contentious.[343] The EDPB suggests "legitimate interest" as a basis, but this requires a balancing test to ensure that the legitimate interest in question overrides the silent party's fundamental rights.[344]

This effectively forces fintechs into a trade-off in which they can either constrain their use of customer data, potentially in a way that limits product development, or risk regulatory enforcement. Thus, with respect to the relationship between data and sharing and data privacy under PSD2/GDPR, the concern is whether innovation driven by mandated data access can be maintained under equally mandated protection.

5.3.1.2. Safeguarding vs. Traceability (AMLD (5th/6th) and EMD2/PSD2)

Safeguarding of funds and traceability of funds are both key pillars of the EU financial framework. However, their core objectives and operational demands can lead to tensions which pose a regulatory burden for fintechs.[345] Safeguarding of funds, as outlined in both PSD2 and EMD2, prioritises the protection of client funds against the insolvency of the financial institution. It ensures that client money is pooled in separate accounts and is easily reconcilable.[346] This approach promotes a simple operational model focused on segregation and oversight. On the other hand, traceability in the AML framework aims to prevent financial crime by focusing on the flow of funds.[347] This requires continuous monitoring, granular data collection, and the ability to link transactions to beneficial owners across borders and demands complex infrastructure capable of such data analysis.[348]

The different objectives of traceability and safeguarding present a potential contradiction in how fintechs must design their foundational technological infrastructure. In order to comply with safeguarding, fintechs have to build a simple, "pool-based" system (where segregated funds are 'pooled' and protected).[349] In order to comply with traceability standards, they have to build a complex layered system where all transaction flows are tracked. As a result of this relationship, fintechs often have to either maintain dual systems or attempt a hybrid structure, which is costly, often insufficient, and resource-intensive.[350] This is particularly burdensome for smaller firms, where such duplication of requirements can set a substantial barrier to entry.[351] It should be emphasized that while these obligations do not directly contradict each-other, their cumulative effect creates a dual pressure that is felt more heavily by smaller firms.

This is further compounded by how safeguarding of user funds is implemented under PSD2 and EMD2. While safeguarding is emphasised by both Directives, PSD2's Strong Customer Authentication mandate is linked to a liability regime particularly relevant for EMIs. If SCA is not properly applied, the payer shall not bear any financial losses unless they acted fraudulently.[352] This places the financial

[343] PSD2 art 67(3)(b), Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance.) [2018] OJ L 69 art 36(1)(a); Ferretti (n 303).
[344] Ferretti (n 303).
[345] Ferrari (n 279).
[346] PSD2 art 10(1); EMD2 art 7(1).
[347] Jonida Milaj and Carolin Kaiser, 'Retention of Data in the New Anti-Money Laundering Directive—"Need to Know" versus "Nice to Know"' (2017) 7 International Data Privacy Law 115.
[348] ibid.
[349] International Monetary Fund, Monetary and Capital Markets Department and Legal Department (n 168).
[350] Sharma and others (n 311).
[351] ibid.
[352] PSD2 art 74(2).

responsibility for refunds or chargebacks solely on the PSP (EMI or PI), creating contingent liabilities it must cover with its own resources.[353]

This leads to a two-fold rigidity in capital management. On one side, EMD2 obliges EMIs to segregate client funds, which limits their liquidity base. On the other hand, PSD2 increases the potential for unexpected outflows through refund obligations if SCA implementation is not up to par. Unlike banks, which may use client deposits to finance lending and investment activities, EMIs cannot re-purpose client funds and must maintain sufficient additional own funds to cover regulatory requirements as well as liability exposure, effectively forcing them to over-capitalise.[354] This immobilisation of capital limits the operational flexibility and investment capacity that an EMI has that could otherwise support market expansion and innovation.[355] It is evident that even in the absence of a direct conflict, overlapping frameworks can still create systemic disadvantages that disproportionately affect payment service providers compared to traditional credit institutions. These disadvantages have pushed advocacy for legislative consolidation of EMD2 and PSD2. This consolidation is addressed in the proposed PSR, with the aim the reduction of regulatory arbitrage and increased clarity for fintechs.[356] That said some have argued that e-money and payments are fundamentally too different to be subject to the same rules, and PSD2 and EMD2 should stay separate but harmonised.[357]

5.3.1.3. Operational Resilience vs. Agility and the Right to be Forgotten (DORA and PSD2/GDPR)

PSD2 aims to promote competition and innovation in the payment services market. Enabling TPPs to access account data is meant to foster agile, user-friendly, and innovative payment solutions[358]. Compliance with PSD2, therefore, presupposes flexible ICT systems capable of quick adaptation and reiteration. However, DORA's framework for ICT risk management requires fintechs to maintain robust, well-documented policies with regard to prevention, detection, and recovery of ICT systems and data.[359] ICT change management must follow formalised, risk-based procedures, where every modification is recorded, tested, approved, and verified.[360] These requirements promote resilience but can directly clash with the agility imperative of PSD2.

One area of friction concerned the handling of major operational incidents, considering that DORA extended ICT risk management obligations already present in PSD2.[361] Incidents that were reportable under PSD2 (Article 96), overlapped with DORA's more comprehensive incident-reporting framework, effectively requiring fintechs to comply with both frameworks simultaneously.[362] This issue was resolved by the 2022 Amending Directive which repealed the requirement for payment service providers to report incidents under PSD2, so that incidents are now reportable exclusively under DORA.[363]

---

[353] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[354] EMD2 art 6(2), art 7(1) art 5.
[355] International Monetary Fund, Monetary and Capital Markets Department and Legal Department (n 170).
[356] Shane Kelleher, Louise McNabola and John O'Connor, 'The Future of EU Payment Services Regulation – PSD3 and PSR' (*William Fry*, 2023) <www.williamfry.com/knowledge/the-future-of-eu-payment-services-regulation-psd3-and-psr> accessed 1 September 2025.
[357] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[358] Helgadottir (n 272).
[359] DORA arts 6–12.
[360] ibid art 9(4)(e).
[361] Banking Stakeholder Group (BSG), European Banking Authority (n 288).
[362] PSD2 art 96; DORA art 19.
[363] Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (Text with EEA relevance) [2022] OJ L 333 (Amending Directive) rec 7.

The GDPR adds another layer of complexity by granting individuals strong rights over their personal data, including the right to erasure ("right to be forgotten").[364] While this principle is essential for data protection, it may be at odds with DORA's requirements for data integrity, recovery, and backups.[365] Long-term storage of data, which is necessary for operational resilience and post-incident analysis under DORA, risks including information that GDPR would otherwise require to be deleted.[366] Additionally, an ICT incident may trigger notification requirements under both DORA (for operational risks) and the GDPR (for data breaches).[367] Given that many major ICT-related incidents inherently involve the compromise of customer data, entities are often required to comply with both sets of reporting procedures, leading to a complex dual reporting regime under careful coordination.[368] There is an expressed need for greater cooperation among supervisory authorities and an integrated reporting process to streamline these obligations.[369]

Cumulatively, these frictions create a duplicative and resource-intensive environment, for which fintechs must build ICT infrastructures that are simultaneously agile (to meet PSD2 requirements), heavily documented (to meet DORA requirements), and flexible enough to reconcile data protection obligations under the GDPR. Building this infrastructure is likely to increase compliance costs, slow down service iteration, and generally pose a larger barrier to entry for smaller firms, thereby undermining the EU's objective of fostering a competitive digital finance sector.

5.3.2. Capital Strains of Compliance

The EU regulatory architecture on fintechs has created a resource-intensive compliance landscape, arguably also structurally constraining innovation. As shown, they often impose parallel obligations, which lead to higher compliance costs, as well as a reallocation of resources from product development or experimentation.

First, data governance rules are scattered within the existing legal framework.[370] The AML framework requires fintechs to collect, verify, and keep extensive customer data for extended periods, inducing them to embed long-term storage into their compliance models.[371] By contrast, the GDPR mandates limited data retention.[372] DORA adds on to this by layering additional ICT incident-reporting obligations, which overlap with the GDPR's breach notification rules (and PSD2's operational incident reporting prior to the 2022 amendment).[373] This regulatory layering forces firms to build multiple compliance infrastructures, which consumes their resources.

