Restoring Trust in European Payment Rails: A Framework for a Shared Liability Reform

Abstract

Author: Elfriede Sixt, Chairwoman of EFRI[1]

Europe's regulator-led modernisation of payments delivered instant, low-cost rails, yet fraud losses and uneven redress have produced an online payment paradox. We identify a double gap: first, deception-induced payments are treated as "authorised" and typically unreimbursed; second, even clearly unauthorised cases face fragmented enforcement and inconsistent outcomes across Member States.

Drawing on 1,750 pig butchering victim cases across 20 countries (€62.5 million in losses) and a validated survey cohort, we show how today's liability rules misalign incentives along the payment chain and enable recurring gatekeeping failures.

Crucially, the current EU Council's narrow draft, limited to PSP Impersonation, violates the Union's long-standing promise that digitalisation would deliver equivalent or better consumer protection across payment channels. Based on our work, we propose a redefinition of consent for (all) fraud-induced payments to establish an outcome-based reimbursement right for APP fraud; liability aligned with functional control (the payer's ASPSP as the reimbursement anchor with calibrated recourse); a binding EU-level ADR (FIN-NET 2.0); a Union Fraud Data Framework; and technology duties (real-time analytics, kill switches, cross-sector intelligence sharing) for the banks and payment companies..

Two PSR landings are realistic. Only the broader version, with full reimbursement for fraud-induced payments, creates the incentives for all participants in the scam chain (sending and receiving PSPs, acquirers, telecoms and platforms) to invest in necessary prevention and to internalise the costs of failure.

Absent an outcome-based reimbursement regime covering the entire scam chain, with the payer's ASPSP as reimbursement anchor and calibrated recourse, the single market will cement an equilibrium that rewards institutions and harms consumers. It will erode trust in the financial system and in public institutions, weaken democratic legitimacy, and create conditions in which cybercrime thrives.

Keywords: Payment fraud; Authorised Push Payment (APP); Authorised Push Payment Fraud (APP fraud); PSD1, PSD2; PSR, PSD3, PSR Article 59; Consumer protection; Liability

[11] Elfriede Sixt, Austrian Certified Public Accountant, Co-Founder and Chairwoman of the European Funds Recovery Initiative (EFRI), a not-for-profit consumer protection organisation registered in Vienna, Austria. EFRI supports victims of online fraud.

framework; ADR/FIN-NET; Regulatory enforcement; EFRI dataset; Comparative liability frameworks (UK/Singapore/Australia), FinTech regulation, consumer protection, digital transformation, and regulatory enforcement.

Content

List of Abbreviations

Abbreviation	Meaning
ACCC	Australian Competition and Consumer Commission (hosts NASC)
ACMA	Australian Communications and Media Authority
ADR	Alternative Dispute Resolution
AFCA	Australian Financial Complaints Authority
APP	Authorised Push Payment
ASCom	Anti-Scam Command (Singapore Police Force)
ASPSP	Account Servicing Payment Service Provider
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (DE supervisor)
BGB	Bürgerliches Gesetzbuch (German Civil Code)
BGH	Bundesgerichtshof (German Federal Court of Justice)
CFPB	Consumer Financial Protection Bureau (US)
CHAPS	Clearing House Automated Payment System (UK)
CNP	Card-not-Present
CoP	Confirmation of Payee (also: VoP – Verification of Payee)
DNB	De Nederlandsche Bank (NL supervisor)
EBA	European Banking Authority
ECB	European Central Bank
ECSP	Electronic Communications Service Provider
EDR	External Dispute Resolution (Australia)
EECC	European Electronic Communications Code
EFRI	European Funds Recovery Initiative
EFTA	Electronic Fund Transfer Act (US)
EMI	Electronic Money Institution
EUPG	E-Payments User Protection Guidelines (Singapore)
FCA	Financial Conduct Authority (UK)
FIDReC	Financial Industry Disputes Resolution Centre (Singapore)
FIN-NET	EU network of financial ADR bodies
FOS	Financial Ombudsman Service (UK)
FPS	Faster Payments System (UK)
FTC	Federal Trade Commission (US)
IBAN	International Bank Account Number
IMDA	Infocomm Media Development Authority (Singapore)
IPR	Instant Payments Regulation (EU)
MAS	Monetary Authority of Singapore
MCC	Merchant Category Code
MiFID	Markets in Financial Instruments Directive
MLaaS	Money-Laundering-as-a-Service
NASC	National Anti-Scam Centre (Australia)
NCA	National Competent Authority
OCCRP	Organized Crime and Corruption Reporting Project

OCHA	Online Criminal Harms Act (Singapore)
ODR	Online Dispute Resolution (EU platform; repealed 2024)
OSA	Office of Servicemember Affairs (CFPB)
OWiG	Gesetz über Ordnungswidrigkeiten (DE Act on Regulatory Offences)
PSD1	First Payment Services Directive (2007/64/EC)
PSD2	Second Payment Services Directive (2015/2366/EU)
PSD3	Third Payment Services Directive (proposal)
PSP	Payment Service Provider
PSR	Payment Services Regulation (EU proposal)
PSU	Payment Service User
QEG	Qualified Entities Act (Austria)
RAD	Representative Actions Directive (EU)
Reg E	Regulation E (implements EFTA in the US)
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SCT Inst	SEPA Instant Credit Transfer
SEPA	Single Euro Payments Area
SMS	Short Message Service
SPF	Scams Prevention Framework (Australia)
SRF	Shared Responsibility Framework (Singapore)
STR	Suspicious Transaction Report
TILA	Truth in Lending Act (US)
TPP	Third-Party Provider
VoP	Verification of Payee (see CoP)
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme (NL AML law)

1. Introduction: The Electronic Payments Protection Gap

1.1 The Promise of European Digital Finance

Over the past two decades, Europe has pushed one of the most ambitious policy-led transformations of financial infrastructure in modern history. Unlike sectors where digitalisation developed through market forces, payments have been reshaped by sustained regulatory strategy and investment.

From the creation of the Single Euro Payments Area (SEPA) in 2008[2] to the adoption of the first and second Payment Services Directives (2007/64/EC[3] and 2015/2366[4]) (PSD1 and PSD2) and the launch of real-time payments rails under the Instant Payments Regulation (IPR)[5] in 2024, European regulators have not only supported modernisation of the financial systems, they have actively driven it. The vision has been consistent: a unified, borderless payment space that reduces transaction costs, accelerates settlement, supports economic modernisation, and positions Europe as a global standard setter in financial technology.

The European Commission's Digital Finance Strategy (September 2020) made this ambition explicit[6]: to establish the EU "as a global standard-setter for digital finance while ensuring that innovation and competition serve consumers and businesses." This strategy crowns more than a decade of coordinated regulatory action to accelerate electronic payments adoption across the financial sector.

1.2 Measurable Outcomes of Europe's Payments Reform

The outcomes are striking by any quantitative measure. Payment transactions across the euro area are now transparent within seconds in 20 European countries, a dramatic shift from the days when cross-border credit transfers could take several business days. Since its 2017 launch, the SEPA Instant Credit Transfer scheme (SCT Inst)[7] has expanded continuously and processes millions of transfers daily with settlement typically under ten seconds.[8] With the IPR taking full

[2] European Central Bank (ECB), "SEPA goes live – official launch of the single euro payments area" (press release, 21 January 2008), https://www.ecb.europa.eu/press/pr/date/2008/html/pr080121.en.html, last accessed 25 August 2025.

[3] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC [2007] OJ L 319 1–36.

[4] 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 [2015] OJ L 337 35–127.

[5] Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro [2024] OJ L 2024/886, 19 March 2024.

[6] European Commission, Digital Finance Strategy for the EU' COM(2020) 591 final (24 September 2020) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591.

[7] European Payments Council (EPC), SEPA Instant Credit Transfer (SCT Inst) (scheme webpage), https://www.europeanpaymentscouncil.eu/what-we-do/sepa-instant-credit-transfer, last accessed 25 August 2025.

[8] European Payments Council, "Launch of the SCT Inst scheme – Press Kit" (November 2017), https://www.europeanpaymentscouncil.eu/news-insights/news/epc-launches-sepa-instant-credit-transfer-scheme, last accessed 25 August 2025.

effect, PSPs in euro-area Member States must offer receiving instant euro credit transfers by 9 January 2025 and sending by 9 October 2025 (with later deadlines for non-euro Member States).[9]

The scale shows up in system-level throughput. In the second half of 2023, 34 retail payment systems in the euro area processed roughly 51.8 billion transactions with a combined value of €25 trillion.[10] Instant credit transfers accounted for about 16% of the number and 4% of the value of all credit transfer transactions, evidence of rapid adoption with a significant economic footprint.[11]

Digital usage has scaled accordingly. Eurostat reports[12] that in 2024, about 72% of EU internet users used online banking, while 93% of adults used the internet, together implying approximately 67% of all adults used online banking[13].

At this level of penetration, abstaining from electronic payment rails is, for all practical purposes, no longer feasible in ordinary life in the modern West.

Digitalisation has also transformed bank economics. Industry research attributes material efficiency gains to straight-through processing and automation, with estimated cost reductions (up to approximately 30%), profitability improvements (approximately 20%), and sharp error-rate reductions (on the order of around 85%).[14][15][16] While the exact magnitudes vary by institution, the direction of travel is clear: banks and payment companies have captured and will continue to capture substantial benefits from the shift to digital operations.

---

[9] Regulation (EU) 2024/886 of 13 March 2024, amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro, Art 5a(8) (euro-area PSPs: receive by 9 January 2025; send by 9 October 2025; non-euro PSPs: receive by 9 January 2027; send by 9 July 2027), [2024] OJ L 2024/886.

[10] European Central Bank, 'Payments statistics: second half of 2023' (Press release, 25 July 2024), https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2023_1~10a5662f81.en.html, last accessed 28 August 2025.

[11] European Central Bank, "Payments statistics: second half of 2024**"** (Press release 23 July 2025), https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2024h2~5ada0087d2.en.html, last accessed 24 August 2025.

[12] Eurostat, "Digitalisation in Europe – 2025 edition" (interactive publication 29 April 2024), https://ec.europa.eu/eurostat/web/products-interactive-publications/w/ks-01-25-000, last accessed 25 August 2025.

[13]Eurostat, "People online in 2024" (News release 17 December 2024), – 93% of people aged 16–74 used the internet in 2024. Together with footnote 9, this implies ~67% of all adults used online banking in 2024 (author's calculation), https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20241217-1, last accessed 25 August 2025.

[14] McKinsey & Company, "How banks can boost productivity through simplification at scale" (13 March 2025), https://www.mckinsey.com/industries/financial-services/our-insights/how-banks-can-boost-productivity-through-simplification-at-scale, last accessed 25 August 2025.

[15] McKinsey & Company, The 2023 McKinsey Global Payments Report' (18 September 2023), finds that modernising payments technology can reduce operating costs by ~20–30% https://www.mckinsey.com/industries/financial-services/our-insights/2023-2024-global-payments-report, last accessed 25 August 2025.

[16] McKinsey & Company, "Rewired to outcompete" (20 June 2023) – estimates ~20% EBIT improvement from robust digital programs, https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/rewired-to-outcompete, last accessed 25 August 2025.

1.3 The Broken Promise of Consumer Protection

Beneath these gains lies a persistent contradiction. The policy promise, repeated in EU strategies and legislation, has been that online payments would provide the same or better consumer protection than traditional finance. PSD1 and PSD2 embed this commitment, as do the Digital Finance Strategy[17] and the Retail Payments Strategy[18] (both September 2020), which frame consumer trust as essential to a thriving digital economy.

Yet Europe faces a growing crisis of consumer confidence, driven by payment fraud, which includes both unauthorised transactions (such as account takeovers through compromised credentials) and authorised push payment, also called APP fraud, where increasingly sophisticated social-engineering tactics induce payment transactions. According to the 2024 Payment Fraud report established jointly by the European Central Bank (ECB) and the European Banking Authority (EBA), covering the period July 2022 up to June 2024, total fraud losses related to payment instruments in the euro area are material (approximately €4.3 billion for 2022 and around €2 billion in H1 2023).[19]

For unauthorised payment transactions - those executed without the payer's consent - PSD2 provides clear rules: immediate refund (Art 73) and a €50 maximum payer liability, except for cases of fraud or gross negligence (Art 74).[20] However, in practice, payment service providers (PSPs) often deny or delay reimbursements, cite the "authorised" status of the transactions, or broadly allege gross negligence of the PSU. This discrepancy between legal rules and actual implementation reveals structural weaknesses in the regulatory framework and supervisory enforcement.

In contrast, for transactions authorised through social engineering (APP fraud), losses are currently borne exclusively by the payment service users (PSU). Financial institutions and payment companies (PSPs) generally reject refund requests because there is no regulatory obligation to reimburse in these cases.

1.4 The Empirical Foundation

This study builds on comprehensive empirical work by the European Funds Recovery Initiative (EFRI). Between 2019 and 2024, EFRI documented the experiences of more than 1,750 investment-scam victims from 20 mainly European countries. Victim narratives, payment records, and supporting documentation provide a detailed view of payment fraud's scale, patterns, and consequences.

The methodology extends beyond individual accounts. Using documents provided by victims and materials from criminal case files, the research traces financial flows and examines the

[17] European Commission, 'A Digital Finance Strategy for the EU' COM(2020) 591 final (24 September 2020) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591.

[18] European Commission, 'on a Retail Payments Strategy for the EU' COM(2020) 592 final (24 September 2020) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0592.

[19] European Central Bank, 'ECB and EBA publish joint report on payment fraud' (Press release, 1 August 2024) https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.en.html, last accessed 25 August 2025.

[20] PSD2, Art 73–74 (Directive (EU) 2015/2366, OJ L 337/35, 23.12.2015).

functioning of redress mechanisms across civil and criminal avenues. This combined evidence set (EFRI dataset 2019-2024) shows where, how, and why redress fails in practice.

1.5 The Institutional and Regulatory Failure: A Multi-Dimensional Crisis

The data reveal multi-layered failure points across the full consumer protection chain, involving PSPs, dispute-resolution bodies, supervisory authorities and law enforcement/civil judicial systems.

Payer's PSPs[21]: Victims always turn first to their account servicing payment service provider (ASPSP) upon discovering they have been scammed. In the vast majority of cases, assistance is limited or refused. Disputed transfers are characterised as "authorised" and non-refundable even when payments were induced by sophisticated impersonation or coercion, or denials rest on expansive readings of gross negligence.

Alternative dispute resolution (ADR): Although FIN-NET and national ombudsman schemes exist, awareness and accessibility across Europe remain low.[22]

Supervision and oversight: Appeals to National Competent Authorities (NCAs), both in the victim's home state and the beneficiary bank's jurisdiction, for enforcement on money laundering rules, as well as on misinterpretation of gross negligence by the supervised PSPs, are rarely effective. In our dataset, supervisory intervention requests were consistently dismissed, ignored, or delayed. PSD2's rules on unauthorised transactions are not enforced; broader duty-of-care obligations are not operationalised.

Criminal enforcement actions: National law enforcement agencies and criminal courts lack the resources to handle high numbers of victims and the cross-border complexity of online fraud. Investigations, when opened, do not translate into timely victim restitution. Cross-border criminal units like Eurojust and Europol are administrative units and not accessible to victims.

Civil litigation efforts: A small subset of victims pursue civil claims against their ASPSPs and or the beneficiary PSP. They face well-resourced defendants and judicial attitudes that confine a payment service provider's obligations to execution, recognising a broader duty of care only in exceptional "red-flag" scenarios. Litigation is slow, costly, and uncertain.

In summary, PSPs deflect responsibility; supervisory bodies seldom enforce rules; ADR mechanisms are obscure or ineffective; and criminal or civil avenues rarely provide restitution. Consequently, the economic burden of sophisticated, cross-border online fraud is systematically shifted onto individual consumers.

1.6 The Economic Justice Imperative

The present allocation of loss violates fundamental principles of fair risk-sharing. Those who benefit most from digitalisation, such as financial institutions, payment companies, and social media companies, have been able to externalise the largest portion of fraud costs to consumers.

[21] We use the term Payer's PSP interchangeably with the term account servicing payment service provider (ASPSP).

[22] European Commission, "About FIN-NET" (webpage, n.d.), https://finance.ec.europa.eu/consumer-finance-and-payments/retail-financial-services/financial-dispute-resolution-network-fin-net/about-fin-net_en, last accessed 1 September 2025.

With little direct financial exposure in APP fraud cases, incentives to invest in prevention, friction, and consumer-facing safeguards are weakened.

Experience from the treatment of unauthorised payment transactions and with chargeback systems from card regimes suggests the opposite dynamic: when liability sits with the financial industry, providers invest in stronger authentication, monitoring, and user communication, and unauthorised fraud falls. The absence of comparable, enforceable liability for APP fraud has left a protection gap that criminals exploit.

In short, the same technologies that deliver efficiency and profitability to firms also introduce vulnerabilities.

A coherent liability framework, paired with credible enforcement, ensures those risks are internalised by the actors best placed to manage them.

1.7 The Human Cost Beyond Financial Loss

The impact extends well beyond monetary harm. Victims frequently experience sustained psychological distress, anxiety, depression, and trauma, compounded by denial of redress and secondary victimisation during complaint handling. EFRI's analysis indicates that a large majority report persistent anxiety or insomnia; many exhibit depressive symptoms; and a significant minority require clinical or pharmaceutical interventions.

Social consequences are common. More than half of victims report negative reactions from family, friends, or colleagues, reinforcing isolation and blame. These patterns underscore that payment fraud is not merely a financial offence; it is a public-health and social-welfare concern with lasting effects.

1.8 Loss in Trust

Systemic failure to protect victims erodes confidence not only in individual providers but in the enforcement and regulatory architecture itself. In EFRI's evidence, 39% of victims terminated long-standing relationships with their original account servicing payment service provider following the experience; many reduced their use of online channels and methods. Similar patterns appear in other studies, like in a study done by Gethe et al. (2023) that surveyed 60 victims of digital-payment fraud in India and found that 28% reduced their use of online payments after an incident (with 8% reverting entirely to cash).[23]

When consumers observe authorities declining to enforce clear legal obligations, they question the integrity of the entire framework intended to safeguard them. The resulting trust deficit risks

[23] Gethe/Ruangmei, A Study on Modes of Digital Payment Systems – Analysis of Frauds Occurring through Digital Payment Systems, Int. Research J. of Modern Engineering, Technology and Science (July 2023) (DOI: 10.56726/IRJMETS42773) (accessed 25 July 2025), https://www.irjmets.com/paperdetail.php?paperId=42773, last accessed 25 August 2025.

a vicious cycle: lower adoption, higher friction, and a drag on Europe's competitiveness. Addressing this requires not just better rules on paper, but enforcement that works, timely remedies, clear presumptions and timelines, accessible ADR with binding outcomes, supervisory transparency, and sanctions that change behaviour.