Second, outsourcing and vendor controls under DORA, GDPR, and EMD2 create burdens that primarily hit smaller fintechs. DORA requires fintechs to catalogue all service-provider relationships, whereas the GDPR imposes strict requirements on data controllers that outsource processors.[374] EMD2's

[364] GDPR art 17.
[365] Bibitayo Ebunlomo Abikoye and others (n 277).
[366] ibid; Iwona Karasek-Wojciechowicz, 'Reconciliation of Anti-Money Laundering Instruments and European Data Protection Requirements in Permissionless Blockchain Spaces' (2021) 7 Journal of Cybersecurity.
[367] American Chamber of Commerce to the European Union, 'Our Position: Digital Operational Resilience Act (DORA)' (2021) <http://amchameu.eu/system/files/position_papers/digital_operational_resilience_act.pdf> accessed 3 September 2025.
[368] Helgadottir (n 272).
[369] Banking Stakeholder Group (BSG), European Banking Authority (n 288).
[370] Sharma and others (n 311).
[371] 5AMLD, art 1(25); AMLR art 77
[372] GDPR art 5(1).
[373] GDPR art 33; DORA art 19; PSD2 art 96.
[374] GDPR art 28(1); DORA art 28(3).

safeguarding arrangements for customer funds also frequently involve outsourcing to credit institutions or insurance providers.[375] These overlaps lead fintechs to fragmented outsourcing arrangements, and for startups whose business models revolve around partnerships with cloud and banking service providers, such compliance structures can undermine scalability and their market entry timeline.[376]

Third, compliance obligations necessitate costly expertise. Fintechs must, simultaneously, work with AML compliance officers, GDPR data protection officers, ICT specialists, and other legal staff. This leads to substantial costs, but may also drive away capital from innovation-oriented initiatives. While already-established financial institutions can absorb these costs, they serve as a barrier to entry for smaller players, in turn intensifying market concentration and restricting consumer choice.[377]

Beyond these structural overlaps, which can be said to drive investment away from innovation, the total level of direct compliance costs is excessive for smaller players. In fact, implementing PSD2 was very costly and complicated even for incumbent banks with more resources.[378] For smaller firms, the PSD2 operational and security requirements represent a disproportionate burden. Similarly, heavy entry costs imposed in EMD2 (initial capital requirement of €350,000 plus ongoing capital adequacy obligations) make e-money issuance costly from the get-go.[379] Then, fintechs also have to deal with costs pertaining to data handling, cybersecurity measures, AML controls, and risk management, thus having to continuously invest in somewhat convoluted compliance structures. With AML in particular, the FATF/AMLD requirement of conducting detailed risk assessments before launching any new product or technology inherently demands continuous human and technological resources.

Finally, the dynamic and fragmented nature of EU regulation adds to the compliance strain. Frequent updates, evolving technical standards, and divergent national interpretations require constant adaptation of compliance systems.[380] For instance, the initial absence of clear API standards under PSD2 led to fragmentation, interoperability problems, and significant compliance burdens for Third-Party Providers.[381] These uncertainties translate into sunk costs and legal risk, reducing the capital that fintechs can dedicate to innovation.

In short, compliance costs in the EU fintech space, beyond being representative of operational frictions within the framework, can also manifest as structural barriers to entry and expansion. This is especially emphasised in early-stage firms, where the combination of high fixed costs and overlapping obligations diverts scarce capital from product development, thereby reinforcing advantages for larger, established banks.

5.3.3. Constraints on Scaling and Cross-Border Growth

Differing national implementations of relevant directives means that a product cleared in one Member State may require significant reform to be approved in another.[382] This fragmentation is particularly evident in PSD2 APIs, where the lack of a specified standard format across the EU means that each bank may develop a different API standard, requiring TPPs to build separate solutions for each bank.[383] Not

[375] See PSD2 art 10(1).
[376] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[377] Sharma and others (n 311)
[378] Radnejad, Osiyevskyy and Scheibel (n 119).
[379] International Monetary Fund, Monetary and Capital Markets Department and Legal Department (n 168).
[380] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[381] ibid.
[382] Sharma and others (n 311)
[383] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).

only does this significantly increase costs for TPPs, it also hinders cross-border activity.[384] Furthermore, diverging licensing and supervisory mechanisms for payments and EMIs across Member States also create legal uncertainty, and incentivise forum shopping, with firms seeking authorisation in less stringent jurisdictions, and then passporting their services across the EU.[385] "De-risking" policies in traditional banks, wherein they unilaterally close accounts for non-bank payment service providers to avoid AML risks, which have been criticised by TPPs for breaching PSD2, have also made it more difficult for them to provide services.[386]

Another area of ambiguity regarding cross-border movement concerns the use of third-country ICT service providers and intra-group delegation. DORA explicitly prohibits financial entities from relying on "critical" third-country ICT providers, unless that provider establishes a subsidiary within the EU within 12 months of its designation.[387] This provision is problematic, in part because financial firms often lack the capacity to determine which of their providers fall under this category, which may lead to non-EU ICT providers essentially getting ousted outright.[388] This, in turn, puts EU entities at a competitive disadvantage. Restricting the geographical scope of providers may even paradoxically weaken resilience by limiting access to technology available in third countries.[389] Critics, therefore, have argued that DORA should follow GDPR standards, which extend jurisdictional reach through adequacy mechanisms instead of blanket prohibitions.[390]

These challenges are compounded by the supervisory architecture within the EU. The European System of Financial Supervision (ESFS) operates largely along sectoral lines, with competent national authorities sharing responsibility with the European Central Bank and the European Supervisory Authorities.[391] For large multinational enterprises, this means they will have to answer to different regulators for different parts of the same business.[392] Furthermore, incident reporting under DORA requires firms to implement different national solutions for each Member State for major ICT-related incidents and registers of information, which increases costs.[393] There have been calls for a single EU hub to centralise incident reporting and improve supervisory convergence.[394]

The lack of harmonisation directly affects fintechs' capacity to innovate and scale.[395] In this environment, firms channel their innovation capacity into workarounds for compliance rather than product development. By contrast, a more coordinated framework across the board would lower entry barriers, provide predictability for cross-border operations, and enhance legal certainty.

[384] Sharma and others (n 311)
[385] *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)* (n 49).
[386] ibid.
[387] DORA art 31(12).
[388] American Chamber of Commerce to the European Union (n 367).
[389] ibid.
[390] ibid.
[391] Buttigieg and Zimmermann (n 248).
[392] Banking Stakeholder Group (BSG), European Banking Authority (n 288).
[393] Buttigieg and Zimmermann (n 248).
[394] ibid.
[395] Sharma and others (n 311).

5.4. Net Effects

The analyses in Sections 5.2 and 5.3 show how the EU's comprehensive framework produces legal effects that indirectly boost growth and innovation but are also characterised by overlaps and constraints that significantly burden fintechs, particularly smaller EMIs and PIs. The table below summarises the key EU instruments covered, the main benefits and frictions that come with them, and relevant overlaps within the same landscape.

Instrument	Primary objective	Key benefit	Key friction	Overlap
PSD2	Competition & innovation in payments	Mandated data access; passporting	Implementation divergence; complexity of SCA; fragmented APIs	GDPR (consent/minimisation); DORA (incident/reporting)
EMD2	Protection of customer funds in electronic money accounts	Safeguarding certainty; reduced insolvency risks	Capital immobilisation; operational rigidity	AMLD (traceability); PSD2 (SCA and refund liability);
AMLDs	Prevention of money laundering and terrorist financing	Standardised KYC; reduced risk of financial crimes	Ongoing monitoring costs; resource-intensive compliance	GDPR (data retention/processing); EMD2 (safeguarding/traceability)
GDPR	Protection of personal data	Trust and user control	Chilling effect; limits flexibility in data use	PSD2 (access to account / explicit consent); DORA (data retention); AMLD (KYC data handling)
DORA	Strengthening ICT security & resilience	Operational resilience; incident preparedness	Heavy ICT documentation; limits agility; cross-border vendor restrictions	PSD2 (incident reporting before Amendment); GDPR (data retention)

Table 1: Cumulative Legal Effects of EU Fintech Regulatory Instruments

Overall, the net effect of these regulations can be characterised as double-edged. While each instrument has clear benefits, including consumer protection and improved systemic resilience, overlaps and cumulative frictions constrain fintechs' ability to manage capital effectively, innovate, or scale operations. The following chapter extends this analysis by comparing this landscape with those in non-EU jurisdictions, aiming to identify how different approaches shape innovation incentives.

Chapter VI: Comparative Analysis

6.1. Introduction

This chapter examines how regulatory approaches of the U.S. and Singapore are structured and affect fintech innovation, with particular attention to payment services and e-money institutions. Building on the detailed discussion of EU fintech regulation in Chapters III–V, this chapter serves as a comparative lens to assess the regulatory effects of alternative frameworks. It aims to determine which approach is most favourable to innovation whilst still maintaining security and market integrity.

6.2. Fintech Regulation and Innovation in the United States

6.2.1. The Institutional Framework and Money Services Businesses (MSBs)

The U.S. financial legal framework is characterised by a fragmented, state-federal structure with multiple overlapping regulators. Regulatory intervention generally occurs after violations or risks have been identified, rather than through pre-emptive measures.[396] Unlike the EU's PSD2 mandates on SCA and mandatory Open Banking, the U.S. lacks unified technical standards for APIs or payment access, resulting in greater flexibility initially for increasingly operational frictions as it progresses.