2. Empirical Analysis of Victimisation in Cyber-Enabled Crime and Payment Fraud

2.1 Research Methodology and Data Collection

EFRI is a not-for-profit organisation founded in Vienna, Austria, in early 2019 to support European consumers affected by online investment fraud. Between 2019 and 2024, EFRI documented 1,750 individual fraud cases across 20 countries, with total reported losses exceeding €62.5 million. These transfers resulted from five large-scale investment fraud schemes, commonly referred to as "pig butchering scams".[24]

Fraud Systems	**Victims**	**Loss**	**Prosecution**
Lenhoff/Wolf of Sofia (i.e. Xtraderfx, Option888, Tradovest)	650	€22 million	Scammers identified
Blue Trading	225	€11million	No prosecution
ALGOTECH/BEALGO	110	€4.5 million	No prosecution
Kayafx/Kontofx	190	€9.5 million	Scammers identified
ASIA Scams	145	€15.5 million	No prosecution

According to EFRI dataset, approximately €57.6 million of the scammed amounts (losses) were transferred to the scammers via so-called "authorised" payment transactions[25] (credit transfers, Card-not-Present (CNP) transactions), and an additional €4.9 million through unauthorised payment transactions.

EFRI's activities during the past five years included supporting the victims in filing criminal complaints, collecting victim data and payment slips, analysing the fraud schemes, studying criminal court files, and investigating the role of financial intermediaries and regulated entities in processing fraud-related transactions. In selected cases, the organisation has provided victims with legal and procedural support. EFRI has filed criminal complaints against financial institutions and payment companies, showing up in multiple fraud cases. EFRI has approached NCA's and ADRs in different countries and asked for enforcement actions. Although operating independently of public institutions, EFRI has cooperated with law enforce-

[24] Pig butchering scams are long-con investment frauds that begin with prolonged social-engineering "grooming" (often via romance or friendship), then move victims onto convincing fake trading/investment platforms to induce repeated, escalating authorised push payments; the scheme ends with a "slaughter" phase where withdrawals are blocked and victims are pressed for final "tax/fee" payments before funds are laundered through banks, EMIs, and crypto rails. See FBI, *Operation Level Up* (accessed 25 August 2025) (describing "cryptocurrency investment fraud, also known as pig butchering," in which scammers groom victims online, induce escalating deposits into bogus platforms, and then block withdrawals); FinCEN, *Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"* (8 September 2023; accessed 25 August 2025); U.S. SEC, Press Release 2025-63, *SEC's Anti-Fraud Public Service Campaign Warns Investors About Relationship Investment Scams* (14 May 2025; accessed 25 August 2025); INTERPOL, *INTERPOL urges end to "Pig Butchering" term, cites harm to online victims* (17 December 2024; accessed 25 August 2025

[25] The victims authorised the payment transactions as cybercriminals tricked them into believing that the transferred money would be invested in risk-free, profitable investments on their behalf.

ment authorities in several jurisdictions. As of 31 March 2025, EFRI was designated a qualified entity under Section 1 of the Austrian QEG[26] (Qualified Entities Act) established in line with Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020, on representative actions for the protection of the collective interests of consumers, and is now authorized to initiate cross-border class actions.[27]

EFRI's operational work has been complemented and academically validated by independent research conducted by Martin Grasel, a senior official with the Cybercrime division of the Austrian Criminal Intelligence Service (BKA), for the University of Applied Sciences in Wiener Neustadt. Grasel's study, titled *Cyber-Trading-Fraud – Viktimisierungsmerkmale bei Internet-Anlagebetrug*, aimed to identify common victimisation patterns associated with internet-based investment fraud (also known as Cyber-Trading-Fraud). The analysis was based on a survey conducted in late 2023. Martin Grasel was the lead investigator in the Wolf of Sofia criminal case.[28]

A total of 420 victims registered with EFRI were invited to participate in the online survey via email and existing victim chat groups orchestrated by EFRI, with reminder messages. The final response rate was 176 participants, of which 152 responses were largely complete and usable. Most participants came from German-speaking countries, Germany, Austria, and Switzerland, accounting for nearly 80% of the total. The questionnaire was administered in both German and English, depending on the victim's language, and the findings were evaluated accordingly.

The data are not population-representative; they reflect self-reported experiences of victims who engaged with EFRI. Potential limitations include selection and recall bias, incomplete documentation in some cases, and cross-country comparability constraints.

2.2 Fraud Scheme Characteristics and Evolution

Empirical analysis reveals that contemporary payment fraud, encompassing all hacking, phishing, spoofing, or deceptive acts targeting payment service users to unlawfully obtain funds, has evolved into a highly sophisticated and industrialised form of transnational crime. Among these, online investment fraud, particularly the pig butchering scams, stands out for its complexity, scalability, and devastating impact on victims. These scams are characterised by professional victim recruitment, sustained psychological manipulation, deceptive digital infrastructure, and seamless integration with global financial systems.[29][30]

[26] Approval for EFRI to become a qualified entity as of 31 March 2025 (official notice, available via EFRI).
[27] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (Text with EEA relevance) OJ L 409, 4.12.2020, pp. 1–27.
[28] EFRI, "Gal Barak – 'Wolf of Sofia' sentenced to 4 years in prison in Vienna, Austria" (blog article, 1 September 2020), https://efri.io/news/gal-barak-wolf-of-sofia-sentenced/, last accessed 25 August 2025.
[29] US-China Economic and Security Review Commission, "China's Exploitation of Scam Centres in Southeast Asia" (Report, July 2025), https://www.uscc.gov/research/chinas-exploitation-scam-centers-southeast-asia, last accessed 25 August 2025.
30 Council of Europe, Octopus Conference 2023 – Main Session 3 (summary report) – noting UNODC's characterisation of pig butchering as a "complex form of fraud with global impact", https://www.coe.int/en/web/octopus/octopus-conference-2023, last accessed 25 August 2025.

Victim Recruitment and Initial Engagement**:** Modern investment fraud schemes employ highly targeted victim acquisition strategies, applying data-driven advertising campaigns on platforms like Facebook, Instagram, and YouTube. As documented by both EFRI and the Organized Crime and Corruption Reporting Project (OCCRP),[31] fraudsters invest substantial resources in paid advertising to lure victims to fake trading platforms. These ads often appear indistinguishable from legitimate financial services promotions and exploit algorithms to target individuals based on age, location, interests, or recent online behaviour.

Once a potential victim clicks on such an advertisement, they are redirected to professionally designed fraudulent platforms that convincingly mimic regulated trading undertakings. These platforms include real-time price charts, secure-looking login interfaces, account dashboards showing simulated returns and display logos of the card regimes. As the Wolf of Sofia's law enforcement investigation revealed, fraud groups often license or repurpose entire software suites to build such investment interfaces, enabling them to operate hundreds of near-identical scam websites simultaneously (compare also the OCCRP report[32]).

Social Engineering and Psychological Manipulation: Communication is script-driven and sustained via messaging apps, email, and phone. Initial deposits are intentionally low (often around €250) to reduce friction. As relationships deepen, victims face staged "wins," fabricated urgency, and pseudo-regulatory events that induce progressively larger transfers. Internal coaching manuals and performance incentives for call-centre staff have been documented in case files.

Remote Access and Authorisation Exploitation: A frequent enabler for scammers is the misuse of remote-access tools (such as AnyDesk, TeamViewer). In a large share of EFRI-documented cases, victims were persuaded to install such software "for assistance", granting direct access to online banking. Fraudsters then initiated credit transfers or card transactions while maintaining the appearance of victim consent. These practices blur the line between authorisation and deception, leading PSPS to treat technically SCA-compliant transactions as "authorised," despite vitiated consent.

2.3 Victim Demographics and Vulnerability Patterns

EFRI represents 1295 male and 455 female victims; 87% of the victims registered with EFRI are older than 40 years.

Demographic Profiles: The analysis of 152 victims in Grasel's study reveals a consistent demographic profile that contradicts common stereotypes about online fraud victims. The typical victim of Cyber-Trading-Fraud (also known as pig butchering scam) is a male, aged

[31] Organized Crime and Corruption Reporting Project (OCCRP), "Behind the Scam: How Fraudsters Use Social Media, Software, and Shell Companies to Steal Millions" (blog posting, 25 June 2025). https://www.occrp.org/en/investigations/behind-the-scam-how-fraudsters-use-social-media-software-and-shell-companies-to-steal-millions, last accessed 25 August 2025.
[32] OCCRP, ibid.

between 50 and 70, with an average age of 59 years.[33] Across both language groups in the study (German and English), over 50% of participants fell into the 51–65 age range, while more than 25% were over 65. This age structure indicates that victims tend to be individuals with accumulated savings and financial reserves making them attractive targets for high-value fraud schemes.

Educational and Professional Background: The victims came from a wide range of professional backgrounds, including technically skilled professionals, public servants, entrepreneurs, retirees, and single parents

Education levels varied notably by language group: nearly half (49.1%) of German-speaking participants had completed higher school education, whereas 45.6% of non-German-speaking respondents held a university degree.[34] Approximately 20–30% in both groups had completed secondary school (Matura or Abitur), and a small percentage reported only compulsory education.

This diversity contradicts common assumptions about victim naivety or financial irresponsibility. The research demonstrates that fraud victimisation crosses educational and professional boundaries, indicating that sophisticated criminal operations can overcome even professional scepticism and financial knowledge.

Financial Mindset and Knowledge: A striking 81.3% of participants described themselves as conservative investors, with 85.9% of German-speaking and 73.2% of English-speaking respondents[35] selecting "very" or "rather" cautious investment attitudes. Simultaneously, 83% of participants self-reported having little or no financial market knowledge, particularly regarding cryptocurrencies and derivatives.

English-speaking victims reported slightly higher familiarity with digital assets; the overwhelming majority had limited technical understanding of the financial products involved.

This evidence directly contradicts the narrative of the “greedy risk-taker.” Instead, the data show that fraudsters specifically target conservative and financially less sophisticated individuals, those who would not typically engage in speculative markets. Their trust is built through persuasion, staged professionalism, and psychological manipulation.

Re-Victimisation Frequency and Gender Disparities: Approximately 40% of participants reported having been targeted by internet fraud only once, and over 60% had experienced such fraud at most twice. However, a minority indicated they had been defrauded more than three or even five times.

A significant gender difference emerged, particularly among German-speaking respondents. Two-thirds (66%) of women had been victimised only once, whereas only 32.5% of men

[33] Grasel, Martin, „Cyber-Trading-Fraud: Viktimisierungsmerkmale bei Internet-Anlagebetrug“ (Master’s thesis, Fachhochschule Wiener Neustadt 2024), 25.

[34] Grasel, *Cyber-Trading-Fraud* (2024), 26.
[35] Grasel, *Cyber-Trading-Fraud* (2024), 27.

reported the same. No female respondent in the German-speaking group had been victimised more than three times, compared to 13% of men. Among English-speaking participants, the gender distribution was more balanced, but even there, women were slightly less likely to report repeated victimisation.

Pathway to Victimisation: When asked how they became aware of the fraudulent platforms, over two-thirds cited online advertising (DE: 74.0%; EN: 67.9%).

Review websites also played a role, mentioned by 23.0% of German-speaking victims and 13.2% of non-German-speaking victims. For this question, a "Other" option with a free-text field was also provided. Some participants from both victim groups indicated that they had been contacted via telephone calls ("cold calls").[36]

Particularly notable is that over half of the respondents were not actively searching for investment opportunities at the time they encountered the fraud (DE: 68.7%; EN: 55.8%)

Among the group of respondents who were not actively searching or could not recall doing so, an even larger proportion indicated that advertising was the decisive factor (DE: 77.1%; EN: 68.6%).

2.4 Financial Impact and Loss Distribution

The financial consequences of online investment fraud are often devastating and long-lasting. Victims not only lose significant sums of money but also face fundamental disruptions to their financial stability and retirement planning. According to EFRI's database, the most significant individual loss reported was €5.2 million, while the smallest amounted to €150. The median reported loss across all EFRI-registered cases was €18,500. However, this figure conceals wide disparities:

- 25% of victims lost less than €5,000 (typically during early phases of fraud engagement),
- 50% lost between €5,000 and €50,000, often constituting major portions of lifetime savings,
- and 25% lost more than €50,000, with some cases exceeding €300,000, leading to severe financial dislocation and, in several cases, existential crises.

Grasel's study confirms these findings: in the German-speaking sample, nearly 60% reported losses up to €20,000, while in the English-speaking group, over 55% lost more than €50,000.

Only a small fraction of victims, 6.1% (DE) and 7.9% (EN), recovered any portion of their losses.[37]

Grasel's study confirmed that most of the money transferred to the scammers was funded from personal savings (DE: 90.9%; EN: 75.0%). Borrowing was common: 16.1% (DE) and 34.6% (EN) reported private or bank loans, evidence of deep manipulation and escalating

[36] Grasel, *Cyber-Trading-Fraud* (2024), 30.
[37] Grasel, *Cyber-Trading-Fraud* (2024), 31.

commitment. Many rated the harm "significant" (DE: 56.6%; EN: 44.2%); a high-loss subset described it as "existence-threatening."

Case files and survey narratives reveal a typical fraud path: (i) low-entry test (€250-€1,000); (ii) simulated profit via dashboards; (iii) major extraction (€10,000-€100,000+) via urgency and pseudo-regulatory pretexts; (iv) final exploitation at withdrawal via fictitious "taxes/fees/compliance costs."

The most cited initial motivator was a low entry amount (DE: 71.7%; EN: 53.8%), followed by high profit potential (DE: 57.6%; EN: 38.5%). Many referenced family support goals and retirement savings. Contextually, ultra-low interest rates (2016-2019) reduced returns on conservative products, making modest online "opportunities" unusually salient.

Grasel's study found that over 70% identified trust in the personal "advisor" as the key reason for additional deposits (DE: 70.7%; EN: 76.9%). Emotional dependency frequently overrode initial caution; many continued investing even after suspecting fraud, hoping to recover earlier losses.

2.5 Psychological Impact and Secondary Victimisation

Our research found that the psychological consequences for victims are significant and persistent. Respondents reported sleep disturbances, anxiety, and depressive symptoms, with a meaningful minority requiring clinical or pharmaceutical treatment. Many described long-lasting effects on trust in financial services, social withdrawal, and reduced confidence in decision-making, especially among victims with losses exceeding €20,000. Social reactions compounded the harm: over half reported blame from their social environment, their account servicing payment providers, and authorities, with comments like "should have known" or "acted out of greed," intensifying shame and isolation. This reflects secondary victimisation, where victims suffer further harm due to negative responses from others rather than the initial crime itself (see more on secondary victimisation[38]). Some victims have not disclosed to their families that they lost all their savings to scammers. Trust erosion was common, leading some to reduce or abandon online banking and online payment usage.

2.6 Re-Victimisation and Recovery Scam Phenomena

Re-victimisation is widespread in the fraud industry. A substantial share of the victims continue to receive fraudulent "recovery" offers months and years after the initial scam, purported law enforcement contacts, pseudo-law firms, or fee-for-service "asset recovery" intermediaries. 47% of the victims interviewed by Grasel (DE: 51.5%; EN: 40.4%) reported responding and making further payments[39]. Higher initial losses correlate with higher susceptibility to recovery scams. Ongoing contact attempts (DE: >70%; EN: ~50%) suggest that victim data circulates among criminal networks. These secondary schemes replicate primary-scam tactics, such as

[38] Secondary victimisation denotes further harm not from the crime itself but from the way institutions or individuals (e.g., police, courts, health services, media) respond to the victim, such as disbelief, blame, repeated questioning, or exposure to the offender. See European Institute for Gender Equality (EIGE), "Secondary victimisation" (definition), accessed 25 August 2025; Directive 2012/29/EU (Victims' Rights Directive), Recital 9 (duty to prevent secondary victimisation); and UNODC, "The right of victims to an adequate response to their needs" (examples), last accessed 25 August 2025.

[39] Grasel, Cyber-Trading-Fraud 2024, 35

urgency, authority mimicry, and staged insider access, and their prevalence points to structural failures: scarce trustworthy recovery avenues and weak institutional support.

2.7 Cross-border and International Dimensions

The evidence confirms an inherently transnational model: more than 85% of the payment transactions done by 1,750 victims involved cross-border elements (EFRI Dataset). This is in line with online criminal networks distributing functions across jurisdictions (marketing, "client service," payment processing), thereby exploiting coordination lags. EFRI's dataset and criminal court files, mainly the Wolf of Sofia investigation, document multi-layer laundering chains (rapid hops, crypto conversion, dozens of shell companies) that prevent timely freezes and hinder recovery of the stolen funds. Even when scammers are identified, assets are often beyond reach by the time criminal proceedings end, underscoring the need for faster cross-border cooperation and harmonised enforcement tools.

2.8 Conclusions from Empirical Analysis

The combined evidence from EFRI and Grasel reveals sophisticated operations that exploit psychological vulnerabilities, digital interfaces, and institutional weaknesses to result in large-scale losses for European consumers. Victim profiles challenge common stereotypes, with harm extending beyond financial losses to affect health and social functioning. The transnational nature of online fraud organisations greatly exceeds the capacity of domestic enforcement frameworks.

Importantly, the findings demonstrate that victimisation is not an individual failing, but a systemic consequence of regulatory gaps and weak redress mechanisms. These insights provide the foundation for the following chapters, which cover legal baselines, enforcement shortfalls, comparative models, and a blueprint for liability and enforcement designed to restore protection at scale.

3. Financial Industry as the Critical Enabler and the Only Effective Redress Opportunity for APP Fraud and Pig Butchering Scam Victims

Industrialised online fraud operates as a coordinated supply chain: Industrial call-centre operations design scripts and maintain ongoing manipulation of victims, software vendors license turnkey trading platforms and Customer Relationship Management (CRM) systems; performance-marketing intermediaries purchase and optimise targeted ad funnels; and Money-Laundering-as-a-Service (MLaaS) networks arrange acquiring relationships, mule-account stacks, and layered cash-out paths. However, this machinery ultimately depends on access to regulated European payment rails.

A defining feature of cyber-enabled fraud,[40] unlike most traditional crime, is that offenders cannot get hold of their gains (the victims' money) without using the payment rails of the incumbent financial industry. Even if the first hop begins in crypto or via informal channels, monetisation ultimately requires an interface with one or more licensed PSPs: acquiring banks and payment facilitators, payment processors, e-money institutions (EMIs), correspondent and Payees' PSPs, and crypto exchanges.

As a result of professional MLaaS used, the Wolf of Sofia criminal operation worked with more than four different payment gateway providers that all brought different payment channels with them (four different acquirers, 14 banks with dozens of drop accounts, 3 EMIs).

EFRI's evidence base confirms that this dependency creates multiple leverage points that are, too often, ignored or exploited.

3.1 How the Money Moves: Roles and Hand-offs in the Scam Chain

Illicit flows need to be integrated seamlessly into the legitimate financial system. To convert deception into money, scammers route payments through a dense ecosystem of intermediaries, each controlling a distinct choke-point.

Victim-side Authorisation (Payer's PSP / Card issuer / ASPSP): Fraudsters induce victims to authorise a transfer or to disclose credentials that enable an "unauthorised" debit. Where the victim authorises the payment, transactions often pass because Strong Customer Authentication (SCA) is formally satisfied, even though consent was vitiated by deception.

[40] Cyber-enabled fraud is fraud whose underlying offence could occur offline, but whose *scale, reach, speed or concealment* is materially amplified by information and communications technologies (e.g., the internet, messaging platforms, social networks, or digital payment rails). It contrasts with *cyber-dependent* crimes (which cannot be committed without ICT). Typical manifestations include phishing-led credential theft, spoofed websites, online investment/romance/BEC schemes, and e-commerce/CNP abuse, as defined in the IOCTA 2024 report from Europol, https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf, last accessed on 25 August 2025.

Merchant Acquiring / Payment Facilitation: On card and wallet rails, specialist acquirers or payment facilitators board high-risk (or synthetic) merchants, assign misleading merchant category codes (MCCs), and route large cross-border volumes. EFRI's dataset shows acquirers frequently acted as scale enablers, converting hundreds of thousands of card transfers into apparently legitimate commerce. Mis-coding (MCC camouflage), fragmented merchant IDs (MIDs), and third-party "payment orchestration" obscure the merchant's true nature.

Payee's PSPs, ASPSPs/EMIs: Victims' funds commonly land first in (cross-border) "drop accounts", accounts opened solely to receive and move stolen funds, often held by shell companies with their own International Bank Account Numbers (IBANs). Once credits arrive, they are pushed out rapidly in bursts of transfers, frequently by another cross-border transaction, followed by cash withdrawal or conversion into cryptocurrency. Although PSPs are expected to detect such typologies through transaction-monitoring systems, our evidence shows recurring failures: large amounts exceeding €100,000 leaving soon after arrival, payments to brand-new recipients, unusually high-value transfers, and frequent transfers to jurisdictions with elevated money-laundering risk.

Layering and cash-out (MLaaS): MLaaS specialists work with multiple payment gateway providers, choreograph merchant arrangements, mule networks, account stacks, and crypto on/off-ramps to layer and dissipate funds. Their business model depends on negligent or tolerant PSPs and on predictable non-enforcement.

3.2 MLaaS: the industrial Supply Chain of Fraud Monetisation

Modern scam syndicates outsource collection and laundering to MLaaS specialists who (i) arrange acquiring for sham "investment" or "education" merchants, (ii) operate mule accounts and shell companies across jurisdictions, (iii) move proceeds through layered bank/EMI/crypto paths, and (iv) sell "compliance theater" (plausible websites, invoices, MCC narratives) to pass onboarding checks. In EFRI's dataset and the Wolf of Sofia criminal court files, MLaaS appears as a dedicated capability with explicit price lists, revenue-sharing, and premiums for top-tier bank names.

MLaaS providers rely heavily on the negligence, or, at times, the willing cooperation of licensed PSPs and processors to access and move funds across regulated rails. We use the term financial crime enablers (FCEs) to denote actors who facilitate financial crime, whether deliberately or through negligence. FCEs are critical to execution and concealment by providing infrastructure, services, or legal coverings that allow fraudsters to operate and evade enforcement. The set of potential enablers includes banks, PSPs, payment companies, FinTechs, and crypto exchanges that, knowingly or not, make it easier for cybercriminals to launder funds and re-enter the legitimate financial system.

3.3 Channel Opacity in Payment Rails: Accountability Leakage by Design

Channel opacity refers to the limited visibility and lack of transparency that consumers, supervisors, and even counterpart payment service providers (PSPs) have regarding the actors, hand-offs, and controls involved between payment initiation/authorisation and final cash-out in online transactions. Understanding the four-party system of a simple Card Present transaction requires specialised knowledge, and even more expertise is needed to grasp the many intermediaries involved in a single CNP payment. Terms such as payment gateway provider, payment facilitator, acquirers, and issuers, key players in online card payments, are unfamiliar to most retail investors and law enforcement personnel.

In practice, multiple layers of intermediation (merchant acquirers, payment facilitators, sponsor banks, EMIs/virtual IBANs, orchestration gateways) obscure the actual counterparty and spread risk information across disconnected silos. This creates a "black box" that weakens fraud prevention and leads to “responsibility gaps” after losses occur.

Importantly, this lack of transparency is deliberate: it allows criminal organisations to scale their operations. For prevention, opacity hides anomaly signals that only become useful when combined across institutions. For redress, it creates evidentiary asymmetry, critical data needed to identify the “least-cost avoider” (such as alerts, Know Your Customer (KYC), Know Your Customer’s Customer (KYCC), Enhanced Due Diligence (EDD) files, velocity flags, and freeze attempts) are scattered across private logs inaccessible to victims and Alternative Dispute Resolution (ADR) bodies. This systematically delays case triage, frustrates recall efforts, and enables institutional denials unsupported by end-to-end facts.

3.4 Gatekeeping Failures observed in EFRI Cases (mapped to duties)

Across fraud systems the EFRI dataset identified, recurring failure modes included: (1) onboarding high-risk merchants with obvious fraud signals; (2) mis-coding of MCCs to hide risk; (3) inadequate EDD for shells; (4) absence of risk-based warnings/friction for atypical victim-side transfers; (5) failure to hold or recall suspect credits; and (6) pass-through patterns at beneficiary banks that transaction monitoring should flag. These map directly to legal obligations (KYC, KYCC/EDD), ongoing monitoring, and anomaly response that PSD2 and the Regulatory Technical Standards(RTS)[41] make technology-neutral, and that national Anti-Money Laundering (AML) laws (such as the Dutch Wwft[42]) operationalise.

[41] Regulatory Technical Standards (RTS) are a set of rules and guidelines established by the European Banking Authority to ensure that banks and other financial institutions comply with the regulations set out in the Second Payment Services Directive (PSD2), https://en.cubemos.com/sustainabilityglossary/regulatory-technical-standards-rts, accessed 25 August 2025.

[42] The Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft) entered into force on 1 August 2008. The Wwft provides a comprehensive set of measures to prevent the use of the financial system for money laundering or terrorist financing. The Wwft was changed in 2020 to implement the EU’s changed Fourth Anti-Money Laundering Directive. https://www.dnb.nl/en/sector-information/open-book-supervision/laws-and-eu-regulations/anti-money-laundering-and-anti-terrorist-financing-act/introduction-wwft/, accessed 25 August 2025.

Case studies: Regulated European payment companies as financial crime enablers

Across the dataset, EFRI observed a non-random pattern at the monetisation layer: although different criminal organisations ran front-end scams, the same small set of payment companies and crypto-asset exchanges repeatedly appeared as counterparties willing to accept the risk. This recurrence reflects institutional choices, risk appetite, onboarding and monitoring standards, rather than any inevitability of the rails. Equally, it demonstrates that participation is avoidable: many banks, processors and exchanges are largely absent from these flows, consistent with stricter KYC/EDD, MCC governance, and beneficiary-side controls. The evidence thus supports the conclusion that fraud enablement is contingent, not inevitable, and it strengthens a liability model that places default responsibility on institutions that choose to intermediate high-risk flows, with calibrated rights of recourse.

Acquiring at scale, as seen with the European payment companies Payvision BV, Amsterdam (see Section 3.4.1) and Wirecard AG, Munich (see Section 3.4.2), did not merely process fraud proceeds; it legitimised and amplified them. On the beneficiary side, Københavns Andelskasse, Copenhagen and Deutsche Handelsbank AG, Munich, enabled industrial-volume pass-through of stolen funds.

3.4.1 Payvision B.V., Amsterdam, ING Group, The Netherlands

Payvision B.V. was founded in 2002 and licensed as a Dutch payment institution in 2012. In March 2018,[43] ING Bank N.V. (in charge: Steven van Rijswijk) acquired a 75% stake at a valuation of €360 million. During 2018, it became public knowledge that Payvision has acted as a payment gateway provider and acquirer for high-risk merchants for many years.

In October 2021[44], ING Bank N.V. announced it would phase out Payvision's acquiring/PSP activities; the wind-down was completed in 2022. According to their press material, Payvision connected over 300 business partners with 5,000 web merchants and processed over 100 million transactions annually.[45]

EFRI's victim documentation and the Wolf of Sofia criminal court files show that Payvision acted as an acquirer for fraudulent binary options/forex networks tied to Gal Barak and Uwe Lenhoff, Algotech/Bealgo, as well as 24option alongside Wirecard AG (see below). Documents sourced from Payvision's own records attribute approximately €154 million of processed CNP volume to the Wolf of Sofia criminal organisation alone.

[43] ING, "ING completes acquisition of majority stake in Payvision" (press release 13 March 2018), https://www.ing.com/Newsroom/News/Press-releases/ING-completes-acquisition-of-majority-stake-in-Payvision.htm, last accessed 26 August 2025.
[44] ING, "ING phases out Payvision" (press release 28 October 2021), https://www.ing.com/Newsroom/News/ING-phases-out-Payvision.htm, last accessed 26 August 2025.
[45] Sunset, "What Happened to Payvision & Why Did It Fail"? (blog post 25 January 2025), https://www.sunsethq.com/blog/why-did-payvision-fail, last accessed 25 August 2025.

In its late-2019 money-laundering complaint to De Nederlandsche Bank (DNB),[46] EFRI documented in detail that Payvision B.V. approved and continued processing for high-risk merchants despite apparent fraud red flags, including offshore shell structures, conflicted or opaque UBO arrangements, the absence of MiFID licences, and public warnings from supervisory authorities.

The complaint further evidenced that, during ongoing monitoring, pronounced chargeback spikes and renewed supervisory warnings were neither appropriately escalated through enhanced due diligence/risk-committee channels nor remediated by effective measures (such as freezing, suspension, or off-boarding), contrary to basic AML/CTF and card-scheme control expectations.

As a large-scale acquirer, Payvision B.V. converted illicit "investment" schemes into ordinary card transactions by providing access to Visa/Mastercard rails, conferring legitimacy by using misleading MCCs, enabling frictionless cross-border collection, and materially increasing reach and volume.

Following a formal complaint by DNB in 2020, a criminal investigation found that from 2016 through April 2020, Payvision's customer due diligence was systematically inadequate: identity and ultimate beneficial owner (UBO) checks were insufficient; the purpose and intended nature of relationships were not properly established; and ongoing monitoring was ineffective. In April 2024, the Dutch Public Prosecution Service (Openbaar Ministerie) issued penal orders totalling €330,000, fining two former directors (Rudolf Booker and Cheng Liem Li) for structural violations of the Wwft, explicitly reproaching Payvision's failure as a gatekeeper.[47]

3.4.2 Wirecard AG, Munich, Germany

The case of the German Wirecard AG illustrates how a regulated European payment company turned into a central facilitator of large-scale consumer fraud and laundered hundreds of millions, if not billions, of stolen money for transnational criminal organisations, similar in function to Payvision.

While the Wirecard group presented itself as a leading German fintech success story, criminal investigations later revealed its systemic role in processing payments for fraudulent online trading platforms, binary options brokers, and other high-risk merchants. Already in early 2020, EFRI filed a detailed money laundering complaint with German prosecutors and Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin),[48] documenting that Wirecard processed hundreds of millions of euros in consumer payments linked to online investment scams and associated boiler rooms.

[46] European Funds Recovery Initiative (EFRI), "Our criminal complaint against Payvision B.V. and its former management!" (blog post), https://efri.io/our-criminal-complaint-against-payvision-b-v-and-its-management/, accessed 25 August 2025.
[47] Openbaar Ministerie, „Geldboetes voor voormalig bestuurders betaaldienstverlener vanwege tekortkomingen bij het bestrijden van witwassen," https://www.om.nl/actueel/nieuws/2024/04/05/geldboetes-voor-voormalig-bestuurders-betaaldienstverlener-vanwege-tekortkomingen-bij-het-bestrijden-van-witwassen, accessed 25 August 2025.
[48] European Funds Recovery Initiative, "EFRI's Wirecard money laundering complaint" (blog post, 31 January 2020), https://efri.io/efris-wirecard-money-laundering-complaint/, accessed 25 August 2025.

The complaint highlighted that Wirecard's acquiring units and subsidiary networks acted as deliberate facilitators, providing payment connectivity and legitimacy to criminal schemes that would otherwise have been excluded from regulated financial systems. The collapse of the Wirecard group in 2020,[49] following the exposure of a €1.9 billion balance-sheet fraud, underscored not only massive internal misconduct but also the failure of the German supervisory authorities to recognise and halt Wirecard's function as a global fraud enabler.

Summarising, Payvision B.V. and the Wirecard case show that acquirers can be critical amplifiers in fraud monetisation. When gatekeeping fails (weak KYC/EDD, MCC masking, poor monitoring), scams can collect hundreds of thousands of card payments quickly. ING's 2021–2022 wind-down of Payvision and the bankruptcy of Wirecard underscore the reputational cost of prolonged control failures.

For victims of online investment fraud, Payvision and Wirecard did not act as neutral service providers: by onboarding and processing for high-risk merchants despite clear red flags, they facilitated the cross-border movement of victims' funds into opaque networks.

3.4.3 Københavns Andelskasse (KBH), Copenhagen, Denmark

Between 2016 and mid-2018, Københavns Andelskasse (KBH), a small Danish cooperative bank, acted as a pass-through hub for broker and pig butchering proceeds on a large scale, fed by regulated European payment companies, including Moorwand Limited, a British EMI showing up in several fraud systems in EFRI´s dataset. According to a report of the Danish Financial Supervisory Authority (Finanstilsynet; FSA), KBH processed approximately €550 million (DKK 4 billion) in suspicious transactions between October 2017 and September 2018.[50]

In 2017 alone, its transaction-monitoring system generated 5,598 alerts; only 156 were reviewed, and one suspicious activity report was filed, despite hundreds of transactions exhibiting clear risk indicators.

Following a critical on-site inspection in 2018, FSA notified the national resolution authority (Finansiel Stabilitet) that the institution was likely to fail. On 13 September 2018,[51] Finansiel Stabilitet assumed control and placed the bank into resolution; the licence was subsequently surrendered.

In January 2025, it was made public that FS Finans VI A/S (formerly KBH) accepted a fine of DKK 794,296,500 from the National Unit for Special Crime (NSK)[52] for extensive AML

[49]Reuters, "The rise and fall of Wirecard, a German tech champion", (16 March 2021), https://www.reuters.com/article/technology/timeline-the-rise-and-fall-of-wirecard-a-german-tech-champion-idUSKBN2B811J/, last accessed 25 August 2025.

[50] European Funds Recovery Institution, "The Danish FSA and its relaxed approach regarding Københavns Andelskasse" (2022), https://efri.io/the-danish-fsa-and-its-relaxed-approach-regarding-kobenhavns-andelskasse-and-clearhaus-a-s/, last accessed 25 August 2025.

[51] Finansiel Stabilitet, "Beslutning nr. 1 om afvikling af Københavns Andelskasse" (13 September 2018), https://www.finanstilsynet.dk/media/52808/11%20Beslutning%201%20%20Overtagelse%20af%20kontrol%20pdf.pdf, last accessed 25 August 2025.

[52] B.T., 'Andelskasse gav fri bane for hvidvask og får bøde på 794 millioner' https://www.bt.dk/krimi/andelskasse-gav-fri-bane-for-hvidvask-og-faar-boede-paa-794-millioner, last accessed 25 August 2025

breaches committed in 2017 up to Finansiel Stabilitet's takeover in 2018, levied by the Copenhagen City Court. The Court found that the bank lacked adequate internal controls, customer due diligence, and transaction monitoring. High-risk customers received transactions totalling DKK 3,177,185,489, and the bank failed to investigate transactions for three major customers exceeding DKK 2 billion (approximately €225 million).[53] The fine equals roughly 25% of the relevant transaction amounts. Under Denmark's bank-resolution law, such penalty claims can be written down to zero via bail-in, so FS Finans VI A/S is legally barred from paying the fine as part of the resolution.

In 2025, the former chief executive of Københavns Andelskasse, Bo Stengaard, received a four-month suspended sentence[54] for anti-money-laundering breaches committed during 2017-2018.

Both court judgements[55] found that at Københavns Andelskasse, client risk classification was deficient: customers were not appropriately risk-rated, and Enhanced Due Diligence (EDD) for foreign and other high-risk relationships was minimal or absent. Transaction monitoring and suspicious transaction reporting (STR) processes were ineffective: the volume of alerts overwhelmed the control environment, escalation pathways failed, and as a result, APP fraud proceeds were able to pass through at an industrial scale without timely intervention. Governance was misaligned: the institution's focus on providing payment accounts for foreign EMIs and PIs led to a disproportionate increase in transactional risk exposure, without a commensurate build-out of compliance capabilities or oversight, a classic failure on the beneficiary-bank side.

In summary, KBH did not just "miss" suspicious activity; it became a conduit, its beneficiary-side responsibilities (EDD, transaction monitoring, KYCC) failed at scale, enabling organised networks to exploit regulated rails. Tens of thousands of European consumers bore the resulting loss exclusively.

3.4.4 Deutsche Handelsbank, Munich, Germany

Deutsche Handelsbank, a small bank in Munich, also showed up in many fraud systems between 2016-2020 as a recurring recipient/transit point for victim funds routed via regulated European payment companies (such as PPRO Financial Limited, another FCA-regulated EMI) connected to broker and "forex/binary" schemes like 24option and the Wolf of Sofia fraud scheme.

In November 2020, the BaFin ordered[56] Deutsche Handelsbank to implement appropriate internal safeguards and to comply with general anti-money-laundering due diligence

[53] B.T. "Andelskasse gav fri bane for hvidvask og får bøde på 794 millioner, https://www.bt.dk/krimi/andelskasse-gav-fri-bane-for-hvidvask-og-faar-boede-paa-794-millioner, last accessed 25 August 2025.
[54] European Funds Recovery Initiative (EFRI), "Københavns Andelskasse: Former CEO Convicted in Denmark's AML Scandal!"(blog post 2025), https://efri.io/kobenhavns-andelskasse-former-ceo-convicted-in-denmarks-latest-aml-scandal/, last accessed 25 August 2025.
[55] National enhed for Særlig Kriminalitet (NSK), 'Københavns Andelskasse har brudt hvidvaskloven' (20 January 2025), https://politi.dk/national-enhed-for-saerlig-kriminalitet/nyhedsliste/koebenhavns-andelskasse-har-brudt-hvidvaskloven/2025/01/20, last accessed 25 August 2025.
[56]BaFin, „Deutsche Handelsbank AG: Anordnung zur Prävention von Geldwäsche und Terrorismusfinanzierung" (press release 23 November 2020), https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Massnahmen/60b_KWG_84_WpIG_und_57_GwG/meldung_201120_57_gwg_deutsche_handelsbank.html, last accessed 25 August 2025.

obligations. On 7 April 2021, the Munich Public Prosecutor's Office[57] searched the bank's premises as part of a money-laundering investigation; documentation from the Bavarian State Parliament confirms the raid. In July 2021,[58] the bank publicly announced that it would discontinue its payment services business line.

In October 2022 (published January 2023[59]), BaFin imposed two administrative fines totalling €17,500 under the German Banking Act.

In March 2023, media reports[60] stated that an investigation by the Munich I Public Prosecutor's Office resulted in a €1 million fine against Deutsche Handelsbank (nowadays: DKAM Capital AG) under § 30(4) OWiG. The prosecutor found that, between 2016 and 2020, the bank failed to implement and maintain an adequate transaction-monitoring system and to staff its anti-money-laundering function adequately.

Reliance on third-party payment service provider (PSP) pipelines exposed the bank to concentrated flows associated with fraudulent schemes. The contemporaneous records show recurring inbound credits followed almost immediately by rapid onward transfers, a pattern characteristic of classic layering in money laundering.

A beneficiary/processing bank can either stop or normalise fraud proceeds. Here, supervisory intervention plus reputational pressure eventually forced the bank to shut the highest-risk line, years after widespread consumer harm.