A number of federal agencies play distinct and sometimes overlapping roles in overseeing financial activities, particularly those related to payment services and e-money. This includes the Office of the Comptroller of the Currency (OCC) as the primary federal regulator for nationally chartered banks; the Federal Deposit Insurance Corporation (FDIC), which insures deposits and examines financial institutions (including fintechs); the Consumer Financial Protection Bureau (CFPB), focusing specifically on consumer protection; and the aforementioned finCEN, responsible for implementing the BSA.[397]

The provision of payment services in the US largely falls under the purview of Money Services Businesses (MSBs), a broad category of nonbank financial institutions that offer services including money transmission, prepaid instruments, or currency exchanges.[398] State-level licensing for MSBs is similar to the EU's licensing and safeguarding requirements under EMD2 and PSD2, but lacks a single harmonised regulatory authority. Licensing for money transmitters happens at state level and payment providers need individual licenses from each state they operate in, subject to state-specific requirements for minimum capital, security (e.g. bonds), and examinations.[399] Consumer protection laws dictate credit terms, meaning fintech companies may fall under the jurisdiction of states where their customers reside, even if the fintech does not operate from there. Meanwhile, at the federal level, MSBs have to register with the Financial Crimes Enforcement Network (FinCEN), which is primarily responsible for implementing the Bank Secrecy Act, which aims to combat money laundering and the financing of terrorism.[400]

Compliance challenges primarily stem from these diverging state-by-state requirements, although efforts have been made to harmonise them.[401] To streamline multi-state licensing, the Nationwide

[396] Marc Labonte, 'Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework' (Congressional Research Service, R44918, 2023).
[397] ibid.
[398] Labonte (n 396).
[399] ibid.
[400] Päivi Hutukka, 'Fintech Law in the European Union, the United States and China: Regulation of Financial Technology in Comparative Context' (2024) 31 Maastricht Journal of European and Comparative Law 559.
[401] ibid.

Multistate Licensing System and Registry (NMLS) provides a uniform license application that can be submitted to multiple states for approval.[402] Nonetheless, review of applications and approvals remain under the discretion of each state.[403]

In the absence of a singular framework, this approach means regulatory jurisdiction is typically based on the charter type of an entity, rather than the specific financial function it performs.[404] Many fintech companies in the U.S. seek a bank charter due to its structural advantages.[405] Most significantly, a bank charter allows engagement in banking activities across different states without needing a separate license for each state, and is shielded from state laws through federal pre-emption.[406] The OCC has proposed a special-purpose bank charter (often referred to as the "fintech charter") for fintech companies that do not take deposits, which would also grant federal pre-emption.[407]

Rather than seeking bank charters themselves, many other fintech companies instead opt for partnerships with existing banks, where they function to enhance bank processes, such as by underwriting models, or referring loan applicants directly to banks.[408] However, banks often view these partnerships as higher risk, especially regarding their AML practices.[409] Furthermore, regulators exercise discretion when scrutinising "true lender" arrangements where the fintech partner plays a significant role in credit extension and regulators may classify them as "institution-affiliated".[410] Non-bank fintechs also face challenges in maintaining operations post-approval, including AML compliance, consumer protection audits, and operational reporting obligations.[411] These persisting challenges may ultimately offset the initial advantages of rapid market entry.

It's worth noting that the U.S. does not maintain a distinct regulatory category for "e-money issuers". Payment services, including mobile payment providers, are typically classified and regulated under the MSB framework.[412] In entering the market, fintechs are met with a friendly environment. The absence of a singular regulatory framework, as well as the slow pace of legislative processes, can create an initial "white space" where new models (like the buy-now-pay-later model) can be developed under relatively lighter conditions, or without being explicitly prohibited.[413] This allows them to often launch without explicit regulatory hurdles.

6.2.2. Anti-Money Laundering and Know-Your-Customer Obligations

The primary federal mandate governing AML compliance stems from the Bank Secrecy Act (BSA) and the subsequent USA PATRIOT Act of 2001.[414] Under these statutes, MSBs and other financial

[402] See Conference of State Bank Supervisors, 'Nationwide Multistate Licensing System (NMLS)' (*CSBS*) <https://www.csbs.org/nationwide-multistate-licensing-system-nmls> accessed 18 November 2025.
[403] ibid.
[404] Brian Christiansen, Khalil Maalouf and Patrick Brandt, 'A Look at US and EU Fintech Regulatory Frameworks' (Skadden, Arps, Slate, Meagher & Flom LLP, 2018).
[405] ibid.
[406] ibid.
[407] ibid.
[408] ibid.
[409] Ryan Clements, 'Regulating Fintech in Canada and the United States: Comparison, Challenges and Opportunities' (2020) (Forthcoming, The Routledge Handbook of FinTech, Routledge 2020) <https://ssrn.com/abstract=3557576> accessed 29 August 2025.
[410] Christiansen, Maalouf and Brandt (n 404).
[411] ibid.
[412] Labonte (n 396).
[413] Hutukka (n 400).
[414] Labonte (n 396).

institutions are required to establish and maintain comprehensive risk-based AML programmes.[415] These programmes are designed to prevent the financial system from being used for illicit activities, including money laundering and terrorist financing.[416]

Bank and non-bank financial institutions are obliged to employ CDD measures to ensure customers are not identified on government lists of suspicious individuals.[417] This includes record-keeping obligations for transaction-related data and information used for customer identification, as well as reporting obligations for any suspicious activity regarding transactions or activities that are deemed suspicious.[418]

At the federal level, compliance and enforcement are overseen by FinCEN.[419] Recent federal law, in particular the Anti-Money Laundering Act of 2020 (AML Act), reinforced FinCEN's authority. The AML Act mandated that the Secretary of the Treasury, in consultation with regulators, establish and publish national AML/CFT Priorities.[420] Covered non-bank financial institutions are expected to eventually incorporate these priorities into their risk-based AML programmes.[421] The AML Act also granted FinCEN additional enforcement powers. Under this framework, non-U.S. financial institutions with U.S. accounts may be subpoenaed by FinCEN and the DOJ to provide account records for anti-money laundering monitoring.[422] In a similar vein, the Corporate Transparency Act incorporated within the AML Act also introduced ownership reporting requirements for non-US firms operating in the U.S, partly in order to combat illicit financial activity.[423]

Finally, as mentioned previously, fintechs that partner with banks are often required to also subscribe to the bank's AML programs, which can impose heightened standards compared to stand-alone MSBs, as chartered banks are subject to heightened prudential control.[424] As such, these partnerships may be characterised as higher risk for AML compliance purposes.

6.2.3. Data Protection and Operational Resilience

Data protection in the U.S. financial sector is governed through a patchwork of federal and state regulations, instead of a comprehensive law comparable to the EU's GDPR. The primary statute at federal level relevant to fintechs is the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions to collect, use, and safeguard consumers' personal information, as well as report data-sharing practices.[425] Fintech firms involved in payment service must also comply with consumer protection measures where applicable.[426] Credit card-based mobile transactions are governed by the Truth in Lending Act, while debit and bank-funded payments are protected by the Electronic Funds Transaction Act, and users thereby are granted the same protections against fraud as traditional card transactions.[427]

---

[415] Financial Crimes Enforcement Network, 'Statement for Non-Bank Financial Institutions' (2021) (FinCEN Statement).
[416] Labonte (n 396).
[417] Brian S. Korn and Bernhard Alvine, 'Fintech Laws and Regulations: USA 2025' in *ICLG - Fintech Laws and Regulations* (Global Legal Group 2025).
[418] ibid.
[419] Labonte (n 396).
[420] FinCEN Statement (n 415).
[421] ibid.
[422] ibid.
[423] ibid.
[424] Christiansen, Maalouf and Brandt (n 404).
[425] Korn and Alvine (n 417).
[426] ibid.
[427] Hutukka (n 400).

While data protection is not as strictly regulated as in the EU, there is an increasing shift toward stricter measures, evident especially at state level. Laws such as the California Consumer Privacy Act (CCPA) and the later California Privacy Rights Act (CPRA) impose additional transparency and consumer-rights obligations, including the right to access, deletion of data, and opt-out rights, akin to some extent to GDPR protections.[428] Several other states, including Virginia, Colorado, and Texas, have enacted similar privacy laws.[429] These state-level initiatives have led to a gradual convergence toward stronger user data protections.

Fintech companies engaged in payment services and e-money issuance must therefore comply with both GLBA-based financial privacy requirements and any state-specific data-protection laws applicable to their operations or customers.