3.4.5 Postbank, Deutsche Bank Group, Frankfurt, Germany

Cybercriminals consistently used different branches of Postbank Germany (a subsidiary of Deutsche Bank) between roughly 2016 and 2020 as a preferred institution for opening bank accounts linked to shell companies engaged in broker fraud and investment scams (also called drop accounts). Tens of thousands of online fraud victims transferred their money to these drop accounts. EFRI's dataset (victims' payment slips) identified over 90 shell entities, each holding Postbank accounts scattered across branches in cities like Dortmund, Berlin, Cologne, Leipzig, and Nürnberg. These accounts served no legitimate business purpose: they had no operations, no employees, pure strawmen as management and no beneficial owners within Germany. Funds flowed in and out quickly, often within days, corresponding to victim money deposits and onward transfers to the operators of scam platforms like xTraderFX, BlueTrading, Safemarkets, and OptionStarsGlobal.

---

[57] Handelsblatt, „Geldwäsche-Verdacht und Strategieprobleme – Die Bank der Industriellenfamilie Reimann steckt in der Krise" (7 Juli 2021), https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/privatbank-geldwaesche-verdacht-und-strategieprobleme-die-bank-der-industriellenfamilie-reimann-steckt-in-der-krise-/27356608.html, last accessed 25 August 2025.

[58] European Funds Recovery Initiative (EFRI), "Deutsche Handelsbank closes down its payment services business (blog post July 2021), https://efri.io/deutsche-handelsbank-closes-down-its-payment-services-business/, last accessed 25 August 2025.

[59] BaFin, " Deutsche Handelsbank AG (jetzt: DKAM Capital AG): BaFin setzt Geldbußen fest" (4 January 2023), https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Massnahmen/60b_KWG_84_WpIG_und_57_GwG/meldung_2023_01_05_Deutsche_Handelsbank_AG.html, last accessed 25 August 2025.

[60] Fintelegram, Deutsche Handelsbank fined with €1 million for money laundering issues" (blog post 9 March 2023), https://fintelegram.com/breaking-deutsche-handelsbank-fined-with-e1-million-for-money-laundering-issues/, last accessed 25 August 2025.

On the beneficiary-side KYC, transaction monitoring, rapid pass-throughs to offshore recipients, recurrent high-value credits and debits, and payment references indicating "investment" purposes should have triggered immediate holds, enhanced reviews, and interdiction measures (including freezes and recall attempts). EFRI's dataset indicates consistent non-intervention despite these red flags.

Criminal records show active involvement of BaFin in addressing the issue beginning in 2018, but no effective enforcement action.

3.4.6 ING BANK N.V., Amsterdam, The Netherlands

Like Postbank Germany, the Dutch ING Bank N.V. was consistently used by cybercriminals between at least 2016 and 2020 as a preferred institution for opening bank accounts linked to shell companies engaged in broker fraud and investment scams. Shell companies with foreign ultimate beneficial owners (UBOs) and no demonstrable economic activity were able to open accounts and obtain IBANs across ING Bank N.V.'s retail branches and subsidiaries all over Europe.

Already in autumn 2018, Dutch prosecutors[61] concluded that ING Bank N.V. had systematically violated anti-money laundering (AML) obligations by failing to prevent accounts under its control from being used for money laundering and criminal transactions. The investigation documented structural deficiencies in customer due diligence, ongoing monitoring, and suspicious transaction reporting. Back in 2018, ING Bank N.V. admitted serious compliance failures and agreed to pay a record settlement of €775 million[62] to Dutch authorities to avoid criminal prosecution.

This case, as well as the Postbank case, demonstrates that even systemically essential banks, subject to intensive supervision, function for years as facilitators of illicit flows on a massive scale.

For fraud victims, the implications are stark. If Tier-1 European banks (supposedly intensely supervised) do not fulfil their anti-money-laundering obligations, criminal enterprises obtain access to payment systems and the legitimacy conferred by globally recognised institutions.

3.5 Summary of our Findings about the Actors in the Payment Channels

EFRI's dataset points to a structural dynamic: large-scale scams do not scale without failures by payment service providers. Across the cases examined, Tier-1 banks and licensed institutions enabled fraud at distinct choke-points: acquirers legitimised sham "investment" flows as ordinary card sales (Payvision; Wirecard); a cooperative bank acted as a pass-through hub (Københavns Andelskasse); a processing bank repeatedly routed victim funds through high-risk PSP corridors (Deutsche Handelsbank); and large retail groups (Deutsche Bank; ING Bank

[61] ING, "ING reaches settlement agreement with Dutch authorities on regulatory issues in the ING Netherlands business" (4 September 2018), https://www.ing.com/Newsroom/News/Press-releases/ING-reaches-settlement-agreement-with-Dutch-authorities-on-regulatory-issues-in-the-ING-Netherlands-business.htm, last accessed 25 August 2025.
[62] GMF, "Europe Needs Money Laundering Penalties That Hurt" (blog post), https://www.gmfus.org/news/europe-needs-money-laundering-penalties-hurt, last accessed 3 September 2025.

N.V.) maintained accounts for dozens of shell beneficiaries. Each failure maps to a legally recognised control, KYC/EDD, KYCC, merchant-category (MCC) governance, transaction monitoring, and freeze/recall duties. Actors in the payment chain control these specific prevention levers: onboarding KYC/EDD; merchant and transaction monitoring (including MCC governance); payee-name verification; sender-side warnings and friction; and beneficiary-side holds and recalls. EFRI's dataset documents repeated breakdowns at each control, with losses externalised to victims in authorised push-payment (APP) cases.

In APP fraud, the receiving institution often has the last clear chance to prevent the criminals from getting hold of the stolen money. When beneficiary-side controls fail, funds exit the regulated system within hours. Taken together, the cases show that enablement was not confined to marginal or under-capitalised entities but spanned the full spectrum of the European financial system, from small co-operative banks to Tier-1 institutions, and persisted amid inadequate supervision and weak enforcement for years.

4. Victim Support and Redress Experiences

Chapter 3 identified functional choke-points across banks and licensed payment institutions and illustrated enablement patterns. This chapter turns to outcomes after loss: what victims encounter when seeking help from their ASPSPs, from ADR bodies, the criminal and/or civil-justice systems, and why redress typically fails at scale. It provides the factual foundation for the liability and enforcement proposals developed in Chapters 7, 10, and 11.

A central finding in EFRI´s dataset is the extraordinarily low rate of redress across the victim samples we analysed. According to Grasel's report, only a small fraction of losses were recovered (DE: 6.11%; EN: 7.93%).[63]

These low figures reflect the combined effect of (i) ASPSPs' negative initial handling of complaints, (ii) supervisory and ADR pathways that rarely produce redress, (iii) the practical limits of cross-border law enforcement, and (iv) structural barriers to individual civil recovery.

Over five years, EFRI accompanied victims in efforts to recover losses. The following sections summarise those experiences and outcomes.

4.1 First line of Help: Victim´s Account Servicing Payment Service Providers

Most EFRI-registered victims had long relationships (often >20 years) with their account-servicing PSPs (ASPSPs). Yet initial reimbursement claims were almost uniformly rejected, both for (a) unauthorised debits arising during the fraud journey and (b) authorised push payments that were "technically authenticated" but obtained by deception. Standardised letters typically blame the victim for authorising the payment, ignoring the professional manipulation used to vitiate consent.

In APP cases, banks routinely treat formal SCA as dispositive despite sophisticated social-engineering tactics. In unauthorised cases, "gross negligence" is alleged on speculative grounds (such as that victims must have mishandled credentials)

4.2.1. Germany: Enforcement Practice and Gross Negligence Interpretation

Germany's consumer watchdog published a study at the end of October 2024[64] documenting that victims of unauthorised payment fraud are frequently left to bear losses because banks allege gross negligence, while providers' due diligence duties remain under-defined and are seldom tested in court. The dossier identifies six recurring PSP-side failures that exacerbate harm: inconsistent behaviour, unintelligible texts and processes, poor reachability in emergencies, inadequate transaction analytics, flawed technical design, and consumer-harming responses. It calls for clear statutory duties, real-time monitoring, timely blocking of suspect

[63] Grasel, *Cyber-Trading-Fraud* (2024), 35.
[64] vzbv Germany, „Banken tun nicht genug gegen Kontobetrug" (press release 14 October 2024), https://www.verbraucherzentrale.de/wissen/vertraege-reklamation/kundenrechte/der-vzbv-stellt-fest-banken-tun-nicht-genug-gegen-kontobetrug-100832, last accessed 3 September 2025.

transfers, and practical limits. The legal analysis further notes that German case law has historically required "massive suspicion" before banks must act. That monitoring for unusual activity is not treated as a binding duty, which in practice shifts the litigation burden onto consumers. Taken together, this national evidence supports our proposal to treat fraud-induced payments as unauthorised, to define gross negligence narrowly with the burden on the PSP, and to mandate operational prevention duties at the EU level, ideally supported by EBA guidelines to ensure uniform application.

After weeks or months of unproductive exchanges with fraud departments, many victims report a strained relationship with their ASPSP; a substantial share of the victims (around 40% according to EFRI´s dataset) ultimately switch banks. Very few victims report timely, risk-based warnings from their ASPSP at the moment of making unusually high, cross-border transfers.

4.2 Supervisory and ADR Routes: Limited Redress, Fragmented Accountability

Across jurisdictions, victims who escalated beyond their banks to supervisors or complaint bodies encountered four recurring features: delays, deflection (matters recast as "commercial disputes"), opacity (non-publication of key findings), and enforcement actions that did not translate into restitution. The sections below summarise EFRI's documented experiences with the Dutch, Danish, and German frameworks, distinguishing between supervision/enforcement and consumer redress/ADR.

4.2.1 The Netherlands: DNB and Payvision B.V.

From 2002 to early 2019, Payvision B.V. acted as a payment gateway provider and acquirer for international fraud networks (such as Barak/Lenhoff) (see Section 3.4.1). Despite obvious warning signals, public regulator alerts, extreme chargeback rates, and business models indicative of investment/binary fraud, merchant processing continued, and victims lost millions through this channel.

Though media reporting about Payvision's exposure began as early as summer 2018 in specialist and advocacy outlets, DNB's decisive steps came only in 2020, first by pushing for an external review, then conducting an on-site inspection in summer 2020. This lag meant that large volumes continued to be processed over regulated rails in the interim. In 2020, DNB conducted an on-site inspection and found systematic violations of core Dutch financial laws, including the Anti-Money Laundering and Counter-Terrorism Financing Act (Wwft), the Financial Supervision Act (Wft), and the Sanctions Act. The findings confirmed that fraud signals were ignored and customer due diligence (CDD) was grossly neglected. Yet, rather than immediate sanctions or licence action, the group owner (ING) proceeded to wind down Payvision's acquiring business during 2021, completing the phase-out in 2022.

The public and EFRI learned about the findings of the DNB report and the subsequent filing of a criminal complaint via Dutch media only in October 2022.[65] No public announcement was

[65] NOS Nieuws, "ING opnieuw betrokken bij witwaszaak" (14 October 2022), https://nos.nl/artikel/2448382-ing-opnieuw-betrokken-bij-witwaszaak, last accessed 25 August 2025.

made on DNB`s website about the negative inspection report or the fine, respectively. The findings of the Dutch prosecutor were not made public, nor was the public informed about what happened to Payvision B.V.´s payment institution licence.

The Dutch supervisory authority, under the leadership of Klaas Knot, has been declining requests from victims to provide the inspection report about their findings regarding Payvision B.V.'s failures required for civil proceedings against Payvision B.V. for confidentiality reasons up to today.

The Dutch case shows that enforcement arrived late relative to early media signals (2018) and, even when it did arrive (2020–2024), there was no bridge from supervision to support in restitution for payment fraud victims.

Evidently, DNB did not bother to apply the Naming-and-shaming approach[66]. Naming-and-shaming should be a core AML deterrent, with public, searchable enforcement notices that outline breach typology, scale, timelines, and governance failures, tied to board-level accountability, thereby converting reputational risk into real market discipline. Transparent disclosures enable counterparties, investors, and customers to update risk assessments, restrict correspondent relationships, and increase funding costs for chronic offenders. For victims and compliant firms, it breaks the silent forbearance and regulatory capture.

When fines alone are priced in as a cost of doing business (as it is done with AML fines right now), sunlight changes incentives: executives face personal scrutiny, remediation is trackable, and serial non-compliance becomes commercially untenable. To work, publications about wrongdoings must be swift, standardised, machine-readable, and linked to procurement blocklists and licensing reviews, so AML breaches trigger both legal sanctions and immediate market consequences.

The Dutch Ombudsman for financial services, the KiFiD Stiftung, told EFRI that they are only in charge of cases with contractual relationships between PSPs and their customers.

4.2.2 Denmark: Finanstilsynet / Finansiel Stabilitet, the Danish Financial Complaint Board, and

Between 2016 and 2018, the Danish FCA identified pervasive AML failures at KBH Andelskasse and, on 13 September 2018, notified the resolution authority that the small cooperative bank was "likely to fail," prompting control by Finansiel Stabilitet. So, since September 2018, Københavns Andelskasse (KBH) has been under bankruptcy proceedings, and any claims raised by victims/EFRI have been rejected up to today.

EFRI escalated multiple victim cases to the Danish Financial Complaint Board, Denmark's designated ADR body under Directive 2013/11/EU. In practice, victims had to file individual complaints, each with a DKK 200 fee. After more than 17 months of correspondence in

[66] Cambridge Dictionary, 'naming and shaming' https://dictionary.cambridge.org/dictionary/english/naming-and-shaming,: Naming and shaming means the activity of saying publicly that a person, company, etc. has behaved in a bad or illegal way, accessed 25 August 2025.

aggregate, the Board[67] declined to issue any decisions in the cases EFRI supported. The Board advised victims to pursue private civil actions, undermining ADR's purpose as a low-cost, expeditious remedy for consumers.

So the Danish ADR framework functioned as a procedural barrier rather than a remedy in EFRI´s effort for redress.

4.2.3 Germany: BaFin, the Postbank context and Wirecard

Hundreds of victims from across the EU who transferred life savings to accounts at Postbank and/or via Wirecard reported large volumes of complaints to BaFin. According to EFRI's records, many responses characterised the matters as private "commercial disputes" outside BaFin's remit, despite consumer protection and AML obligations, resulting in no supervisory assistance with reimbursement.

However, these supervisory tracks did not generate APP fraud restitution for individual victims. Consumers were left to pursue civil claims, a process that is slow, costly, and uncertain, while the beneficiary-bank side of transactions typically refused recalls or freezes post-factum.

In Germany, supervision acknowledged compliance problems at firms within the ecosystem but offered no practical route to reimbursement for APP victims whose funds transited German accounts.

Neither Bundesbank nor BaFin arbitration channels turned out to offer support for cross-border non-contractual payment fraud cases.

4.3 No Redress through Criminal Proceedings

Across Europe, criminal justice pathways rarely deliver meaningful redress for APP fraud victims. Police units are understaffed and underresourced, lacking specialist financial crime capacity, misclassifying complaints as "civil matters," and are overwhelmed by cross-border complexity. While cybercriminals operate transnationally, moving funds out of reach in minutes (often via crypto), victims face bureaucratic hurdles and limited prosecutorial support. Heterogeneous legal frameworks and the absence of rapid, standardised procedures for evidence and information exchange further hinder cooperation among European authorities. Mutual legal-assistance requests routinely take months or years.

Neither national law enforcement bodies nor criminal courts are equipped to manage thousands of victims in a single case, so mass joinder is impracticable. This vacuum fuels "recovery-scam" offers that exploit institutional abandonment, promising asset recovery in exchange for additional fees and personal data, thereby compounding harm.

[67] European Funds Recovery Initiative (EFRI), "Poor performance of the Danish Financial Complaint Board!"(blog post 2023), https://efri.io/poor-performance-of-the-danish-financial-complaint-board/, last accessed 25 August 2025.

Even when perpetrators are identified, arrests and extraditions frequently fail to materialise because many nations lack clear bases to prosecute transnational online fraud.

Asset freezes seldom translate into timely compensation. Distributions to victims are delayed for years, or never occur at all. For example, approximately €2 million frozen in Bulgaria in the Wolf of Sofia matter has remained immobilised since January 2019, and about €1.8 million seized in the P2P GmbH case (Sparkasse Aachen/BUNQ) from mid-2018 only began accepting claims at the end of July 2025.

Unlike the United States, where the Consumer Financial Protection Bureau (CFPB) public enforcement can be paired with restitution, the EU lacks a comparable redress infrastructure.

Regarding money laundering fines as levied on Financial Crime Enablers involved in pig butchering scams, Denmark illustrates a broader European pattern: decisive supervisory statements and even significant sanctions may occur, yet without a channel that converts findings into restitution; ADR, as implemented, proved ill-suited to complex cross-border fraud.

The sentence levied by the Dutch Prosecutor for Payvision B.V.'s long-term involvement in global scams for many years, amounting to €330.000, in no way reflected the harm done by Rudolf Booker and his colleagues to tens of thousands of European consumers.

4.4 Risky Redress Routes through National Civil Actions

Civil litigation on an individual basis remains the principal private pathway for victims seeking compensation from their ASPSPs and beneficiary PSPs.

4.4.1. The long and risky routes for individual claimants

Victims must confront well-resourced banks and processors that deploy specialist legal teams, rely on sophisticated contractual terms, and invoke statutory limitations and procedural defences. Fee exposure (including “loser pays” in many Member States), evidentiary asymmetries, and cross-border fact patterns compound this imbalance.

Addressing ASPSPs and receiving banks in national courts for missed “duty of care” obligations:

Courts in European jurisdictions tend to characterise banks and payment processors as pure executors of customer mandates rather than gatekeepers of transaction legitimacy. In this framing, echoing the logic of the UK’s *Quincecare*[68] line and analogous civil-law doctrines, the primary duty is to execute clear instructions unless the institution is on notice of fraud.

[68]Lawteacher, Barclays Bank plc v Quincecare Ltd [1992] 4 All ER 363 (QB), https://www.lawteacher.net/cases/barclays-v-quincecare-9622.php, last accessed 1 September 2025.

Absent a contemporaneous duty-triggering regulation, courts often decline to impose liability for APP fraud, even where consent was vitiated by deception.

Where liability is recognised, it typically turns on contemporaneous red flags that made fraud objectively suspect at the time of execution. Qualifying indicators include sudden changes to instructions or payees, anomalous payment patterns, unusual destinations or references (such as "investment" deposits to a first-time offshore beneficiary), or live industry alerts about active scams. By contrast, historical media reports, past misconduct, or generic reputational concerns are usually insufficient; the suspicion must relate to *present-day* dissipation of funds.

When victims go against the ASPSP or the beneficiary's PSP, the burden of proof generally rests on the victim to show that the PSP ignored red flags and failed to escalate, pause, or warn. Doing so requires granular evidence, timestamps, internal alerting, device/behavioural anomalies, chargeback ratios, and staff interactions that sit within the institution's systems. Data asymmetry and banking secrecy make this difficult; victims often need court-ordered disclosure, litigation holds, or expert reconstruction of transaction flows to meet their burden.

Even when claimants clear these hurdles, remedies are constrained by causation and contributory-negligence analyses (such as deductions where victims followed instructions from fraudsters), limitation periods, and jurisdiction/applicable-law disputes. Many cases fail on procedural grounds before reaching the merits; those that succeed tend to be fact-specific, producing refunds in narrow circumstances rather than systemic relief.

A structural reason why civil redress often fails is evidence asymmetry. Victims and many ADR bodies cannot compel timely disclosure of the end-to-end chain: onboarding files, merchant risk re-ratings, transaction-monitoring alerts, freeze/recall timestamps, and payee-identification checks. Without a standardised duty to disclose these artefacts within fixed timelines, adjudicators cannot determine which actor breached which duty. Opacity thus converts institutional non-cooperation into consumer loss. EFRI's dataset shows that where chain data are produced, liability can be located; where they are withheld, denial prevails.

Examples of recent relevant decisions in different countries are as follows:

Germany's Federal Court of Justice (BGH) clarified bank liability in multi-party credit transfers in XI ZR 327/22 (14 May 2024).[69] The Court confirmed that contracts between participating banks do not extend protective effects to third parties; instead, claims are allocated via Drittschadensliquidation. It further held that, before crediting funds, a beneficiary's PSP may owe a duty to warn its intermediary bank where a risk to the payer's interests is objectively evident. The BGH also applied the presumption of properly informed conduct (Vermutung aufklärungsrichtigen Verhaltens) to breaches of warning/notice duties in payments, easing the claimant's causation burden. Finally, in assignments arising from Drittschadensliquidation, the limitation period under § 199(1) no. 2 BGB runs by reference to the assignor's knowledge, not the injured third party's. The ruling is directly relevant to APP fraud patterns: it recognises

[69]BGH, „BGH Judgement of 14 May 2024, XI ZR 327/22",https://juris.bundesgerichtshof.de/cgi-bin/bgh_notp/document.py?Art=en&Blank=1&Datum=2024-5&Gericht=bgh&Seite=3&Sort=1&anz=236&nr=86901&pos=105&utm_souce, last accessed 25 August 2025.

potential receiving-side warning obligations and strengthens victims' ability to prove loss causation.

In the Netherlands, Dutch case law recognises a *special duty of care* of banks toward third parties. Where a bank knew or ought to have known that account activity posed serious risks to others, it must investigate and may be liable if it allows payments to proceed (the "Safe Haven" and Ponzi-fraud rulings).

Addressing receiving banks' for breach of anti-money laundering rules in Europe:

EFRI's dataset across 1,750 cases with €62.5 million in losses shows that receiving banks systematically fail at gatekeeping, particularly in onboarding and KYC, mule account detection, ongoing transaction monitoring, and the timely stopping and recall of suspicious transfers. But private civil liability cannot be grounded in anti-money-laundering statutes in Europe. AML obligations are public-law compliance duties (supposedly) enforced by supervisors, not consumer-facing rights. Across European jurisdictions, courts rarely treat AML rules as protective statutes for individual payers, and alleged AML deficiencies therefore do not translate into a private damages claim. This enforcement design leaves victims with weak leverage in civil litigation against the beneficiary's banks, even when receiving-side gatekeeping failed.

Summarising national civil actions is structurally ill-suited to APP fraud that exploits harmonised rails and cross-border execution. Identical scams should not depend on individual Member State procedures for outcomes. Adequate protection must therefore be anchored at Union level, with predictable reimbursement rules and binding redress that mirror the cross-border nature of both fraud and Europe's payment infrastructure.

4.4.2. Collective mechanisms still have severe failures.

The EU Representative Actions Directive (RAD, Directive (EU) 2020/1828)[70] enables injunctive and redress actions by qualified entities (QEs), with cross-border standing subject to independence criteria and a demonstrable 12-month track record of consumer protection activity. The Commission's EC-REACT platform[71] facilitates information exchange. Still, material constraints remain: cross-border actions are generally opt-in, domestic opt-out (where available) does not extend across borders, funding requirements are stringent, and key conflict rules under Brussels I (Recast) and Rome II in mass cross-border harm are unsettled in practice.

4.5 Rejection Results in huge Re-Victimisation Numbers

When supervisory and ADR avenues are ineffective, opaque, slow, or non-binding, the system externalises resolution costs onto victims. The proliferation of fraudulent "asset-recovery"

[70] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (Text with EEA relevance) [2020] OJ L 409, 4 December 2020, 1–27.

[71] European Commission, EC-REACT (Representative Actions Collaboration Tool), "Cross-border qualified entities", https://representative-actions-collaboration.ec.europa.eu/cross-border-qualified-entities, last accessed 25 August 2025.

operators is not merely a downstream criminal adaptation; it is a predictable market response to an institutional vacuum. Where victims are denied timely reimbursement, clear guidance, or a credible pathway to redress, they face acute information asymmetries and psychological pressure that increase their susceptibility to secondary exploitation. In this sense, re-victimisation is best understood not as a matter of individual imprudence but as a structural outcome of institutional non-assistance: had consumers been provided with rapid triage, a credible refund process, and authoritative counselling after the initial fraud, the demand for fraudulent recovery services would be minimal. This mechanism links post-incident abandonment directly to the emergence of a lucrative secondary market that monetises despair and uncertainty.

4.6 Effective Redress must be Anchored at the European Level

Summarising, national legal systems are not designed to provide effective remedies in large-scale cross-border fraud cases. The scams themselves operate transnationally, exploiting harmonised payment infrastructures such as SEPA credit transfers, instant payments, or international card networks. Yet victims seeking redress are forced into fragmented national civil procedures, where outcomes vary dramatically by jurisdiction. This incoherence creates the paradox that two victims of the same fraud, executed over the same payment rail, face entirely different remedies depending solely on their Member State of residence. Such fragmentation undermines the principle of a single European payments market and weakens consumer trust. Fraudsters exploit these divergences deliberately, channelling transactions through jurisdictions with weaker enforcement or slower courts. As a result, national civil litigation is not only prohibitively costly and time-consuming but conceptually ill-suited to address a structurally cross-border phenomenon. Effective redress must therefore be anchored at the European level, aligning liability with the infrastructure through which the fraud was executed, rather than with the nationality or residence of the victim.

5. The Crisis of Institutional Legitimacy in Payments

The empirical evidence documented in Chapters 2–4 reveals not merely isolated cases of consumer harm but a systemic crisis of institutional legitimacy that threatens the foundations of European digital finance. Online Fraud victims consistently encounter abandonment at every institutional level: banks deny liability, regulators avoid enforcement, and alternative dispute resolution bodies impose procedural barriers without delivering remedies.

This pattern erodes consumer confidence in payment services, undermining the reliability and inclusiveness that the Euro system deems essential to maintaining trust in the euro.[72] Drawing on sociological theories of trust and legitimacy,[73] this chapter argues that institutional failure transcends operational inadequacy. Instead, it constitutes a violation of fiduciary responsibility[74] that recasts trusted actors as adversaries. The consequences extend far beyond individual losses, generating a systemic erosion of legitimacy that undermines the very foundation of digital economic development.

The institutions entrusted with consumer protection have, paradoxically, become enablers of exploitation. Banks benefit from the cost savings of electronic and digital payment rails while systematically denying protection to victims of sophisticated criminal operations. Regulatory authorities, despite legal mandates to ensure consumer protection, often exhibit inertia or selective enforcement. ADR bodies, intended for accessible redress, frequently impose procedural and resource burdens that exhaust victims without delivering remedies.

5.1 Financial Industry Betrayal: From Trusted Partners to Consumer Adversary

The financial industry's response to payment fraud provides the most visible evidence of institutional failure. Empirical data from EFRI show that 97% of legitimate reimbursement claims are initially rejected, suggesting not random errors but a coordinated industry practice of denial (EFRI dataset). These denials are often issued within 48 hours, relying on template responses that blame victims for "negligence," regardless of the sophistication of the fraud schemes. However, it is not only the rejections of the ASPSPs; it is, above all, the active involvement of the financial industry in the scam chain, as evidenced by EFRI's dataset, which results in a loss of trust among consumers in the financial industry.

Several cases illustrate this betrayal vividly. Payvision B.V., a subsidiary of one of Europe's biggest banks (ING Bank N.V.) in the Netherlands, facilitated over €154 million in fraudulent CNP transactions for organised crime networks between September 2015 and January 2019, despite overwhelming red flags. Københavns Andelskasse in Denmark processed more than

[72] European Central Bank, *Study on the payment attitudes of consumers in the euro area (SPACE)* (December 2020) https://www.ecb.europa.eu/pub/pdf/other/ecb.spacereport202012~bb2038bbb6.en.pdf

[73] Mayer/Davis/Schoorman, An Integrative Model of Organisational Trust, *Academy of Management Review* 20(3) (2012) 709–734; Luhmann, Familiarity, Confidence, Trust, in Gambetta (ed), *Trust: Making and Breaking Cooperative Relations* (1988).

[74] Boatright, Fiduciary Duties and the Shareholder–Management Relation, *Business Ethics Quarterly* 10(1) (2000) 33–51.

€550 million in suspect credit transfer transactions, ignoring more than 5,500 alerts in 2017 alone. Deutsche Handelsbank in Germany routinely onboarded high-risk payment service providers that were linked to fraud schemes. Postbank branches in Germany maintained accounts for more than ninety shell companies tied to broker scams between 2016 and 2020. Together, these cases demonstrate that the financial industry prioritises profit and client acquisition over consumer protection.

5.2 Regulatory Capture: The Complete Abdication of Consumer Protection

The failure of regulatory authorities to fulfil their legal consumer protection duties and to enforce the rules represents an even more profound betrayal of public trust, given their explicit legal mandate to enforce consumer protection[7576] and to enforce compliance with financial sector rules. The systematic abdication of these responsibilities has not only allowed banking industry misconduct to persist but has also exacerbated consumer harm by adding further layers of institutional neglect (EFRI dataset).

Evidence shows that regulatory capture operates through multiple mechanisms. In APP cases, evidence shows that liability is routinely shifted onto consumers: the EBA/ECB report[77] records that payment service users bore 86% of losses from fraudulent credit transfers in H1 2023, a pattern at odds with PSD2's consumer-protection allocation of liability for unauthorised transactions to PSPs. This illustrates documented awareness of systemic legal infringements combined with failure to implement effective corrective measures. National Competent Authorities dismiss consumer complaints without substantive review, routinely reclassifying them as "commercial disputes," which signals institutionalised strategies rather than mere resource or legal constraints.

Authorities consistently fail to share information with consumers or coordinate enforcement on regulatory requirements (AML rules, PSD2 rules for unauthorised payments), enabling both banks and criminals to exploit jurisdictional arbitrage. These patterns reflect not capacity limitations but strategic avoidance, amounting to a de facto conspiracy with the industry against consumer interests.[78]

Despite having the legal authority to investigate and sanction systematic non-compliance, many NCAs chose to refrain from exercising these powers. Such regulatory passivity undermines the credibility of the enforcement regime and perpetuates regulatory gaps exploited by financial institutions.

Claims of non-existent jurisdictional limitations, obstacles created through procedural complexity, and de facto coordination with industry actors foster an environment of minimal enforcement while maintaining the façade of regulatory oversight.

---

[75] European Commission, *Commission Staff Working Document: Impact Assessment Report* accompanying the Proposal for a Regulation on payment services in the internal market and amending Regulation (EU) No 1093/2010 and the Proposal for a Directive on payment services and electronic money services in the internal market (Brussels, 28 June 2023) SWD(2023) 231 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023SC0231.

[76] Coffee, J. C. Jr., Failing to Prevent Financial Misconduct in Banks (2020) (SSRN Working Paper).

[77] European Central Bank and European Banking Authority, 2024 Report on Payment Fraud (1 August 2024) 25–26, Chart 19 ("majority of losses … borne by the PSU (86% in H1 2023)")

[78] Dal Bó, Regulatory Capture: A Review, *Oxford Review of Economic Policy* 22(2) (2006)

5.3 Alternative Dispute Resolution: The Illusion of Consumer Redress

The European Alternative Dispute Resolution (ADR) framework was constructed through the ADR Directive (2013/11/EU)[79] and ODR Regulation (524/2013), establishing what appeared to be a comprehensive consumer protection infrastructure. The ADR Directive aimed to "provide individuals and traders with access to a simple, fast and low-cost method of dispute resolution." This should result in a high level of consumer protection, boosting consumers' confidence in the internal market, and should contribute to the proper functioning thereof.

The FIN-NET[80] - also set up with the ADR Directive - is a network of national alternative dispute resolution (ADR) bodies responsible for handling consumer complaints in financial services. Its purpose is to facilitate cooperation between these bodies when a consumer from one EEA country has a dispute with a financial service provider in another country, promising efficient cross-border resolution mechanisms that would enable consumers having issues to seek redress regardless of jurisdictional complications.

For payment fraud victims, this framework theoretically provides multiple avenues for relief when banks may systematically deny reimbursement claims.

National financial ombudsmen were positioned as accessible alternatives to costly litigation for consumer–bank disputes (with cross-border cases coordinated via FIN-NET), whereas the EU Online Dispute Resolution (ODR)[81] platform was designed to route consumer–merchant disputes from online purchases, domestic and cross-border, to ADR bodies, not to handle payment-services complaints.

In practice, however, ADR has never lived up to this promise: EFRI's empirical research reveals the profound gap between ADR promises and payment fraud realities. Among the 1,750 documented fraud victims, only 185 approached their domestic ombudsman due to bank rejection of support. The low number can be explained by the systematic invisibility and inaccessibility applied. Most fraud victims remain unaware of ADR options despite legal obligations for the financial industry requiring institutional disclosure. Payment Service Providers (PSPs) fulfil these obligations through formalistic notifications buried in terms and conditions rather than meaningful consumer education.

None of EFR´s victims obtained any meaningful relief through ADR processes, representing a 100% failure rate for the most vulnerable consumers seeking institutional protection.

This failure is not accidental but systemic. European ADR in financial services suffers from structural weaknesses. FIN-NET comprises around 60 schemes across 27 countries. However, across the broader EU ADR landscape, only about 20% of entities issue outcomes binding on both parties, while 64% are non-binding, and trader participation is generally voluntary.[82] Capacity and resource gaps persist, with significant differences in expertise, resources and

[79] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), *OJ L 165, 18.6.2013, pp. 63–79.*

[80] European Commission, About FIN-NET (see footnote 19).

[81] Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) *OJ L 165, 18.6.2013, pp. 1–12.*

[82] Arbitro Bancario Finanziario (Bank of Italy), 'Fin-Net' ("Fin-Net currently has 60 members in 27 countries…") https://www.arbitrobancariofinanziario.it/abf/fin-net/index.html?com.dotmarketing.htmlpage.language=3, last accessed 3 September 2025, European Parliament Research Service (EPRS), *EU framework on alternative dispute resolution for consumers* Briefing (14 February 2024) 2 (around 430 entities; 20% binding on both parties; 64% non-binding; trader participation generally voluntary), https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757788/EPRS_BRI(2024)757788_EN.pdf, last accessed 3 September 2025.

independence across Member States; uptake remains low and trader engagement uneven.[83] Moreover, strict 90-day timelines, only extendable for "highly complex" disputes, push many schemes towards simpler cases and away from complex, cross-border fraud.[84] In practice, the result is uneven compliance and under-use, making ADR too often a symbolic process rather than an adequate remedy.[85]

Procedural design further undermines victims' trust in institutions. Institutions typically have 90 days to resolve complaints, but complex fraud disputes often extend to nine months or more. EFRI's experience with the Danish Financial Ombudsman illustrates the systematic inadequacy of existing mechanisms for payment fraud cases. After providing comprehensive evidence of Københavns Andelskasse's involvement in processing hundreds of millions of euros in fraud proceeds over two years, the ombudsman, after 18 months, declined jurisdiction and referred the matter to civil courts, precisely the expensive, time-consuming process that ADR was designed to avoid.

Banks exploit these delays to exhaust victims financially and emotionally, pressuring them into abandoning claims or accepting unfavourable settlements. Victims are also forced to bear the burden of proof, a nearly impossible task in sophisticated international fraud cases where evidence lies within the institutions themselves. Hidden costs and bureaucratic hurdles add further barriers, effectively excluding older or less technically literate victims from participation.

The European Commission has acknowledged these failures but continues to pursue cosmetic reforms. It's October 2023, and the ADR reform proposal, along with the June 2025 Council-Parliament agreement,[86] promised improvements in scope and enforcement. However, the reforms preserve the voluntary compliance model, meaning institutions can still ignore unfavourable decisions. Moreover, the repeal of the ODR Regulation in November 2024 and the planned discontinuation of the ODR platform in July 2025[87] symbolise retreat rather than progress in cross-border consumer protection. For fraud victims, these measures represent form rather than substance, an institutional theatre of redress without meaningful outcomes.

For payment fraud victims, these reforms offer cosmetic improvements rather than meaningful protection. Enhanced reporting obligations and mandatory response timelines cannot address fundamental problems when institutions can ignore unfavourable decisions without consequence.

---

[83] BEUC, "*Modernising Consumer ADR in the EU",* (15 December 2023) 5–8 (structural differences in capacity, expertise, resources; under-use; trader reluctance), https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-164_Modernising_Consumer_ADR_in_the_EU.pdf, last accessed 3 September 2025.

[84] Directive 2013/11/EU, art 8(e)/art 9 (90-day completion; extension for "highly complex" disputes) OJ L 165, 63–79; Sacha Voet (European Commission study), *ADR Report – Final* (2022) 157–160 (90-day limit incentivises "easy cases" over complex ones), https://commission.europa.eu/system/files/2022-08/adr_report_final.pdf, last accessed 3 September 2025.

[85] EPRS, *EU framework on ADR* (14 February 2024) 4–6 (under-use; complex national landscapes; low awareness; uneven trader compliance with outcomes depends on legal effect and monitoring). https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757788/EPRS_BRI(2024)757788_EN.pdf, last accessed 3 September 2025.

[86] Council of the EU, "Consumer protection: Council and Parliament reach a deal to modernise ADR rules" (press release, 26 June 2025), https://www.consilium.europa.eu/en/press/press-releases/2025/06/26/consumer protection-council-and-parliament-reach-deal-to-modernise-adr-rules/, last accessed 25 August 2025.

[87] Regulation (EU) 2024/3228 of the European Parliament and of the Council of 19 December 2024 repealing Regulation (EU) No 524/2013 and amending Regulations (EU) 2017/2394 and 2018/1724 (discontinuation of the European ODR Platform).

5.4 The Erosion of Social Trust and Its Consequences

The failures of banks and payment companies, supervisory authorities, and dispute resolution mechanisms do not merely affect individual victims; they create a systemic erosion of social trust that threatens the legitimacy of Europe's financial institutions and regulatory frameworks. Trust is not a peripheral element of economic systems, but the very foundation upon which financial intermediation rests. When consumers lose confidence that institutions will protect them, the broader social contract underpinning digital finance is destabilised.

The visible pattern of abandonment has systematically undermined consumer confidence. Victims who discover that their ASPSPs deny responsibility, that regulators fail to enforce their legal rights, and that dispute resolution systems lead nowhere are forced to conclude that the financial system itself is stacked against them. This loss of trust extends beyond the immediate experience of fraud: it raises fundamental questions about whether European financial institutions are reliable custodians of consumer welfare.

The psychological harm caused by this betrayal is profound. Victims frequently report that the denial of redress was more traumatic than the fraud itself. The reasoning is clear: while being deceived by criminals is painful, the abandonment by trusted institutions destroys the very assumption of reciprocity and protection that makes participation in a financial system possible. This "secondary victimisation" produces long-term trauma, often requiring psychological or psychiatric treatment, and fundamentally reshapes how victims view financial institutions.