With regard to operational resilience, regulation is similarly decentralised. For fintechs in particular, specific standards depend on their mode of operation. If a fintech operates as a licensed MSB, it should follow federal cybersecurity and operational risk standards under the Bank Secrecy Act (BSA) and FinCEN regulations, but there's no comprehensive resilience regime for bank or non-bank financial institutions comparable to the EU's DORA.[430] If it partners with a bank, and performs core functions for the bank, it may be subject to requirements under the Bank Service Company Act (BSCA) which obliges them to notify a bank-designated point of contact if it has experienced a computer security incident.[431]

At the federal policy level, there are sectoral frameworks (like the FTC Safeguards Rule for nonbank financial institutions, or NIST Cybersecurity Framework) which are recommended but not mandatory unless incorporated into state licensing rules or specific supervisory guidance.[432]

6.2.4 Evaluation and Innovation Policy

US policy makers, particularly at state level, do utilise tools like regulatory sandboxes to allow firms to experiment with financial services under supervision. For instance, Arizona launched the first U.S. regulatory sandbox for fintechs in 2018, allowing local firms to test new products and services without incurring compliance burdens[433]. Other states, including Florida, Arizona, and Nevada, have also adopted similar models.[434] Innovation is fostered at the federal level, with the OCC and the CFPB having launched an Office of Innovation explicitly to stimulate fintech innovation.[435] Overall, early-stage fintechs in the U.S. can typically launch quickly and test products without significant centralised regulatory burdens.[436] They also benefit from flexible frameworks when experimenting with new products or services.

[428] Korn and Alvine (n 417); Cal Civ Code §§ 1798.100–1798.199.100.
[429] Korn and Alvine (n 417).
[430] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021).
[431] ibid; Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37,920 (June 9, 2023).
[432] Jonathan Rogers, Alessandro Zappasodi and Roseann Cook, 'Operational Resilience in the UK, EU and US: A Comparison' (White & Case LLP 2022) <www.whitecase.com/insight-our-thinking/financial-regulatory-observer-2022-operational-resilience-uk-eu-and-us> accessed 4 December 2025.
[433] Greater Phoenix Economic Council, 'Things to Know About Arizona's FinTech Sandbox' (GPEC, 8 April 2021) <https://www.gpec.org/blog/things-to-know-about-arizonas-fintech-sandbox/> accessed 28 August 2025.
[434] Korn and Alvine (n 417).
[435] ibid.
[436] Hutukka (n 400).

However, state-by-state fragmentation as well as agency fragmentation make scaling very difficult, and create uncertainties for fintechs on enforcement jurisdictions.[437] When a fintech firm attempts to scale beyond a pilot stage and operate on a national basis, it will face complex and potentially conflicting areas of federal and state requirements.[438] This decentralised system significantly increases compliance costs. For instance, PayPal and Stripe initially expanded nationwide without a centralised federal license. However, they were later required to obtain multiple state money transmitter licenses.[439] It is worth noting that U.S. regulators do not necessarily anticipate new business models nor lay down harmonised frameworks from the outset. Instead, fintechs innovate and scale until regulators catch up, at which point regulators impose measures depending on the specific circumstances.[440]

In addition to the high costs of national scaling and the burdens of state-by-state licensing, fintechs that choose instead to partner with traditional banks also face limitations.[441] In particular, this model can limit how far fintech products can deviate from traditional financial rails due to banks' already exhaustive prudential standards and supervisory oversight.[442] This regulatory complexity can influence the types of services fintechs in the US prioritise. For instance, many US fintechs, such as Stripe, tend to focus on B2B services and infrastructure rather than direct consumer wallets.[443] This is because it is simply easier to scale when avoiding the more burdensome regulatory measures associated with consumer-facing activities.

It is evident that, compared to the EU, the US system offers more "white space" for creative pilots and state-level experimentation. However, it provides far less certainty and efficiency for taking those pilots to a wider scale.

[437] Christiansen, Maalouf and Brandt (n 404).
[438] ibid.
[439] See PayPal, 'Licenses' (*PayPal*) <https://www.paypal.com/us/webapps/mpp/licenses> accessed 28 August 2025; Stripe, 'Licenses' (*Stripe*) <https://stripe.com/legal/spc/licenses> accessed 28 August 2025.
[440] Hutukka (n 400).
[441] Christiansen, Maalouf and Brandt (n 404).
[442] Labonte (n 396).
[443] Christiansen, Maalouf and Brandt (n 404).

6.3 Fintech Regulation and Innovation in Singapore

6.3.1. Institutional and Policy Framework

The development and governance of fintechs in Singapore is structured by the Monetary Authority of Singapore (MAS) and its overarching objective to position Singapore as a global leader in fintech innovation otherwise referred to as a "Smart Financial Centre".[444] MAS operates as both the central bank and the integrated financial authority and encourages both innovation and risk mitigation for consumers and other stakeholders.[445] To institutionalise support for its ambitions, the MAS and the National Research Foundation (NRF) jointly established the FinTech Office in May 2016, focusing on coordinating government efforts and identifying gaps in regulation to ultimately market Singapore as an industry hub.[446] MAS continued these efforts by forming the FinTech & Innovation Group in 2015 and an International Technology Advisory Panel to gather expert advice on international developments.[447]

Fintech oversight is guided by principles that inherently (and intentionally) support innovation. The regulatory philosophy adopted by MAS contrasts significantly with traditional or ex-ante approaches to fintech developments. It recognizes that the premature introduction of regulatory restrictions may potentially derail useful technology and therefore operates a responsive "test-and-learn" methodology.[448] Its risk-based approach offers greater business flexibility to firms that pose less significant risks, or are better-managed.[449] Regulation is introduced when risks become "material", with regulatory responses adjusted proportionately to the identified risk.[450] In addition, MAS has implemented a disclosure-based regime, under which firms must disclose accurate and meaningful information for consumers to make informed decisions, rather than the regulator being responsible for assessing product suitability.[451] Firms are expected to self-regulate and self-monitor their riskier activities in order to minimise regulatory interference.[452]

The Fintech Office is a collaborative entity involving MAS and the NRF, alongside representatives from other public and private entities, including the Info-Communications Media Development Authority (IMDA).[453] MAS also works alongside the Cyber Security Agency (CSA) of Singapore to identify threats and ensure operational resilience.[454] Finally, formal mechanisms in place such as the Inter-agency Committee (IAC) and the AML/CFT Steering Committee form part of the structure by facilitating information sharing and coordination, especially with regard to AML/CFT objectives.[455]

6.3.2. The Payment Services Act (PSA 2019)

---

[444] Deirdre M Ahern, 'Regulators Nurturing FinTech Innovation: Global Evolution of the Regulatory Sandbox as Opportunity Based Regulation' (2019) 15 Indian JL & Tech 2.
[445] Pei Sai Fan, 'Singapore Approach to Develop and Regulate FinTech', *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1* (Elsevier 2018) <https://linkinghub.elsevier.com/retrieve/pii/B9780128104415000154> accessed 29 August 2025.
[446] Adrian Ang, Samuel Kwek and Anil Shergill, 'FinTech in Singapore' (2019) 20 Business Law International.
[447] ibid.
[448] Fan (n 445).
[449] Hazik Mohamed, 'Fintech Regulation and Governance from the Singapore Perspective' (2025) 10 International Journal of Islamic Business 1.
[450] Fan (n 445).
[451] ibid.
[452] ibid.
[453] Fan (n 445).
[454] Mohamed (n 449).
[455] Financial Action Task Force, 'Singapore: 3rd Enhanced Follow-Up Report & Technical Compliance Re-Rating' (Financial Action Task Force 2019).

The foundational legal instrument governing fintech activities related to payments in Singapore is the 2019 Payment Services Act (PSA).[456] The PSA follows a modular licensing regime, allowing businesses to customise their licenses based on the specific service they provide in an effort to ensure proportionality and reduce compliance burdens for smaller fintechs while holding larger ones to stricter standards.[457] It defines seven distinct payment services subject to licensing requirements: (1) money-changing services, defined as buying or selling foreign currency notes; (2) account issuance services; (3) domestic money transfer services; (4) cross-border money transfer services; (5) merchant acquisition services; (6) e-money issuance services; and (7) digital payment token (DPT) services.[458] This aligns Singapore's regulatory scope with international standards governing payment and e-money institutions.

The application of this framework is instantiated through three license tiers: the Money-Changing License, the Standard Payment Institution (SPI) License, and the Major Payment Institution (MPI) License. The Money-Changing License is the narrowest, permitting only money-changing services.[459] In contrast, SPI and MPI licenses are not defined by the service being offered, but by quantitative thresholds of risk. MPI status is mandated when monthly transaction volumes exceed a set threshold (namely S$3 million for a single service and S$6 million for multiple services offered), or when the average daily e-money float surpasses S$5 million.[460] As such, the intensity of oversight is directly correlated to the licensee's market scale and their potential for consumer harm or financial instability.

The PSA also enforces strict AML/CFT regulations and KYC procedures for all payment service entities privy to illegal activities.[461] Some entities which are deemed low risk may be exempt from these requirements. For instance, cross-border money transfer services may be exempt from AML/CFT requirements if payments are for goods or services and funding comes from an identifiable AML-regulated financial institution account.[462] These requirements provide oversight, similar to PSD2 and AMLD, but unlike in the EU, they are specifically designed around reducing entry barriers for low-risk innovators.

6.3.3. Cybersecurity and Data Protection

Beyond the PSA, Singapore's framework also includes the Technology Risk Management (TRM) Guidelines and the Personal Data Protection Act (PDPA), which are used to assess entities' IT risk management, cybersecurity, system infrastructure, as well as data protection and incident management, akin to DORA and the GDPR, albeit in a lighter-touch manner.[463] The TRM Guidelines emphasize that financial institutions must establish strong risk governance frameworks to ensure data confidentiality and integrity, as well as system reliability and stability.[464] The level of implementation required under the Guidelines is assessed proportionately in relation to the level of risk and complexity in the provision of the specific service.[465]

For the mitigation of cyber risks, the TRM Guidelines mandate specific measures concerning system security and resilience. Financial institutions must adopt a "defence-in-depth" approach to cyber

[456] Payment Services Act 2019 (Act 2 of 2019) (PS Act).
[457] Mohamed (n 449).
[458] PS Act First Schedule, Part 1, para 1(a)–(g).
[459] ibid 6.
[460] ibid.
[461] Mohamed (n 449).
[462] Ang, Kwek and Shergill (n 446).
[463] Mohamed (n 449).
[464] Monetary Authority of Singapore, 'Technology Risk Management Guidelines' (Monetary Authority of Singapore 2021).
[465] ibid.

resilience which necessitates regular cyber security assessments (e.g. annual penetration testing) and recovery metrics.[466] With regard to data centre resilience, the TRM's scope extends the definition of risk beyond technical threats to include the political and environmental climate of data centre locations.[467]

In consideration of the industry's increasing reliance on third-party vendors for core services, under the MAS Guidelines on Outsourcing, a financial institution may delegate a function to another provider but it cannot delegate its liability or the governance responsibilities of its board and senior management.[468] When entering into any material outsourcing arrangement (an arrangement with the potential to materially impact business operations, reputation, or customer information), the institution must perform comprehensive due diligence on the service provider.[469] Since cloud computing is considered a form of outsourcing, financial entities must ensure that cloud service providers have the ability to identify and segregate customer data through strong controls, and must incorporate legally enforceable exit and transition strategies into outsourcing agreements.[470]

Data protection is governed by the 2012 Personal Data Protection Act (PDPA) and its 2020 amendment which introduced mandatory breach reporting obligations, similar to those laid out in the GDPR.[471] If an organization has reason to believe a data breach affecting personal data in its possession has occurred, it must conduct an assessment, and if the breach is deemed notifiable (i.e., likely to result in significant harm to the affected individual), the organization must notify the Personal Data Protection Commission and the affected individuals without undue delay.[472] This regime adds to the TRM Guidelines, which impose security requirements on fintechs for the safeguarding of data confidentiality and integrity against threats.

To streamline KYC processes, Singapore has developed MyInfo, which provides identity verification and can be used without the need for additional physical documents.[473] MAS accepts MyInfo as a credible source for verifying essential identity elements (such as name, unique identification number, date of birth, nationality, and residential address) for non-face-to-face transactions.[474] This has enabled fintech start-ups and other financial institutions to reduce onboarding costs and time.[475]

6.3.4. Mechanisms for Innovation and Challenges

MAS employs several innovation-support mechanisms to enable responsible innovation. In 2016, MAS introduced the Fintech Regulatory Sandbox for this purpose by providing a controlled environment in which fintechs can test innovative products and services under relaxed regulatory requirements for a defined period.[476] The sandbox is explicitly designed to contain any consequences of failure.[477]

The treatment afforded to participating entities within the sandbox is proportional and discretionary. MAS has the authority to modify specific regulatory requirements on a case-by-case basis for the

[466] ibid.
[467] ibid.
[468] Monetary Authority of Singapore, 'Guidelines on Outsourcing' (Monetary Authority of Singapore 2016).
[469] ibid.
[470] ibid.
[471] Personal Data Protection Act 2012 (No 26 of 2012) pt VIA.
[472] ibid.
[473] Ang, Kwek and Shergill (n 446).
[474] ibid.
[475] ibid.
[476] Mohamed (n 449).
[477] ibid.

duration of the testing period.[478] Requirements that may be relaxed include financial requirements such as minimum capital adequacy requirements, credit ratings, as well as IT risk management and outsourcing rules.[479] Certain protections, however, such as data protection and AML/CFT compliance, cannot be waived.[480]

To be eligible for the sandbox, applicants must demonstrate that the proposed service uses new or innovative technology, or existing technology in an innovative way, brings value to consumers or the industry in some way, and has the intention and ability to be deployed beyond Singapore.[481] Over forty firms have participated in sandbox trials[482]. One example is firm ADDX, which scaled private market access services after testing them under the sandbox[483].

In 2019/2020, MAS launched Sandbox Express as a fast-track option for low-risk innovations, under a block exemption framework and offering quicker approval timelines within those categories.[484] Applicable services include remittance services, certain DPT services, insurance broking, and recognised market operators.[485]

Singapore leverages its small domestic market by participating in international frameworks like the Global Financial Innovation Network (GFIN), which promotes cross-border testing of fintech innovations and the harmonization of regulatory standards internationally.[486] As such, it has collaborated with other countries in the region to establish cross-border payment links (e.g. the integration of Singapore's PayNow and Thailand's PromptPay).[487]

Despite its successes, Singapore still faces challenges in its regulatory framework for fintechs. The rapid evolution of technology often makes it difficult for regulators to understand and define mandates for innovations.[488] Information asymmetries between regulators and market players can impede proper judgment of novelty and risk when it comes to emerging or innovative technologies.[489] Furthermore, the sandbox model has been criticised due to its discretionary nature, with critics arguing that regulators essentially take on the role of "arbiters" of innovations[490]. The limited scale of sandbox testing may also not be efficient in fully predicting the risks that a product carries, especially when scaled up.[491] Finally, the competition among jurisdictions, such as Singapore and Hong Kong, to establish themselves as fintech hubs, could potentially lead to a "race to the bottom" in security standards, moving even further away from true global harmonisation.[492]

---

[478] Fan (n 445).
[479] ibid.
[480] ibid.
[481] Fan (n 445).
[482] János Kálmán, 'The Role of Regulatory Sandboxes in FinTech Innovation: A Comparative Case Study of the UK, Singapore, and Hungary' (2025) 4 FinTech 26.
[483] Economic Development Board (EDB), Singapore, 'How Singapore's FinTech Regulatory Sandbox Is Helping Fintech Innovators Accelerate Time to Market' (EDB 22 August 2022) <https://www.edb.gov.sg/en/business-insights/insights/how-singapore-s-fintech-regulatory-sandbox-is-helping-fintech-innovators-accelerate-time-to-market.html> accessed 29 August 2025.
[484] Ahern (n 444).
[485] ibid.
[486] ibid.
[487] ibid.
[488] ibid.
[489] Ahern (n 444).
[490] ibid.
[491] Christopher J Brummer and Yesha Yadav, 'Fintech and the Innovation Trilemma' (2019) 107 Georgetown Law Journal 235.
[492] ibid.

That said, Singapore has effectively positioned itself as attractive to fintechs, offering proactive solutions with centralised regulation and consistently seeking to invest in innovation. Global fintechs, such as Revolut, have based their regional activities in Singapore, precisely because their environment is one that gives fintechs a lot of room to manoeuvre while still maintaining stability.[493] However, Singapore's smaller domestic market limits cross-border movement in a way that cannot emulate the EU's passporting advantages.

6.4. Comparative Evaluation of Legal Models

6.4.1. Comparative Evaluation of Regulatory Approaches

Legal models govern compliance, but they also shape the trajectory and space of fintech operations. Because payment services and e-money institutions move rapidly across borders, the regulatory environment in which they operate directly impacts their business models, leading different jurisdictions to decide where they want to sit on the scale between fostering innovation and fostering market integrity, depending on their market realities. The aim of this comparison is not to find a "perfect" system, since none can be said to exist, but to evaluate the trade-offs each approach entails. A legal model can encourage rapid integrity at the expense of optimal security and market stability, as it can also protect the market while stifling new entrants.

To assess which approach comes closer to an optimal balance, three aspects can be looked at:

(1) The Legal Foundations for Innovation

As described in Chapters III-V, the EU's regime, composed of PSD2, EMD2, AMDs, DORA, and the GDPR, creates a compliance-heavy environment under which innovation is often a by-product rather than a direct objective. Firms innovate in RegTech solutions, design business models around IT infrastructure and Strong Customer Authentication, but these are largely workarounds to regulatory requirements rather than market-driven innovations.