Social isolation compounds this psychological harm. Fraud victims often withdraw from social participation out of shame or fear of renewed exploitation. Their reluctance to use online banking or electronic/digital payment systems not only reduces their own access to modern financial services but also influences their communities. Family members and peers who witness such experiences adopt defensive attitudes toward online payments, amplifying distrust across generations. What begins as individual disillusionment results in collective scepticism toward financial innovation and digital transformation.

This erosion of trust has cascading social and economic consequences. It slows digital adoption rates, creates resistance to innovation, and undermines public support for EU-led initiatives in financial modernisation. In this way, institutional failures in protecting fraud victims directly weaken Europe's competitiveness and its political project of building a single, trusted digital market.

5.5 The Economic Consequences of Institutional Failure

The direct financial costs to victims are devastating. EFRI's dataset documents €62.5 million in losses across 1,750 cases, but this represents only a small fraction of actual damages across Europe. Many victims report that legal costs exceed the fraud losses themselves, as they seek support from law firms; some are forced into private litigation against well-funded banks. Healthcare costs are equally significant: more than one-third of victims require psychiatric or pharmaceutical intervention, two-thirds experience chronic sleep disorders, and more than four-fifths exhibit symptoms of clinical depression. These externalised costs place a heavy burden on national healthcare systems that were never designed to absorb the fallout of financial system failures. Beyond direct healthcare and litigation costs, institutional abandonment also produces indirect costs. Victims suffering from trauma or financial devastation often lose productivity,

withdraw from the labour market, or depend on social welfare. Governments and taxpayers absorb these costs, effectively subsidising institutional negligence.

Internationally, the perception of weak consumer protection deters investment. Venture capital and technology firms prefer jurisdictions where predictable liability frameworks and credible redress mechanisms create stability. Europe's inability to guarantee such protection signals higher legal risk and lower consumer adoption rates, creating a competitive disadvantage. As a result, capital and talent gravitate toward markets with stronger institutional accountability, such as the UK or Singapore.

5.6 The Enablement of Criminal Enterprise

Institutional failure does not merely harm victims; it supports organised crime. Weak enforcement of AML duties lets fraud proceeds pass through regulated channels, and the rarity of sanctions creates a low-risk environment in which networks expand, internationalise, and diversify. EU-level coordination failures, fragmented mandates, slow or incomplete information-sharing, and bureaucratic barriers mean freezes and recalls arrive too late; once stolen, funds are seldom recovered. The same vacuum fosters a lucrative "recovery-scam" industry. A robust enforcement architecture with clear post-incident pathways would crowd these actors out. The result is a perverse alignment: institutional inaction provides criminals with infrastructure while victims lack effective remedies. Fraud is transnational, yet Europe's consumer protection architecture remains fragmented; criminals, and, at times, payment companies exploit jurisdictional arbitrage by routing flows through Member States with weaker enforcement or lower liability routes.

5.7 The Breach of Democratic Accountability

The systematic failure of European institutions to enforce consumer protection rules is not merely a technical deficiency; it represents a fundamental breach of democratic accountability.

Legislators explicitly mandated consumer protection under PSD2 and related frameworks. Yet regulatory authorities consistently refuse to enforce these mandates. This refusal constitutes more than institutional weakness: it is an act of institutional resistance against the will of elected bodies. When supervisory/enforcement authorities ignore statutory obligations, they undermine both the rule of law and the democratic legitimacy of European governance.

Regulatory and supervisory bodies are funded by taxpayers and entrusted with protecting the public interest. Yet these resources are often redirected to serve the financial industry interests through minimal enforcement and opaque consultation processes dominated by industry voices. In effect, citizens fund institutions that prefer private profit over public welfare.

Transparency failures deepen this crisis. NCAs refuse to publish data on enforcement activities, withhold compliance monitoring results, and deny access to audit findings even when consumer harm is evident (such as the Dutch DNB with the Payvision B.V. inspection report). Without transparency, democratic oversight becomes impossible. The public cannot evaluate institutional performance, and regulators cannot hold supervisory authorities accountable.

The result is an accountability vacuum. When consumers cannot rely on institutional protection, when legislators' mandates are ignored, and when transparency is absent, democratic governance itself is undermined.

6. The Scale and Financial Impact of Payment Fraud and Pig Butchering Scams

Payment fraud has reached an unprecedented scale across major economies. Sophisticated scams such as pig butchering show a paradigm shift from technical intrusion to psychological exploitation. Data from the EU, UK, US, Singapore, and Australia illustrate both the magnitude of losses and the difficulties of producing reliable, comparable statistics.

6.1 Europe: ECB/EBA Data and Limitations

The most comprehensive data for the European Union emerges from the joint Payment Fraud Report published by the European Central Bank (ECB) and the European Banking Authority (EBA) on 1 August 2024. This collaborative analysis documented payment fraud losses involving primary financial instruments, including credit transfers, payment cards, direct debits, electronic money transactions, and cash withdrawals, totalling approximately €4.3 billion in 2022, with an additional €2 billion recorded during the first half of 2023.[88] These figures represent the result of semi-annual reporting mechanisms implemented across payment service providers throughout the EU/EEA region.

However, interpretation of these European figures requires scrutiny due to several methodological limitations that significantly affect their reliability and comparability. Data quality issues, including incomplete submissions from reporting entities and potential misclassifications of fraud types, introduce uncertainties that may necessitate retrospective corrections. Moreover, the harmonised comprehensive coverage framework only became operational from the first half of 2022,[89] constraining the ability to establish meaningful historical comparisons. Methodological divergences[90] from previous reporting frameworks, particularly regarding fraud definitions and analytical scope, further complicate efforts to identify long-term trends. The current analysis[91] encompasses only three semi-annual reporting periods, making long-term trend projections methodologically unsound. Additionally, the predominant aggregation perspective focuses on issuing institutions[92], potentially obscuring other analytical dimensions that could yield more profound insights into fraud patterns and prevention strategies.

[88] European Central Bank and European Banking Authority, *2024 Report on Payment Fraud* (1 August 2024) 5, 9.
[89] ECB/EBA, 2024 Report on Payment Fraud, 7 ("full coverage of EU/EEA countries only applies for reference period H1 2022 onwards"). See also Annex "Scope of the data," 33 (reference periods H1 2022, H2 2022, H1 2023).
[90] ECB/EBA, 2024 Report on Payment Fraud, 7 (caution in comparisons due to "substantial differences in terms of data source, reporting methodology, the scope and content of the collected information, and the geographical coverage").
[91] ECB/EBA, 2024 Report on Payment Fraud, 7 ("only covers three reporting periods… caution should be exercised when attempting to interpret trends over time"); Annex "Data limitations and qualifications," p. 34 ("Due to the short time series…").
[92] ECB/EBA, 2024 Report on Payment Fraud, 8 & n. 3 ("figures for card payments are generally derived from an issuing… perspective; acquiring perspective only in some cases").

6.2 Other jurisdictions: UK/US, Australia, Singapore

Unlike the EU, other jurisdictions provide granular data broken down by fraud typology, offering insights into criminal adaptation and regulatory responses. The UK Finance Annual Fraud Report for 2024, published in June 2025, recorded total payment fraud losses of £1.17 billion (for around 70 million inhabitants) in the United Kingdom throughout 2024[93], virtually unchanged from the preceding year. This stability masks significant compositional shifts within fraud categories, with unauthorised fraud encompassing payment cards, remote banking, and check-related losses totalling £722 million. In comparison, APP fraud accounted for around £460 million in losses.[94]

Investment scams constitute a particularly significant component of UK APP fraud, accounting for nearly one-third of all APP fraud losses in 2024. Their evolution demonstrates a troubling trend: losses increased by 34% even as the number of reported cases declined to the lowest level since 2020.[95] This inverse relationship between case volume and total losses indicates a systematic shift toward high-value targeting, with criminals either becoming more selective in victim profiling or generating substantially larger returns per scheme.

The United States presents an even more dramatic picture of fraud-related financial losses. Federal Trade Commission (FTC) data recorded consumer losses exceeding $12.5 billion (for around 350 million inhabitants) in 2024, a 25% increase over the previous year.[96] Notably, 38% of fraud reports in 2024 involved actual financial losses, compared with 27% in 2023, underscoring the heightened effectiveness of fraudulent schemes.[97] Investment scams dominated the American landscape, generating $5.7 billion in reported losses (+24% year-on-year) and ranking as the single largest fraud category. Imposter scams followed with $2.95 billion in losses.[98] From a payment-methodology perspective, bank transfers and cryptocurrency transactions generated higher losses than all other methods combined, reflecting fraudsters' strategic reliance on irreversible channels that complicate recovery and frustrate law enforcement.

In Singapore, a jurisdiction once regarded as one of the most secure financial hubs globally, losses have escalated dramatically. The Singapore Police Force documented 51,501 scam cases in 2024, with aggregate losses exceeding S$1.1 billion (€737 million) (for around 6 million inhabitants), a 70.6% increase compared to 2023[99]. The average reported loss per incident

[93] UK Finance, Annual Fraud Report 2024 (June 2025), https://www.ukfinance.org.uk/system/files/2025-05/UK%20Finance%20Annual%20Fraud%20report%202025.pdf, accessed 25 August 2025.
[94] UK Finance, "Annual Fraud Report 2024"
[95] UK Finance, "Annual Fraud Report 2024"
[96] Federal Trade Commission (USA), New FTC Data Show Big Jump in Reported Losses to Fraud: $12.5 Billion in 2024 (press release, March 2025), https://www.ftc.gov/news-events/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024, accessed 25 August 2025.
[97] Federal Trade Commission (USA), New FTC Data Show Big Jump in Reported Losses to Fraud: $12.5 Billion in 2024 (press release, March 2025), https://www.ftc.gov/news-events/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024, accessed 25 August 2025.
[98] Federal Trade Commission (USA), New FTC Data Show Big Jump in Reported Losses to Fraud: $12.5 Billion in 2024 (press release, March 2025), https://www.ftc.gov/news-events/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024, accessed 25 August 2025.
[99] Singapore Police Force, Mid-Year and Annual Scam Statistics 2024 (2025), https://www.police.gov.sg/Media-Room/News/Mid-Year-and-Annual-Scam-Statistics-2024, accessed 25 August 2025.

reached S$14,503, while four mega cases alone accounted for more than one-fifth of the total annual damage. Investment fraud and pig butchering scams were key drivers, reflecting the migration of industrial-scale fraud networks into Asian countries.[100]

Australia has likewise witnessed a surge in fraud, although coordinated interventions have already produced some mitigation. According to the National Anti-Scam Centre's Targeting Scams Report,[101] Australians reported combined losses of AU$2.03 billion (€1.1 billion) (for around 27.2 million inhabitants) in 2024, down 26% from AU$2.7 billion in 2023. Despite the decline, investment scams remained the category with the highest figures, accounting for approximately AU$945 million[102] in reported losses.

These country reports not only quantify losses but also provide detailed fraud taxonomies, allowing policymakers to track the evolution of specific scam types.

6.3 Europe's Underreporting Problem

The European figures appear remarkably conservative when compared against data from other advanced economies, particularly considering the EU's substantially larger population base (around 450 million inhabitants) and payment transaction volumes. The unreasonableness of these figures not only limits comparability but also undermines evidence-based policymaking at the EU level.

So right now, Europe operates in what can only be described as a statistical vacuum. Unlike the UK, the US, and Australia, the EU lacks harmonised public data on APP fraud or its sub-categories, such as investment scams, romance scams, or impersonation fraud. The ECB/EBA reports obscure which typologies drive the majority of losses.

European data should therefore be treated as a conservative baseline rather than a comprehensive representation of actual incidence.

This payment fraud data deficit is compounded by fragmented law enforcement reporting. Member States apply divergent definitions, maintain incompatible statistics, and in many jurisdictions, victims cannot even file an online fraud report. The absence of harmonised, accessible, and digital reporting channels means that large numbers of victims remain invisible to official statistics. The result is systemic underreporting and a lack of typological clarity.

Without a harmonised European fraud taxonomy and digital reporting channels, victims remain statistically invisible.

[100] Singapore Police Force, Mid-Year and Annual Scam Statistics 2024 (2025), https://www.police.gov.sg/Media-Room/News/Mid-Year-and-Annual-Scam-Statistics-2024, accessed 25 August 2025.
[101] National Anti-Scam Centre (NASC), *Targeting scams: report of the NASC on scams data and activity 2024* (11 Mar 2025), Foreword p. 1 ("$2.03 billion … a 25.9% decrease from 2023"); Key statistics p. 3 & Table 1 ("$2.7 billion in 2023; $2.0 billion in 2024").
[102] National Anti-Scam Centre (NASC), *Targeting scams 2024*, "At a glance" p. 2 (Top-5 by loss; Investment $945.0 m); also Table 3 p. 4 (combined losses by category confirming $945.0 m)

6.4 Human and Social Impact

Beyond aggregate statistics, the immediate and most devastating impact of payment fraud is borne by victims themselves. Many lose their life savings, are forced to remortgage homes, or postpone retirement. EFRI's case evidence repeatedly documents existential crises resulting from higher-figure losses. The financial harm comes with long-lasting psychological trauma: victims frequently experience anxiety, depression, and social withdrawal, often intensified by feelings of shame and secondary victimisation when institutions deny redress. These harms extend into family life, eroding trust within personal networks and isolating victims from their communities.

These individual tragedies reveal why APP fraud has become one of the most critical and rapidly expanding consumer risks worldwide. Losses are now measured in billions annually, with investment fraud models, particularly pig butchering scams, accounting for the largest share of financial damage. The human and social costs, therefore, represent not only private misfortune but a systemic challenge to public trust in digital finance.

7. PSD1/PSD 2: An Inadequate Liability Framework for the Digital Age

7.1 The Historical Context of European Payment Protection

The evolution of the existing liability framework in Europe reflects broader trends in financial regulation, technological development, and consumer protection policy. Understanding the historical context is essential for appreciating both the achievements and the limitations of the current framework, especially where the original legislators never anticipated new threat vectors.

Before the adoption of harmonised payment-services legislation with PSD1, European consumers faced a highly fragmented legal landscape, also for unauthorised payment transactions. Member States took markedly different approaches to liability allocation, reimbursement timelines, evidentiary burdens, and preventive controls.

This fragmentation produced **four** systemic problems.[103] **First,** it enabled regulatory arbitrage: criminals and high-risk intermediaries could route activity through jurisdictions with weaker rules or enforcement. **Second**, it created consumer uncertainty: cross-border users often encountered inconsistent and even contradictory protections for the same type of transaction. **Third**, it distorted competition: payment service providers faced divergent compliance costs and liability exposures depending on where they operated, which in turn discouraged pan-European offerings. **Fourth**, it erected innovation barriers: firms had to navigate multiple incompatible regimes, slowing the deployment of new payment technologies and business models.

The European Commission recognised early that consumer confidence would be decisive for the Single Euro Payments Area (SEPA)[104] and for broader economic integration: Absent consistent and credible consumer protection, public acceptance of new payment technologies and cross-border services would falter.

Accordingly, the policy response that led to PSD1 was guided by the following principles:[105] It embraced technology **neutrality**, so that comparable protections would apply regardless of the instrument or channel. It pursued **cross-border consistency,** so that consumers and firms could rely on a harmonised baseline throughout the European Economic Area. It sought **to enable**, not stifle, **innovation** by clarifying roles and obligations for incumbent banks and new market entrants. And it aimed at **proportional risk allocation,** placing liability with the actors best positioned to control risk and prevent harm.

---

[103] European Commission, *Commission Staff Working Document: Impact Assessment Report* SWD(2023) 231 final (Brussels, 28 June 2023), accompanying COM(2023) 367 final and COM(2023) 366 final.

[104]European Payments Council (EPC), "Shortcut to Who Does What in SEPA" (Version 4.0, PDF), https://www.europeanpaymentscouncil.eu/sites/default/files/KB/files/EPC317-10%20v%204.0%20Shortcut%20to%20Who%20Does%20What%20in%20SEPA.pdf, last accessed 25 August 2025.

[105] European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52023PC0366

7.2 The PSD1 Foundation: Establishing Enforcement Responsibility and Consumer Protection Principles

So the first Payment Services Directive 2007/64/EC (PSD1), adopted in 2007 and implemented by 2009, focused on establishing a coherent and harmonised legal foundation for the European payment services market, enabling smoother, faster, and more competitive cross-border payments within the EU.

PSD1 established the same set of rules on payments across the whole European Economic Area (European Union, Iceland, Norway, and Liechtenstein), covering all types of electronic and non-cash payments, such as credit transfers, direct debits, card payments, and mobile and online payments. PSD1 introduced and regulated the formal status of Payment Institutions as Payment Service Providers (PSPs)[106], allowing companies other than banks, central banks, and government agencies to conduct financial transactions.

Alongside market-access reforms, PSD1 established transparency duties for PSPs regarding services, processing times, and fees, and it codified rights and obligations for payment service users (PSUs) and PSPs in the event of unauthorised or incorrectly executed transactions.

The Recitals to PSD1 framed these rules.

Recital 1 underscored that dismantling barriers to the free movement of goods, persons, services, and capital required a functioning single market in payment services.

Recital 5 stressed the need to coordinate national provisions on prudential requirements, market access for new providers, information duties, and the respective rights and obligations of PSPs and PSUs.

Recitals 31 to 39 addressed specific consumer protection themes, including liability for unauthorised transactions and error-correction mechanisms.

Recital 34 highlighted the importance of promoting trust in the safe use of electronic payment instruments. It permitted Member States to reduce or waive payer liability, except in cases of

[106] *Payment service providers*, as defined in Article 1(1) of Directive 2007/64/EC (PSD1), are entities legally authorised to provide payment services within the European Union. The Directive identifies six distinct categories of such providers:

1. Credit institutions as defined in Article 4(1)(a) of Directive 2006/48/EC, primarily engaged in receiving deposits and granting credits;
2. Electronic money institutions as set out in Article 1(3)(a) of Directive 2000/46/EC, authorised to issue electronic money;
3. Post office giro institutions, provided they are permitted under national law to offer payment services;
4. Payment institutions established under PSD1, which are non-bank entities explicitly licensed to provide regulated payment services;
5. The European Central Bank and national central banks, insofar as they are not acting in their official capacity as monetary authorities or other public bodies;
6. Member States and their regional or local authorities, likewise, only when not performing official public authority functions

fraud, recognising that instruments carry different risk profiles and that incentives should favour safer products.

Accordingly, PSD1 put in place four foundational consumer protection mechanisms.

First, a clear liability shift with immediate reimbursement for unauthorised transactions was introduced. If the payer did not authorise a transaction, the PSP had to refund the amount without delay and restore the account to its prior state (Article 60(1)).

Second, it introduced a limitation of responsibility. The payer's exposure for losses arising from the use of a lost, stolen, or misappropriated instrument was capped at €150, with exceptions for cases of fraud or gross negligence, after which, once properly notified, the payer bore no further liability (Article 61).

Third, it imposed a notification duty on the PSUs to report unauthorised or incorrectly executed transactions without undue delay, subject to an outer time limit of 13 months where information had been duly provided (Article 58).

Fourth, it shifted the burden of proof: PSPs, not consumers, had to demonstrate that a disputed transaction was authenticated, accurately recorded and accounted for, and not affected by a technical failure or malfunction; PSPs also bore the burden to substantiate any claim of consumer gross negligence or fraud (Article 59).