The U.S. provides a counterpoint to this. It is regarded as a decentralised model built around state-level money transmitter licensing and federal statutes, such as the Bank Secrecy Act (relating to AML) or the Gramm–Leach–Bliley Act (relating to data privacy) and founded on a philosophy of reactive regulation.[494] There is no act in the U.S. that is comparable to the EU's PSD2 or EMD2. This eliminates some statutory conflicts as identified in Chapter V (e.g. the PSD2/GDPR consent inconsistency), but it also brings with it legal uncertainty. Firms have to navigate licensing for each state individually and carry the burden of that cost, whilst also dealing with unclear potential enforcement measures.[495]

Conversely, Singapore has adopted an anticipatory approach. The Payment Services Act 2019 ties together multiple categories in one single, tiered licensing system. This avoids the duality in the EU between Payment Institutions and EMIs as explored in §3.2–3.3 and §5.3.1.2, while still being flexible in mandating different capital and safeguarding requirements depending on the size and risk of the firm. Data protection, as protected by the PDPA, also prevents the dual-consent conflict as seen between PSD2's requirement for explicit consent for payment initiation and account access and the GDPR's standards under Article 6.[496] AML/CFR obligations are also accounted for and harmonised under

[493] Alex Carril, 'Q&A with CEO Raymond Ng on Revolut's Growth in Singapore' (*Revolut Ltd*, 24 June 2025) <https://www.revolut.com/blog/post/q-and-a-with-ceo-raymond-ng-on-revoluts-growth-in-singapore/> accessed 4 December 2025.
[494] Labonte (n 396).
[495] Clements (n 409).
[496] Personal Data Protection Act 2012 (No 26 of 2012) arts 13–14.

MAS.[497] Singapore's legal model, then, is streamlined from the outset to reduce friction as much as possible and provide an innovation-friendly environment for fintechs.

(2) Trade-Offs in Legal Certainty and Market Integrity

These divergent approaches demonstrate a key trade-off. The EU's regulations aim to maximise legal certainty ex ante.[498] They provide detailed rules on fund safeguarding, capital, and operational resilience, leaving little ambiguity between the lines. However, the level of comprehensiveness adopted also paradoxically creates cumulative frictions which are felt most by smaller entrants.[499]

The U.S. model is effectively the opposite of this. Legal certainty is low ex ante, since obligations greatly vary by state and protections are even.[500] Market integrity depends on and revolves around ex post enforcement, with federal agencies acting after cases of non-compliance.[501] This is a very entrepreneurial-focused approach. It allows firms to scale rapidly without facing PSD2/EMD2-like burdens, but it also brings about high legal risks.

Singapore represents a middle ground in this matter. Legal certainty is high because rules regarding licensing, AML, and data protection are clearly set out, but applicable obligations depend on the degree of risk exposure.[502] For instance, unlike the EU's one-size-fits-all safeguarding rules, Singapore imposes more demanding requirements on Major Payment Institutions.[503] This is an attempt to avoid both the rigidity associated with the EU model and the uncertainty associated with the U.S model.

(3) Cross-Border Scalability and Its Legal Roots

The scalability of fintech operations is directly shaped by the legal architecture of the jurisdiction. In the EU, once a firm has overcome the initial burdens of licensing and compliance, it benefits from the passporting regime, an unparalleled legal right to operate across Member States. This does, however, come with the high costs of entry barriers, as noted in Chapter V. The U.S. does not employ any passporting-like policies; instead, it imposes a patchwork of state approvals.[504] The legal cost of expanding to other states increases with each jurisdiction, yielding an exceedingly fragmented environment. Singapore also lacks an equivalent to EU passporting but relies on bilateral and multilateral agreements to give way to regional expansion in Southeast Asia.[505] The sandbox model helps firms expand into these markets, but it is not comparable to the automatic and immediate access EU passporting grants. However, its unified licensing mechanisms render the initial entry barriers quite low, which may enable firms to scale regionally more quickly than they would under the EU's duplicative framework.

6.4.2. Towards an Optimal Regulatory Approach: Lessons for the EU

We can deduce three separate models of fintech regulation: the EU's directive model, which provides comprehensive regulation and harmonisation but imposes significant compliance burdens, especially for new entrants; the U.S.'s reactive model, with regulation adapting to innovation but often leaving

[497] Mohamed (n 449).
[498] Sharma and others (n 311).
[499] ibid.
[500] Hutukka (n 400).
[501] Labonte (n 396).
[502] Mohamed (n 449).
[503] PS Act arts 22–26.
[504] Christiansen, Maalouf and Brandt (n 404).
[505] Mohamed (n 449).

firms in prolonged uncertainty after entry; and Singapore's proactive model, which directly engages with technological developments, but may lead to long-term systemic risks. It is clear that Singapore's system is the most innovation-friendly in practice, although that is not necessarily synonymous with it being the "best" approach overall. Innovation without sufficient safeguards can erode market integrity, and vice versa.[506]

An optimal balanced framework should allow early-stage innovation under controlled conditions (e.g. through sandboxes), but also then transition them into clear compliance standards, and provide mechanisms for cross-border movement and operability. The EU already occupies a middle ground, prioritising market integrity and harmonisation, while also providing the passporting framework that supports cross-border operation. However, it could be argued that the EU's strength is also its weakness: strong harmonisation efforts come at the cost of regulatory flexibility, and overlapping provisions and costs cause complexities that can slow down innovation relative to both the U.S. and Singapore.

While Singapore's proactive model is the most favourable for innovation, it cannot be transplanted as is without raising under-enforcement. The U.S. model demonstrates the benefits of early flexibility but also the costs of regulatory fragmentation. The EU offers predictability and strong protections, though sometimes at the expense of speed. The most effective balance, thus, would be a combination of the U.S.'s emphasis on entrepreneurial freedom, the proactivity of Singapore, and the safeguards and protections of the EU. This would be best suited to promote long-term growth and stability.

To achieve this, for the EU, the lesson is not deregulation, but alignment and simplification of the regulatory framework. Some concrete reforms follow directly from the frictions analysed in previous Chapters:

(i) The adoption of PSD3 consolidating PSD2 and EMD2. This unification would mirror Singapore's PSA, which in turn will eliminate redundancy as well as any uncertainties for firms operating under both regimes. These regulations could also remain separate statutes, but in this case, clearly defined guidance from the EU or coordination mechanisms would be needed to clarify any overlapping provisions and ambiguities.
(ii) Clarification of the PSD2 and GDPR interactions, particularly the consent rules, which currently constrain open banking innovations.
(iii) Streamlining operational resilience by aligning PSD2 risk management and incident reporting obligations with DORA.
(iv) Introducing a tiered capital adequacy framework, as in place in Singapore, where certain requirements are proportionate to the size and risk profile of the firm. This would replace the fixed minimum capital requirements currently in place in the EU and thus reduce the capital strain on smaller firms.

These reforms would lower barriers to entry and reduce current systemic compliance frictions. The result would be a regulatory framework that preserves key aspects of the EU's legal philosophy, including legal certainty, harmonisation, and consumer protection, while also fostering innovation, not as an incidental workaround, but as an intentional direct product of legal design.

[506] Brummer and Yadav (n 491).

Chapter VII: Conclusion

This thesis has examined the regulation of payment service fintechs and e-money institutions in the European Union. This legal framework is characterised by the interaction of multiple instruments, namely PSD2, EMD2, the AML Package, GDPR, and DORA. While the EU framework achieves important objectives for consumer protection and market stability, it does so through a cumulative layering of obligations that create significant burdens for firms, especially smaller ones aiming to enter the market. These frictions are most apparent in three domains: overlapping licensing regimes and capital requirements, the tension between mandated data access and data minimisation, and duplication between operational resilience instruments. In this environment, innovation primarily takes the form of compliance-driven adaptation; firms design tools such as RegTech solutions and IT infrastructures, which, albeit generate market value, were created primarily to satisfy regulatory requirements.

A comparative analysis was used to evaluate how alternative legal architectures in the United States and Singapore, notable for attracting fintech innovations, address these frictions and to propose a more fitting path for the EU. The U.S. model illustrates how regulatory fragmentation can lower some entry barriers by avoiding statutory collisions, but at the cost of legal certainty. Conversely, Singapore shows how proportionality and legal certainty can be used to encourage innovative developments and harmonisation. Neither system is perfect, but they do both highlight certain weaknesses in the EU framework: statutory overlaps (between PSD2 and EMD2), misalignment (between the GDPR and PSD2), and potential duplicative requirements (between PSD2 and DORA).

The primary conclusion is that the EU's regulatory design, while not fundamentally hostile to innovation, is structurally inefficient. Its strengths include a robust legal framework with increased certainty and consumer trust, but these strengths are partly undermined by redundancy and misalignment. Reform should therefore focus not on deregulation as such, but on alignment of the current framework to reduce unnecessary barriers to entry while still maintaining security.

The broader finding is that legal foundations serve as determinants for innovation. Innovation is heightened in jurisdictions where regulation is coherent, predictable, and accessible, not where regulation is absent entirely. By addressing key structural inefficiencies in its framework, the EU can keep its core safeguards and still move toward a regime where innovation in financial technology does not come as a by-product of compliance but is an intended outcome of the legal architecture in place.

Table of Legislation and Cases

European Union

Case C–362/14 Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650

Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Schrems [2020] ECLI:EU:C:2020:559

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 (Text with EEA relevance) [2009] OJ L267/7

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 and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance [2013] OJ L176/338

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 (Text with EEA relevance) [2015] OJ L337/35

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [2018] OJ L156/43

Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (Text with EEA relevance) [2022] OJ L 333

Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (Text with EEA relevance) [2024] OJ L 2024/1640

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

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 [2016] OJ L119/1

Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance.) [2018] OJ L 69

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [2022] OJ L333/1

Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism [2024] OJ L2024/1620

Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2024] OJ L2024/1624

Singapore

Payment Services Act 2019 (Act 2 of 2019)

Personal Data Protection Act 2012 (No 26 of 2012)

Personal Data Protection (Amendment) Act 2020

United States

Cal Civ Code §§ 1798.100–1798.199.100

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed Reg 66424 (23 November 2021)

Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed Reg 37920 (9 June 2023)

Bibliography

Journal Articles and Books

Abikoye BE and others, 'Regulatory Compliance and Efficiency in Financial Technologies: Challenges and Innovations' (2024) 23 World Journal of Advanced Research and Reviews 1830

Adeyemi A, 'A New Phase of Payments in Europe: The Impact of PSD2 on the Payments Industry' (2019) 25 Computer and Telecommunications Law Review 47

Ahern D, 'Regulators Nurturing FinTech Innovation: Global Evolution of the Regulatory Sandbox as Opportunity Based Regulation' (2019) 15 Indian JL & Tech 2.

Akter S and others, 'Transforming Business Using Digital Innovations: The Application of AI, Blockchain, Cloud and Data Analytics' (2022) 308 Annals of Operations Research 7

Ang A, Kwek S and Shergill A, 'FinTech in Singapore' (2019) 20 Business Law International

Arner DW, Barberis JN and Buckley RP, 'The Evolution of Fintech: A New Post-Crisis Paradigm?' (2015) University of Hong Kong Faculty of Law Research Paper 2015/047

Brener A, 'Payment Service Directive II and Its Implications' in Lynn T and others (eds), Disrupting Finance (Springer International Publishing 2019)

Brewczyńska M and Kosta E, 'From the Fight Against Money Laundering and Financing of Terrorism Towards the Fight for Fundamental Rights: Role of Data Protection' (2023) 2 Tilburg Law School Research Paper

Brummer C and Yadav Y, 'Fintech and the Innovation Trilemma' (2019) 107 Georgetown Law Journal 235

Buttigieg CP and Zimmermann BB, 'The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision' (2024) 25 ERA Forum 11

Christiansen B, Maalouf K and Brandt P, 'A Look at US and EU Fintech Regulatory Frameworks' (Skadden, Arps, Slate, Meagher & Flom LLP 2018)

Ryan Clements, 'Regulating Fintech in Canada and the United States: Comparison, Challenges and Opportunities' (2020) (Forthcoming, The Routledge Handbook of FinTech, Routledge 2020) <https://ssrn.com/abstract=3557576> accessed 29 August 2025.

Dini GB, 'The EU's Response to the Fragmented Emergence of Artificial Intelligence' in Costa O, Soler E and Vlaskamp M (eds), EU Foreign Policy in a Fragmenting International Order (Palgrave Macmillan 2025)

Dorfleitner G, Hornuf L and Kreppmeier J, 'Promise Not Fulfilled: FinTech, Data Privacy, and the GDPR' (2023) 33 Electronic Markets 33

Driver C and Johnston R, 'Understanding Service Customers: The Value of Hard and Soft Attributes' (2001) 4 Journal of Service Research 130

Ehrentraud J and others, ‘Fintech and Payments: Regulating Digital Payment Services and e-Money’ (Bank for International Settlements (BIS), Financial Stability Institute 2021) FSI Insights No 33

Fan PS, ‘Singapore Approach to Develop and Regulate FinTech’, *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1* (Elsevier 2018) <https://linkinghub.elsevier.com/retrieve/pii/B9780128104415000154> accessed 29 August 2025.

Ferrari V, ‘Crosshatching Privacy: Financial Intermediaries’ Data Practices Between Law Enforcement and Data Economy’ (2020) 6 European Data Protection Law Review 522

Ferretti F, ‘Open Banking: Gordian Legal Knots in the Uncomfortable Cohabitation between the PSD2 and the GDPR’ (2022) 30 European Review of Private Law 73

Gardner K, ‘Fighting Terrorism the FATF Way’ (2007) 13 Global Governance 325

Gennaro Corvese C, ‘Prudential Requirements for Payment Institutions: A European Union Perspective in View of PSD3’ (2024) 13 Law and Economics Yearly Review 125

Hallak I, ‘Payment Services Framework’ (EPRS | European Parliamentary Research Service 2025) Briefing PE 775.891

Helgadottir D, 'The Interaction between Directive 2015/2366 (EU) on Payment Services and Regulation (EU) 2016/679 on General Data Protection concerning Third Party Players' (2020) 23 Trinity CL Rev 199

Hutukka P, ‘Fintech Law in the European Union, the United States and China: Regulation of Financial Technology in Comparative Context’ (2024) 31 Maastricht Journal of European and Comparative Law 559

Iman N, ‘The Rise and Rise of Financial Technology: The Good, the Bad, and the Verdict’ (2020) 7 Cogent Business & Management 1725309

Kálmán J, ‘The Role of Regulatory Sandboxes in FinTech Innovation: A Comparative Case Study of the UK, Singapore, and Hungary’ (2025) 4 FinTech 26

Karasek-Wojciechowicz I, ‘Reconciliation of Anti-Money Laundering Instruments and European Data Protection Requirements in Permissionless Blockchain Spaces’ (2021) 7 Journal of Cybersecurity

Komandla V, ‘Overcoming Compliance Challenges in Fintech Online Account Opening’ (2017) 1 International Journal of Multidisciplinary and Current Educational Research 1

Korn BS and Alvine B, ‘Fintech Laws and Regulations: USA 2025’ in ICLG - Fintech Laws and Regulations (Global Legal Group 2025)

Kowalewski O and Pisany P, ‘The Rise of Fintech: A Cross-Country Perspective’ (2023) 122 Technovation 102642

Krueger M, ‘E-money regulation in the EU’ in Robert Pringle and Matthew Robinson (eds), E-Money and Payment Systems Review (Centralbanking 2002) 239–251

Labonte M, ‘Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework’ (Congressional Research Service 2023) R44918

Larsson B and others, ‘Digital Disruption Diversified—FinTechs and the Emergence of a Coopetitive Market Ecosystem’ (2024) 22 Socio-Economic Review 655

Lee I and Shin YJ, ‘Fintech: Ecosystem, Business Models, Investment Decisions, and Challenges’ (2018) 61 Business Horizons 35

Maclean F and others, ‘Consent under PSD2 and the GDPR: Squaring the Circle’ [2021] Butterworths Journal of International Banking and Financial Law.

Milaj J and Kaiser C, ‘Retention of Data in the New Anti-Money Laundering Directive—“Need to Know” versus “Nice to Know”’ (2017) 7 International Data Privacy Law 115

Mitsilegas V and Vavoula N, ‘The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law’ (2016) 23 Maastricht Journal of European and Comparative Law 261

Mohamed H, ‘Fintech Regulation and Governance from the Singapore Perspective’ (2025) 10 International Journal of Islamic Business 1

Możdżyński D, ‘The Conceptions of New Payment Methods Based on Revised Payment Services Directive (PSD2)’ (2017) 6 Information System in Management 50

Ndemo B and Mkalama B, ‘Digitalisation and Financial Data Governance in Africa: Challenges and Opportunities’ in Ndemo B and others (eds), Data Governance and Policy in Africa (Springer International Publishing 2023)

Pathak P, ‘Assessment of Compliance of GDPR in IT Industry and Fintech’ in Pradeep Kumar Singh and others (eds), Proceedings of Third International Conference on Computing, Communications, and Cyber-Security, vol 421 (Springer Nature Singapore 2023).