Recitals 50 to 52 emphasised that rights without enforcement would be illusory. Member States were therefore required to provide adequate supervision and sanctioning powers; to ensure accessible, affordable out-of-court redress in addition to judicial remedies; and to prevent contractual waivers of the consumer protection baseline applicable to the PSU's home country.

PSD1's Chapter 5 operationalised these ideas. Article 80 PSD1 obliged Member States to establish procedures by which PSUs and consumer associations could lodge complaints with competent authorities regarding PSP infringements, with authorities required to inform complainants about available ADR mechanisms. Article 83 required Member States to establish adequate and effective ADR bodies, and they cooperate actively in cross-border disputes, so consumers would not lose protection when transactions crossed internal frontiers.

PSD1 was enacted on 13 November 2007 and was to be implemented into national law by 1 November 2009. It was supposed to represent a milestone in harmonising payment regulation across Europe and embedding consumer protection into the architecture of the online payments market, setting the stage for the later, more technology-focused reforms under PSD2.

7.3 The Path to a Revision of PSD1 via PSD2

Over the decade in which PSD1 was applicable, its regulatory framework became increasingly misaligned with market realities: emerging fintech intermediaries introduced innovative, lower-cost payment services, leveraging mobile and web applications, that PSD1 did not envisage. The growth of electronic and digital transactions escalated rapidly, giving rise to substantive concerns around consumer protection, transaction security, and the escalating risk of identity

theft.[107] Under PSD1, authentication requirements were rudimentary; a simple password, PIN, or security question sufficed due to its limited scope and conception at a time when mobile banking and API-driven services were nascent. However, as new payment instruments and third-party providers expanded market reach, vulnerabilities grew: data breaches, fraud, lack of transparency, and increasing interoperability issues became materially problematic, particularly in cross-border and remote payment contexts.[108]

7.4 PSD2 Enhancements: Open Banking Possibilities and Challenges

To address the rapid changes to the payment services market, a revised Directive on Payment Services 2015/2366 (PSD2) for the Payment Service Providers within the European Economic Area was brought into force on 12 January 2016 to be implemented by the Member states by 13 January 2018.

Central to PSD2 is the concept of "open banking," which entails opening up the payment services market more fully, by forcing banks and other payment service providers to share their customers' financial information via secure API channels with new intermediaries (authorised Third Party Providers (TPP)) which started to offer innovative services and payment means as, taking advantage of mobile and web applications - when instructed to do so by the PSP's customers.

The second central point addressed by PSD2 was data security and confidentiality, as both have become the primary concern for everyone in both B2B and B2C transactions.

With more channels, actors, and products, the potential for fraud and loss of transparency increased.[109] PSD2 coupled market opening with stronger authentication and monitoring duties to ensure that, whether for a purchase, an administrative workflow, or a data exchange, parties can be reliably identified.

7.4.1 Strong Customer Authentication and Triggers

PSD2 introduced mandatory Strong Customer Authentication (SCA). Article 4(30) PSD2 requires the use of at least two independent elements from the categories of knowledge (something the user knows), possession (something the user possesses), and inherence (something the user is) for SCA. Independence means that the compromise of one factor does not undermine the others, and the design must preserve the confidentiality of authentication data. Article 97(1) requires SCA when a payer (a) accesses an account online; (b) initiates an electronic payment; or (c) performs any action via a remote channel that may imply a risk of payment fraud or other abuses. SCA was intended to restore confidence in online and mobile payments and to strengthen protection as instant and contactless use expanded.

[107] Jas Shah, "The Regulations That Shaped Fintech" (Fintech: Under the Hood, Substack 2025), https://jasshah.substack.com/p/the-regulations-that-shaped-fintech, last accessed 25 August 2025.
[108] Chakib Kissane, "From PSD1 to PSD2: improving the security of your transactions" (Oodrive Blog, 28 August 2023), https://www.oodrive.com/blog/security/from-psd1-to-psd2-improving-the-security-of-your-transactions, last accessed 25 August 2025.
[109] Kissane, ibid. (Fn 56).

7.4.2 Introduction of a Preventive Security Framework

The European Commission adopted binding Regulatory Technical Standards (RTS) via Delegated Regulation (EU) 2018/389[110] from 27 November 2017 to operationalise SCA for remote electronic payments and common and secure open standards of communication. The RTS requires dynamic linking of authentication to the amount and the payee, defines limited risk-based exemptions subject to real-time transaction monitoring, and obliges PSPs to run systems capable of detecting anomalies and high-risk behaviour. These technical rules are complemented by PSD2 Article 96 incident-reporting duties and EBA guidance, together forming a proactive, preventive security framework.

7.5 Liability and Consumer Protection Under PSD2

PSD2, like PSD1, frames consumer protection as a precondition for the success of Europe's digital strategy in payments. Recital 4 links new rules to closing regulatory gaps, providing legal clarity, and ensuring consistent application across the Union so that innovation can expand without diluting user protection, thereby sustaining consumer trust in a harmonised market. Recital 7 recognises that rising complexity and volume have increased security risks, and requires that users of payment services must be adequately protected if payments are to function as critical infrastructure for economic and social activity.

Recital 85 explains that execution risk sits with providers as the payment service providers design and operate the system, organise recalls of misdirected funds, and choose the intermediaries involved in execution. Because the PSPs control these levers, liability for execution is imposed on the PSPs, save for abnormal and unforeseeable circumstances. Recital 95 then requires that electronic payments be carried out securely, including authentication that dynamically links the user to the amount and the payee (dynamic linking), to reduce fraud "to the maximum extent possible". Recital 96 adds that the strength of security measures must be compatible with the level of risk involved in the payment service, reinforcing a risk-proportionate duty to calibrate controls, monitoring, and intervention.

Enforcement and user redress are addressed by Recitals 97 and 98. These recitals insist that, without prejudice to the right to bring court actions, consumers must have easily accessible, independent, impartial, transparent, and effective ADR, supported by providers' internal complaints procedures with short, clearly defined reply timelines and genuine cross-border cooperation. In short, the Recitals do not treat consumer protection as a paper right; they tether it to practical mechanisms capable of producing outcomes.

7.5.1. Strengthened liability framework for unauthorised transactions only

The statutory refund regime set by PSD2, however, is still bound by the concept of authorisation and largely mirrors PSD1's liability structure for the critical distinction between unauthorised and authorised transactions. Article 64 defines authorisation by the payer's consent in the agreed manner; absent consent, the transaction is unauthorised (Article 64(2)). Recitals 70–72

[110] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 about regulatory technical standards for strong customer authentication and common and secure open standards of communication [2018] OJ L 69, 13 March 2018, 23–43.

reiterate the user's notification duty and require immediate refund for unauthorised transactions, allow a short investigatory window where there is a well-founded suspicion of payer fraud, and limit the payer's liability to €50 unless fraud or gross negligence is proven. Recital 85 recognises that PSPs control the payment system, recall arrangements and intermediaries, which justifies imposing execution liability except under abnormal and unforeseeable circumstances. Recitals 95–98 reinforce security obligations and accessible ADR, as well as adequate internal complaints procedures with short, clearly defined response timelines.

Article 72 PSD2 shifts the burden of proof to the PSP, which must demonstrate that the transaction was authenticated, authorised by the payer, and unaffected by technical or security failures. Article 74 harmonises the consumer liability cap to €50 at the EU level (though some Member States continued €150 in national law), confirms zero liability after notification (absent payer fraud), and requires PSPs to evidence any claim of customer negligence. PSD2 also clarifies that simple credential use does not, by itself, prove authorisation, closing gaps that existed under PSD1.

7.5. 2. A de facto "Duty of Care": Operational and Security Risk Management

While PSD2 does not use the phrase "duty of care," a substantive duty arises from the combined effect of Article 95[111] (operational and security-risk management), Article 72[112] (PSP burden of proof), and Article 74[113] (limited payer liability). These obligations are further specified by the EBA Guidelines on security measures and incident reporting (EBA/GL/2017/17114 and EBA/GL/2018/05)[115], which require PSPs to implement real-time transaction monitoring, risk scoring systems, and technical and organisational safeguards: access, fraud, and security incidents.

PSPs must operate real-time monitoring, risk scoring, and adequate controls; failure to respond to evident risk signals undermines attempts to shift liability to the user. The RTS (notably Articles 2 and 18 of Delegated Regulation (EU) 2018/389) require risk assessment based on behavioural history, amount, geography, device and other indicators.

---

[111] A key element of this obligation is the implementation of effective control and monitoring, with Article 95, the regulatory focus from purely ex-post liability to a proactive, preventive responsibility.

[112] Article 72 PSD2 places the burden of proof on the PSP to demonstrate that a disputed transaction was not only authenticated but also genuinely authorised by the payer and executed without technical failure. This creates an obligation to thoroughly examine and document payment transactions.

[113] Article 74 PSD2 provides that the payer shall not be held liable for unauthorised transactions unless they acted fraudulently or with gross negligence – a condition that presupposes the PSP has fulfilled its own protective obligations.

[114] European Banking Authority, „EBA publishes final Guidelines on security measures under PSD2" (press release 13 December 2017), https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-final-guidelines-security-measures-under-psd2, last accessed 25 August 2025.

[115] European Banking Authority, "Guidelines on reporting requirements for fraud data under PSD2" (EBA/GL/2018/05 18 July 2018), https://www.eba.europa.eu/sites/default/files/documents/10180/2281937/5653b876-90c9-476f-9f44-507f5f3e0a1e/Final%20report%20on%20Guidelines%20on%20fraud%20reporting%20under%20PSD2%20%28EBA-GL-2018-05%29.pdf, last accessed 25 August 2025.

7.6 The Emerging Liability Gap for APP Fraud

Despite PSD2's security advances and its transparent allocation of execution risk to providers in the Recitals, the liability refund regime remains tethered to the unauthorised/authorised dichotomy. Where consent is vitiated by deception but formal SCA steps were followed, the transaction is treated as authorised by the PSPs as well as by the national courts and falls outside the statutory reimbursement rules. This formalism, equating technical authentication with valid consent, creates a protection gap, resulting in tens of thousands of APP fraud victims left without any redress possibilities.

8. The Rise of the APP Fraud

So PSD2 strengthened Europe's protection baseline through SCA, dynamic linking, and real-time monitoring. Multi-factor authentication based on knowledge, possession, and inherence elements reduced classic vectors for unauthorised fraud, and dynamic linking made man-in-the-middle manipulation materially harder. The European Banking Authority's joint analysis with the European Central Bank confirmed the effectiveness of these technical security improvements in reducing unauthorised fraud cases.[116] Card payment fraud rates decreased substantially following SCA implementation,[117] while cross-border payment security achieved harmonisation through unified technical standards.[118] This technical success positioned Europe as a global leader in payment security infrastructure and best practices in regulation.

8.1 The Unintended Consequence: Criminal Evolution to Psychological Exploitation

As unauthorised fraud became harder, criminal organisations pivoted to techniques that bypass technical controls and target the human decision-maker. APP fraud results from genuine payer authorisation through deception, coercion, or grooming, thereby neutralising the technical protections that PSD2 built around credential use. This is a methodological evolution from technical intrusion to psychological manipulation, reflecting sophisticated adversarial learning of the regulatory perimeter. APP fraud achieves execution with valid credentials and SCA-compliant steps, yet the user's intent is vitiated by deception. Criminal networks have professionalised social engineering, employing scripted authority posing (such as bank or police impersonation), credible digital façades (including trading dashboards, CRM systems, and fake support portals), and long-horizon relationship building that exploits trust, urgency, and social proof. The result is a structurally different harm pathway: the system flags "authorised" while the economic reality is coerced or misinformed consent.

8.2 The Regulatory Gap: Authorisation vs. Consent

The current framework draws the reimbursement line at the authorisation boundary. Article 64 PSD2 treats a transaction as authorised if the payer consents in the agreed manner; Articles 72 and 74 then allocate burden and liability for unauthorised payments. What PSD2 does not do is distinguish between consent freely given and consent procured by fraud. This formalism equates technical authentication with valid consent and places the loss on victims of APP fraud once the provider evidences authentication and correct recording. It produces context-blind

[116] ECB/EBA, *2024 Report on Payment Fraud*, Executive Summary: "findings support a beneficial impact of SCA…," and "the widespread adoption of the RTS for SCA and CSC has had a positive effect on reducing fraudulent payments." (5, 7).
[117] ECB, *Report on card fraud in 2020 and 2021* (May 2023): "The value of card-not-present fraud declined by 12% in 2021 in light of the market-wide implementation of SCA…," and "market-wide implementation of the RTS for SCA and CSC appears to have strongly reduced the occurrence of card fraud." (1, 3).
[118] Commission Delegated Regulation (EU) 2018/389 supplementing PSD2 with Regulatory Technical Standards for Strong Customer Authentication and Common and Secure open standards of Communication (RTS on SCA & CSC) (EEA-wide, harmonised rules).

outcomes: identical economic and psychological harms are treated differently depending on whether criminals exploited the system's technical layer or the user's cognition.

8.3 Technology-Neutral Design, Context-Sensitive Consequences

Both PSD1 and PSD2 are explicitly technology-neutral, as the legal obligations for payment service providers are defined in functional terms, not by the underlying tools or fraud vectors. This principle of technology independence allows the framework to remain adaptable across different platforms, devices, and service providers.

So, the failure to distinguish between technological and psychological compromise in determining liability undermines that neutrality in practice. The regulatory treatment of fraud depends not on the outcome or the victim's culpability, but on how the criminal engineered the transaction**,** whether it bypassed technical controls or tricked the user into triggering them.

This inconsistency has no principled justification**.** In contract law and in criminal law, consent obtained through deception is generally invalid**.** The payment regulatory regime is an outlier in this respect, treating consent under duress or manipulation as binding, solely because the authentication process was technically completed.

8.4 Market Distortions and Innovation Consequences

Regulatory gaps in payment fraud protection create systematic market distortions that undermine European strategic objectives for payment technology leadership and digital economic development. Innovation disincentives result from regulatory frameworks that create reputational risks for new payment technologies without corresponding consumer protection benefits. Competitive dynamics favour large international platforms that can absorb fraud losses through scale and offer comprehensive protection as a competitive advantage. Card networks and global platforms like PayPal built their success partly on a trust architecture created through adequate consumer protection, demonstrating that strong protection drives rather than constrains market adoption. Consumer adoption barriers emerge from protection gaps that create hesitancy toward innovative payment technologies, particularly for cross-border transactions. Trust deficits stemming from documented institutional failures diminish the willingness to experiment with European payment solutions, while a preference for familiar methods with established protection hinders European digital transformation objectives.

8.5 Criminal Network Sophistication and Technology Exploitation

Criminal organisations demonstrate unprecedented sophistication in exploiting legitimate technology platforms. Social media platforms serve as primary recruitment tools through advertising techniques that identify vulnerable demographics, while messaging applications enable relationship building and psychological manipulation. Remote access technologies facilitate direct control over victim banking systems, and cryptocurrency platforms provide money laundering capabilities that obscure transaction trails and complicate asset recovery. Artificial intelligence integration enables scalable fraud operations through automated victim targeting, conversational AI for simultaneous manipulation of multiple victims, and predictive analytics for optimising psychological impact. Criminal organisations definitely demonstrate

more advanced technology adoption than regulatory authorities, creating systematic advantages that enable continued exploitation. International criminal networks exploit regulatory fragmentation and enforcement coordination failures to maintain operations across multiple jurisdictions while minimising legal exposure. The transnational nature of contemporary fraud operations requires coordinated regulatory responses that current European frameworks cannot provide.

8.6 Regulatory Philosophy and Future Requirements

The evolution from unauthorised to APP fraud protection reveals fundamental tensions in European regulatory philosophy between technical security approaches and comprehensive consumer protection that will determine future policy effectiveness. Current risk allocation places primary fraud responsibility on consumers despite their limited control over system vulnerabilities and criminal sophistication. Economic efficiency principles suggest that parties with the most significant prevention capabilities and economic benefits from digitalisation should bear corresponding liability, requiring fundamental reconsideration of current approaches. Innovation and protection balance requires recognition that strong consumer protection drives rather than constrains beneficial innovation by building consumer confidence and market adoption.

9. International Comparative Models

9.1 The Global Context of Payment Fraud Protection

As European policymakers grapple with the growing crisis of consumer confidence in payment rails, examining international experiences provides crucial insights into both the possibilities and challenges of comprehensive fraud protection. An increasing number of jurisdictions have already taken action to address APP fraud and related scams, implementing frameworks that offer valuable lessons for European policy development.

As detailed in Chapter 6, losses across major jurisdictions are consistently measured in the billions.

The international landscape reveals significant variation in approaches to payment fraud protection, reflecting different regulatory philosophies.

9.2 The United Kingdom: Mandatory Reimbursement in Practice

The UK is widely recognised as Europe's most advanced payments economy. In 2023, over 48 billion payments were made electronically, with cash usage dropping to just 12% of all transactions.[119] The UK's Faster Payments System (FPS), launched in 2008,[120] enabled near-instant transfers between UK banks and was among the first globally to offer real-time account-to-account payments at scale.

However, this early and widespread adoption of instant digital payment channels exposed the UK to payment fraud quite early. The combination of high digital transaction volumes, fast irrevocable payments, and initially weak consumer protection contributed to the UK becoming the first country in Europe where APP fraud overtook card fraud as the primary category of payment fraud. As shown in Chapter 6, the UK reports are the most granular fraud statistics globally. This statistical clarity provided the empirical basis for the UK Parliament to move from a voluntary reimbursement model for APP fraud to a statutory duty under the Financial Services and Markets Act 2023.[121]

With respect to unauthorised payment transactions, the United Kingdom's legal framework is set out in the Payment Services Regulations 2017.[122] Regulation 75 PSR 2017 requires payment service providers (PSPs) to refund the full amount of an unauthorised transaction immediately and no later than the end of the following business day. The burden of proof lies with the PSP, which must demonstrate that the disputed transaction was authenticated correctly. Regulation 77 PSR 2017 further specifies that the payer is not liable unless he/she acted fraudulently or

[119] UK Finance, "UK Payment Markets 2024"(Summary July 2024), reporting 48.1 billion payments in 2023; and UK Finance, *Cash and Cash Machines Report 2024 – Summary* (Nov. 2024), showing cash at 12% of all payments in 2023, https://www.ukfinance.org.uk/system/files/2024-07/Summary%20UK%20Payment%20Markets%202024.pdf, last accessed 25 August 2025.
[120] Wikipedia, "Faster Payment System United Kingdom" https://en.wikipedia.org/wiki/Faster_Payment_System_(United_Kingdom), last accessed 25 August 2025.
[121] UK Parliament, "Financial Services and Markets Bill 2022–23 (Bill 3326)", https://bills.parliament.uk/bills/3326
[122] The Payment Services Regulations 2017, SI 2017/752, legislation.gov.uk, https://www.legislation.gov.uk/uksi/2017/752/contents.

with gross negligence. In practice, this means that consumer liability is capped at £35 before notification of the unauthorised use, unless exceptions apply. This framework has ensured robust protection in cases of unauthorised fraud and aligns closely with the European model under PSD2.

The regulatory treatment of APP fraud has evolved differently. Initially, the United Kingdom attempted to address the problem through a Voluntary Contingent Reimbursement Model (CRM), introduced in 2019,[123] which covered ten major PSPs. However, the CRM soon proved ineffective, as it lacked legal enforceability, produced inconsistent outcomes across institutions, and failed to create adequate incentives for PSPs to invest in meaningful fraud prevention.