Pavlidis G, ‘Europe in the Digital Age: Regulating Digital Finance without Suffocating Innovation’ (2021) 13 Law, Innovation and Technology 464

Polasik M and others, ‘The Impact of Payment Services Directive 2 on the PayTech Sector Development in Europe’ (2020) 178 Journal of Economic Behavior & Organization 385

Radnejad A, Osiyevskyy O and Scheibel O, ‘Learning from the Failure of the EU Payment Services Directive (PSD2): When Imposed Innovation Does Not Change the Status’ (2021) 6 Rutgers Business Review 79

Ringe W-G and Ruof C, ‘Regulating Fintech in the EU: The Case for a Guided Sandbox’ (2020) 11 European Journal of Risk Regulation 604

Romanova I and others, ‘The Payment Services Directive II and Competitiveness: The Perspective of European Fintech Companies’ (2018) 21 European Research Studies Journal 3

Sharma A and others, ‘Governance Challenges in Cross-Border Fintech Operations: Policy, Compliance, and Cyber Risk Management in the Digital Age’ (2021) 4 Iconic Research and Engineering Journals 278

Skrabba J, 'Modernising Payment Services and Enhancing Open Banking: A Comparison of Recent EU Proposals of Payment Services Directive 3 (PSD3) and Payment Services Regulation (PSR) with

Current PSD2 (2024)' (15th Law in Business of Selected Member States of the European Union conference, Prague, March 2024

Sutton GW, 'The New FATF Standards' (2012) 4 George Mason Journal of International Commercial Law 68

Tosza S and Voordeckers O, 'An Anti-Money Laundering Authority for the European Union: A New Center of Gravity in AML Enforcement' (2024) 25 ERA Forum 405

Turing D and Crown S, '21st Century Payments in Europe: The Payment Services Directive' (2006) 2 Journal of Payment Systems Law 639

Uniwersytet Ekonomiczny w Krakowie and others, 'FinTech Regulation and the Development of the FinTech Sector in the European Union' (2023) 2023 Journal of Banking and Financial Economics 44

Voigt P and von dem Bussche A, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (2nd edn, Springer Nature Switzerland 2024)

Weber RH, 'The European E-Money Directive: Background, Problems, and Prospects' (2000) 5 Yearbook of International Financial and Economic Law 293

Zepeda R, 'PSD2: Regulation, Strategy, and Innovation' [2024] SSRN Electronic Journal https://www.ssrn.com/abstract=4998317 accessed 28 August 2025

Zetzsche DA and others, 'Fintech Toolkit: Smart Regulatory and Market Approaches to Financial Technology Innovation' (2020) University of Hong Kong Faculty of Law Research Paper No 2020/027.

Reports & Web Sources

3rdRisk, 'DORA | Digital Operational Resilience Act' (3rdRisk) <https://www.3rdrisk.com/framework/dora> accessed 1 September 2025

American Chamber of Commerce to the European Union, 'Our Position: Digital Operational Resilience Act (DORA)' (2021)

Banking Stakeholder Group (BSG), 'BSG Own Initiative Paper on DORA: Main Challenges and Recommendations' (European Banking Authority 2023)

Bureau of Consumer Financial Protection, 'Compliance Bulletin and Policy Guidance; 2016-02, Service Providers' (2016) 4810-AM-P

Carril A, 'Q&A with CEO Raymond Ng on Revolut's Growth in Singapore' (Revolut Ltd, 24 June 2025) <https://www.revolut.com/blog/post/q-and-a-with-ceo-raymond-ng-on-revoluts-growth-in-singapore/> accessed 4 December 2025

ComplyAdvantage, 'Guide to EU Anti-Money Laundering Directives (AMLD)' <https://complyadvantage.com/insights/eu-anti-money-laundering-directive/> accessed 1 September 2025

Conference of State Bank Supervisors, 'Nationwide Multistate Licensing System (NMLS)' (CSBS) <https://www.csbs.org/nationwide-multistate-licensing-system-nmls> accessed 18 November 2025

Cyber Risk GmbH, ‘eIDAS 2.0 | Updates, Compliance, Training’ (European Digital Identity Regulation) <https://www.european-digital-identity-regulation.com/> accessed 28 August 2025

CyberUpgrade, ‘DORA Regulation’ (CyberUpgrade) <https://cyberupgrade.net/dora-regulation/> accessed 1 September 2025

Directorate-General for Financial Stability, Financial Services and Capital Markets Union, ‘Fintech Action Plan’ (2018) Communication

Economic Development Board (EDB), Singapore, ‘How Singapore’s FinTech Regulatory Sandbox Is Helping Fintech Innovators Accelerate Time to Market’ (EDB Singapore, 22 August 2022)

European Banking Authority, ‘Guidelines on the Criteria on How to Stipulate the Minimum Monetary Amount of the Professional Indemnity Insurance under PSD2’ (2017) EBA-GL-2017-08

European Commission, ‘EU Blockchain Observatory and Forum’ (Shaping Europe’s digital future, 24 July 2017)

European Commission, ‘EU Digital Identity Wallet’ (European Commission) <https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET> accessed 28 August 2025

European Commission, Directorate General for Financial Stability, Financial Services and Capital Markets Union, VVA, and CEPS, *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2).* (Publications Office 2023) <https://data.europa.eu/doi/10.2874/996945> accessed 28 August 2025

Financial Action Task Force, ‘International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations)’ (FATF 2012)

Financial Action Task Force, ‘Singapore: 3rd Enhanced Follow-Up Report & Technical Compliance Re-Rating’ (FATF 2019)

Financial Action Task Force, ‘Status of Implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity’ (FATF 2024)

Financial Crimes Enforcement Network, ‘Statement for Non-Bank Financial Institutions’ (2021)

FinTech Review, ‘Revolut Review: From Startup to Global Giant’ (*FinTech Review*, 2 April 2025) <https://fintechreview.net/revolut-scaled-from-startup-to-global-fintech-giant/> accessed 1 September 2025

Girling W, ‘Fintech Timeline: Tink’s Acquisition by Payments Leader Visa’ (FinTech Magazine, 24 June 2021) <https://fintechmagazine.com/digital-payments/fintech-timeline-tinks-acquisition-payments-leader-visa> accessed 1 September 2025

Greater Phoenix Economic Council, ‘Things to Know About Arizona’s FinTech Sandbox’ (GPEC, 8 April 2021) https://www.gpec.org/blog/things-to-know-about-arizonas-fintech-sandbox/ accessed 28 August 2025

HG Insights, ‘AWS Market Share 2025: Insights into the Buyer Landscape’ (HG Insights, 2025) <https://hginsights.com/blog/aws-market-report-buyer-landscape> accessed 3 December 2025

Hooper C, ‘Top Fraud Trends in Digital Banking for 2025 – and How to Stay One Step Ahead’ (Veriff Insights, 30 July 2025) <www.veriff.com/fraud/learn/top-fraud-trends-in-digital-banking-for-2025-and-how-to-stay-one-step-ahead> accessed 28 August 2025

International Monetary Fund, ‘E-Money: Prudential Supervision, Oversight, and User Protection’ (2021) DP/2021/027

Kelleher S, McNabola L and O’Connor J, ‘The Future of EU Payment Services Regulation – PSD3 and PSR’ (*William Fry*, 2023) <www.williamfry.com/knowledge/the-future-of-eu-payment-services-regulation-psd3-and-psr> accessed 1 September 2025

Monetary Authority of Singapore, ‘Guidelines on Outsourcing’ (2016)

Monetary Authority of Singapore, ‘Technology Risk Management Guidelines’ (2021)

PayPal, ‘Licenses’ (*PayPal*) https://www.paypal.com/us/webapps/mpp/licenses accessed 28 August 2025

Phoenix Strategy Group, ‘GDPR Checklist for Fintech Startups’ (5 July 2025) <https://www.phoenixstrategy.group/blog/gdpr-checklist-for-fintech-startups> accessed 3 December 2025

Pinot A, ‘Fintech: Friend or Foe to Anti-Financial Crime?’ (ACAMS Today, 3 June 2019) <www.acamstoday.org/fintech-friend-or-foe-to-anti-financial-crime> accessed 28 August 2025

PwC Austria, ‘PSD2 – In a Nutshell’ (2017) <www.pwc.at/de/publikationen/financial-services/psd2-nutshell-01-at.pdf> accessed 28 August 2025

Rogers J, Zappasodi A and Cook R, ‘Operational Resilience in the UK, EU and US: A Comparison’ (White & Case LLP, 2022) <www.whitecase.com/insight-our-thinking/financial-regulatory-observer-2022-operational-resilience-uk-eu-and-us> accessed 4 December 2025

Solowiejczyk N, Strauss RJ and Kirby K, ‘Bank-Fintech Partnerships Under Scrutiny: What Fintechs Need to Know About BSA/AML Expectations’ (Fenwick Insights, 29 May 2025) <www.fenwick.com/insights/publications/fintech-bank-partnerships-under-scrutiny-what-fintechs-need-to-know-about-bsa-aml-expectations> accessed 28 August 2025

Stripe, ‘Licenses’ (*Stripe*) <https://stripe.com/legal/spc/licenses> accessed 28 August 2025.

Tink, ‘How Using Data Will Help You Win More Customers and Earn More Revenue’ (3 July 2018) <https://tink.com/blog/open-banking/open-api/> accessed 1 September 2025.

TrustBuilder, ‘PSD2 and PSD3 Directive: How Are Payments Evolving in Europe?’ <https://www.trustbuilder.com/en/psd2-psd3-directive-future-payments-europe/> accessed 28 August 2025.

Valk L, ‘ComplyAdvantage Alternatives & Competitors’ (Salv, 2023) <https://salv.com/blog/complyadvantage-alternatives-competitors/> accessed 1 September 2025.