In response to widespread dissatisfaction with this voluntary approach, the Financial Services and Markets Act (FSM Act) 2023 was published following Royal Assent on 29 June 2023[124]. Sections 72 to 79 of Part 5 of this Act[125] empower the UK Payment Systems Regulator (PSR) to impose binding reimbursement duties on PSPs, to establish liability allocation rules, and to design enforcement mechanisms.

Acting under this delegated authority, the UK PSR issued binding rules in July 2023[126] requiring all participants in the FPS to reimburse APP fraud victims up to £85,000 per claim from 7 October 2024 onward, subject only to narrow exceptions such as consumer fraud or gross negligence. The regime also mandates that liability be shared equally between sending and receiving PSPs (50:50), thereby recognising the systemic nature of APP fraud and the shared responsibility of both institutions involved in the payment chain.

The scope of this new reimbursement model remains limited to FPS transactions, which, although significant for instant retail payments, accounted for only about 10% of all UK payment transactions in 2023 (approximately 4.9 billion out of 48.1 billion).[127] Card payments, BACS,[128] CHAPS,[129] and cross-border transfers are excluded, even though APP fraud also occurs through these channels. This channel-based limitation produces marked discrepancies in consumer protection, as two victims of otherwise identical scams may face completely

---

[123] UK Government, "Government approach to authorised push payment scam reimbursement," https://www.gov.uk/government/publications/government-approach-to-authorised-push-payment-scam-reimbursement/government-approach-to-authorised-push-payment-scam-reimbursement, last accessed 27 August 2025.

[124] Simmons-Simmons, "The Financial Markets and Services Act receives Royal Consent" (blog post 3 July 2023), https://www.simmons-simmons.com/en/publications/cljmtl4a700rqthbsi294cmhe/fsm-bill-receives-royal-assent, last accessed 23 August 2025.

[125] UK Legislation, "Financial Markets and Services Act 2023, Chapter 29, https://www.legislation.gov.uk/ukpga/2023/29/pdfs/ukpga_20230029_en.pdf, last accessed 21 August 2025.

[126] Allen & Overy (Shearman), "The U.K.'s Authorised Push Payment (APP) Fraud Reimbursement Scheme" (Insight vom 10. 01. 2025), https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/the-uks-authorised-push-payment-APP fraud-reimbursement-scheme, last accessed 25 August 2025.

[127] UK Finance, "UK Payment Markets 2024 – Summary" (Report 2024) S 2, https://www.ukfinance.org.uk/system/files/2024-07/Summary%20UK%20Payment%20Markets%202024.pdf, last accessed 25 August 2025.

[128] Wikipedia, "BACS"; Bacs Payment Schemes Limited (Bacs), previously known as Bankers' Automated Clearing System, is responsible for the clearing and settlement of UK automated direct debit and Bacs Direct Credit and the provision of third-party services, https://en.wikipedia.org/wiki/Bacs, last accessed on 1 August 2025.

[129] Wikipedia, "ChAPS"; The Clearing House Automated Payment System (CHAPS) is a real-time gross settlement payment system used for sterling transactions in the United Kingdom, last accessed 1 August 2025.

different outcomes depending solely on whether the fraudsters induced a transfer via FPS or via card rails. Such discrepancies are difficult to justify normatively, given that English contract and criminal law generally treat consent obtained through deception as invalid.

The first enforcement results demonstrate the tangible impact of the new regime. According to the UK Finance Annual Fraud Report 2025,[130] the overall number of APP fraud cases fell by 18% in 2024, with significant declines in purchase scams (–16%), investment scams (–24%), advance fee scams (–38%), and romance scams (–2%). At the same time, the total value of losses caused by investment scams rose by 34%, reflecting a criminal shift toward fewer but higher-value cases and different payment rails. Within the first six months of the regime's implementation, 86% of in-scope victims received full or partial reimbursement. While 23% of PSPs attempted to invoke the gross negligence exemption, only 2% of claims were ultimately rejected on that basis, a result that illustrates both the narrow application of the exception and effective regulatory discipline.

A crucial element underpinning the enforcement of the UK regime is the Financial Ombudsman Service (FOS), which serves as the enforcement backbone of consumer redress in the UK. The FOS has binding authority, is funded through a compulsory industry levy on FCA-regulated firms plus case fees[131], that guarantees independence from the institutions it oversees, and operates with a substantial annual budget exceeding £250 million.[132] With an average resolution time of three to four months, the FOS provides timely outcomes in complex fraud disputes and ensures that the cost of dispute resolution is borne by the industry rather than by consumers. This combination of statutory reimbursement rules and robust enforcement infrastructure makes the UK the most advanced jurisdiction in Europe in addressing APP fraud, even though critical structural limitations remain due to its channel-restricted scope.

9.3 The United States: Fragmented Regulation and Innovation Pressure

The United States represents one of the world's largest electronic payment markets. It has long maintained statutory frameworks for consumer protection in electronic transactions, most notably the Electronic Fund Transfer Act (implemented by Regulation E) for unauthorised EFTs, the Fair Credit Billing Act/Reg Z for credit card payments. As the numbers in Chapter 6 show, the US has high online fraud losses dominated by investment and imposter scams. The regulatory challenge lies in the fragmented liability architecture: as in Europe, strong protections for unauthorised transactions coexist with a near-total absence of reimbursement for APP fraud.

Consumer complaint data demonstrates a rapidly growing impact. The US Consumer Financial Protection Bureau (CFPB) handled 3.2 million consumer complaints in 2024,[133] representing a

[130] UK Finance, "Annual Fraud Report 2025" (27 May 2025) 15, https://www.ukfinance.org.uk/system/files/2025-05/UK%20Finance%20Annual%20Fraud%20report%202025.pdf, last accessed 25 August 2025.

[131] FOS "Governance and Funding", https://www.financial-ombudsman.org.uk/who-we-are/governance-funding, last accessed 25 August 2025.

[132] FOS: "Our 2024/25 plans and budgets", https://www.financial-ombudsman.org.uk/files/324416/Financial-Ombudsman-Service-Plans-and-Budget-2024-25.pdf, last accessed 27 August 2025

[133] Federal Reserve Board, Office of Inspector General, "The CFPB Effectively Monitors Consumer Complaints but Can Enhance Certain Processes" (report from 24 June 2024), https://oig.federalreserve.gov/reports/cfpb-consumer-complaints-jun2024.pdf, last accessed 25 August 2025.

92% increase compared to 2023. Complaints about money services (incl. mobile/digital wallets) listed fraud/scam as the top issue. In 2022, U.S. servicemembers filed more than 1,100 payment-app complaints (about 41% YoY), and the CFPB's OSA notes[134] that payment-app fraud can cause severe financial harm that jeopardises continued service or security clearances.

Industry data reveals concerning trends in fraud sophistication and impact. The 2025 Javelin Strategy & Research Identity Fraud Study[135] documented $27.2 billion in consumer losses in 2024, with fraud resolution time averaging nearly 10 hours per victim in 2023. First-party fraud, where criminals manipulate consumers into authorising payments, now represents 36% of all reported fraud, up from 15% in 2023, according to LexisNexis Risk Solutions analysis.[136]

From the perspective of payment channels, credit transfers and cryptocurrency transactions accounted for higher losses than all other methods combined, showing fraudsters' strategic reliance on irreversible channels that complicate recovery. These developments highlight the inability of existing legal instruments in the US to provide comprehensive coverage against APP fraud, despite the long-standing existence of strong rules for unauthorised transactions in the United States.

The Fair Credit Billing Act (FCBA), enacted in 1974 as Regulation Z under the Truth in Lending Act (TILA[137]), grants consumers robust chargeback rights on credit card transactions. Similarly, the Electronic Fund Transfer Act (EFTA[138]) of 1978, implemented through Regulation E, establishes clear reimbursement duties for banks in cases of unauthorised electronic transfers, including debit card and Automated Clearing House (ACH) payments. Under Regulation E, banks must recredit disputed amounts within ten business days while they investigate, and ultimate liability for consumers is capped between $50 and $500, depending on how promptly the unauthorised transaction is reported.

Notably, CFPB issued updated guidance on 13 December 2021, through its Electronic Fund Transfers FAQs,[139] providing critical clarifications on unauthorised electronic fund transfer definitions and the scope of Regulation E coverage. Transfers initiated with account credentials obtained through fraud or deception (such as phishing) are considered unauthorised transactions under Regulation E. This clarification closed a loophole by making clear that victims who are

---

[134] CFPB Office of Servicemember Affairs, *Annual Report 2022* (servicemembers submitted **>1,100** payment-app complaints; among fastest-growing complaint types; harms may jeopardise continued service or security clearances). https://files.consumerfinance.gov/f/documents/cfpb_osa-annual-report_2022.pdf, last accessed on 1 August 2025.

[135] Javelin Strategy & Research, press release, „Identity Fraud Flourishes Amid Consumers' Growing Digital Presence, Costing Them Time and Money" (10 April 2024), https://www.javelinstrategy.com/press-release/identity-fraud-flourishes-amid-consumers-growing-digital-presence-costing-them-time, last accessed 25 August 2025.

[136] Javelin Strategy & Research, Press release, „Identity Fraud Flourishes Amid Consumers' Growing Digital Presence, Costing Them Time and Money" (GlobeNewswire, 28 March 2023), https://www.webwire.com/ViewPressRel.asp?aId=338403, accessed 25 August 2025.

[137] Consumer Financial Protection Bureau (CFPB), Regulation Z (12 CFR 1026; Truth in Lending,2024), https://www.consumerfinance.gov/rules-policy/regulations/1026, last accessed 25 August 2025.

[138] Consumer Financial Protection Bureau (CFPB), Regulation E (12 CFR 1005; Electronic Fund Transfers, 2024), https://www.ecfr.gov/current/title-12/chapter-X/part-1005, last accessed 25 August 2025.

[139] Consumer Financial Protection Bureau (CFPB), "Electronic Funds Transfers FAQs", https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/, last accessed 25 August 2025.

induced into providing login credentials have not “furnished the access device” within the meaning of the regulation. As a result, banks remain liable to reimburse such cases, and consumer negligence cannot be considered when determining liability.

The December 2021 guidance (Coverage: Financial Institutions FAQ Question 1) also definitively clarified that P2P payment providers operating "pass-through" payments using consumer debit cards are covered financial institutions, as are providers offering mobile wallets or prepaid account functionality. Notably, the narrow "service provider" exception under 12 CFR § 1005.14(a) rarely applies to major P2P platforms because ACH agreements combined with debit card acceptance arrangements constitute "agreements" that trigger full institutional responsibilities.

But the situation is very different for APP fraud in the US. If a consumer willingly initiates a payment based on deception, such as through investment scams, romance fraud, or purchase fraud, existing law provides no general statutory right to reimbursement. APP fraud victims, therefore, receive (voluntary) compensation in only a fraction of cases.

A Federal Reserve Bank of Atlanta analysis puts it plainly[140]: APP scams aren’t subject to mandatory reimbursement under EFTA because the payments are technically authorised.

The protection gap for APP fraud becomes starkest when examining reimbursement rates across payment types. Traditional card payments benefit from robust chargeback protections under the Fair Credit Billing Act, while debit cards receive strong unauthorised transaction protections under Regulation E.

US consumers face not only the non-existent APP fraud reimbursement but also a lack of enforcement of refunding unauthorised debit transactions in the US, similar to the situation in the European Union, as found by an investigation started by Senator Elizabeth Warren in April 2022[141] into Zelle, the popular P2P US payment network.

The Zelle network, which is operated by Early Warning Services LLC, Arizona (EWS) and owned by seven central US banks, processed $806 billion in P2P payment transfers during 2023[142] while reporting a fraud-free completion rate of 99.95%. Zelle is one of the most widely used P2P US payment systems integrated into over 2,200 financial institutions, including major banks. It enables fast, convenient, and near-instant transfers between bank accounts within minutes, often without fees, making it a popular alternative to cash or checks for consumers

[140] Federal Reserve Bank of Atlanta, “Addressing Authorised Push Payment Scams in the US” (blog post 23 September 2024, https://www.atlantafed.org/blogs/take-on-payments/2024/09/23/addressing-authorized-push-payment-fraud-in-us, last accessed 28 August 2025.

[141] Warren Office, “ Facilitating Fraud: How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created It,”, https://www.warren.senate.gov/imo/media/doc/ZELLE%20REPORT%20OCTOBER%202022.pdf, last accessed 1 August 2025.

[142] PRNewswire, “Zelle soars with $806 billion transaction volume, up 28% from prior year” (blog post 4 May 2024), https://www.prnewswire.com/news-releases/zelle-soars-with-806-billion-transaction-volume-up-28-from-prior-year-302077432.html, last accessed 31 August 2025.

and small businesses. In 2024, Zelle processed over $1 trillion in transactions with 151 million enrolled users[143], highlighting its large scale and significant role in American digital payments.

In mid-2023, the Senate Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations (PSI) initiated its own investigation. It held public hearings explicitly focused on consumer scams and banks' reimbursement failures on Zelle and other instant payment platforms. The investigations and hearings[144] showed that Zelle issues span both unauthorised transfers (covered by Reg E) and APP scams (generally not mandated for reimbursement). In 2023, at JPMorgan, Bank of America, and Wells Fargo, consumers disputed $165.8 million in unauthorised "fraud" transactions and $206.8 million in authorised "scam" transactions, $372.6 million in total, of which $270.5 million (~73%) was not reimbursed. PSI also reported that Zelle's June 2023 (voluntary) imposter-scam policy resulted in $18.3 million in reimbursements over its first six months, covering approximately 15–20% of scam disputes.

The CFPB, which emerged from the 2008 financial crisis with a broad mandate for consumer protection, has pursued numerous enforcement actions, obtaining an estimated $3.6 billion in consumer redress and penalties in 2023.[145] The CFPB's November 2024 digital payment app supervision rule[146] marked a significant expansion of regulatory authority over nonbank payment platforms. The rule subjects companies handling over 50 million annual transactions to bank-like supervision, covering privacy and surveillance issues under the Gramm-Leach-Bliley Act, error and fraud dispute resolution, and prevention of "debanking" practices. However, Congressional Republicans voted 51-47 in the Senate and 219-211 in the House to nullify[147] the rule via the Congressional Review Act, demonstrating the actual political challenges facing comprehensive regulatory reform.

Recent legislative proposals illustrate a growing recognition of the problem. The Protecting Consumers From Payment Scams Act, introduced in August 2024 by Senators Blumenthal and Warren and Representative Waters,[148] seeks to expand Regulation E to cover "fraudulently induced electronic fund transfers," effectively treating APP fraud as unauthorised. The bill

---

[143] Clearly Payments, "What is Zelle Real-Time Payments in the USA?" (blog post), https://www.clearlypayments.com/blog/what-is-zelle-real-time-payments-in-the-usa/, last accessed 31 August 2025.(Zelle works by linking to users' bank accounts. Once set up, users can send money directly from their bank accounts to another person's account. All they need is the recipient's phone number or email address.

[144] U.S. Senat, *Hearing* „Examining Consumer Protections in the Federal Payments Landscape" (118. Kongress, 27 September 2023).https://www.congress.gov/event/118th-congress/senate-event/336040, last accessed 25 August 2025.

[145] Consumer Financial Protection Bureau, *The CFPB's enforcement work in 2023 and what lies ahead* (29 Jan 2024) reporting ≈$3.07bn in consumer relief + $498m in civil penalties in 2023 (≈$3.57bn total). https://www.consumerfinance.gov/about-us/blog/the-cfpbs-enforcement-work-in-2023-and-what-lies-ahead/, last accessed on 31 August 2025.

[146] Holland & Knight, "CFPB Finalizes New Federal Supervision of Certain Providers" (Nov 2024), https://www.hklaw.com/en/insights/publications/2024/11/cfpb-finalizes-new-federal-supervision-of-certain-providers, last accessed 25 August 2025.

[147] Congress, *Public Law 119-11, Joint Resolution Disapproving the CFPB Rule on Larger Participants in General-Use Digital Consumer Payment Applications*, 119th Cong., May 9, 2025 (disapproving 89 Fed. Reg. 99582), https://www.congress.gov/119/plaws/publ11/PLAW-119publ11.pdf, last accessed 25 August 2025.

[148] House Committee on Financial Services (Democrats), *Press Release zu* HJ Res 66 (14 June 2023), https://democrats-financialservices.house.gov/news/documentsingle.aspx?DocumentID=412650 last accessed 25 August 2025.

proposes a 50:50 liability split between financial institutions, similar to the UK model, and would extend protections to wire transfers and telephone-authorised transactions.

In the absence of comprehensive reform, the United States remains vulnerable to escalating APP fraud losses despite its otherwise advanced consumer protection architecture for unauthorised payments.

9.4 APP Fraud in Singapore: Regulatory Evolution, Empirical Outcomes and Comparative Insights

Singapore has established one of the most digitally integrated financial systems in Asia, with real-time payments forming the backbone of consumer and business transactions. The country's PayNow system, launched in 2017, enables instant peer-to-peer transfers linked to mobile numbers or national ID numbers and has achieved broad adoption across the population. This firm's reliance on instant, irrevocable transfers, combined with rapid growth in mobile banking, created fertile ground for deception-based fraud.

Singapore's transition from a low-crime, high-trust financial hub to the jurisdiction with the world's highest per-capita scam losses has been remarkably swift. In 2024 alone, the Singapore Police Force (SPF) recorded 51,501 scam cases, a year-on-year rise of 10.6%, with aggregate losses exceeding S$1.1 billion, an increase of 70.6% over 2023.[149] As documented in Chapter 6, Singapore now suffers the highest per-capita scam losses worldwide. The regulatory response has been to layer consumer protection guidelines with multi-sector duties, yet mandatory APP reimbursement remains absent. The mid-year brief for 2024 revealed an average loss per incident of S$14,503 and showed that four "mega incidents" accounted for more than one-fifth of the annual damage, signalling a shift toward high-impact, low-volume attacks[150]. Phishing and investment scams now compete with social-media job scams as primary vectors; together, they represent more than 70% of the financial toll. Alarmingly, law enforcement intelligence attributes much of the current wave to industrial-scale call centres operating from enclaves in the Mekong region, where trafficked call centre employees deploy deep-fake voice cloning to imitate Singapore's major dialects and official typography, thereby outflanking earlier two-factor and caller-ID defences.[151]

Singapore's E-Payments User Protection Guidelines (EUPG),[152] issued by the Monetary Authority of Singapore (MAS), represent a central component of the city-state's regulatory infrastructure for retail payment security. Initially introduced in 2019 and most recently revised in October 2024, the EUPG set out a conditional liability framework for unauthorised electronic payment transactions**.** Although the Guidelines are non-statutory, MAS expects full compliance from all licensed banks and Major Payment Institutions (MPIs) regulated under the *Payment*

[149] Singapore Police Force (SPF), Annual Scams and Cybercrime Brief 2024 (Berichtsdatum 05. 02. 2025), https://www.police.gov.sg/Media-Room/Police-Life/2025/02/Five-Things-You-Need-to-Know-About-Scams-and-Cybercrime-in-2024, accessed 25 August 2025.
[150]SPF, Mid-Year Scams and Cybercrime Brief 2024 (22. 08. 2024), https://www.police.gov.sg/-/media/Spf/Statistics/Mid-Year-Scams-and-Cybercrime-Brief-2024.pdf, accessed 25 August 2025.
[151] SPF, *Annual Scams and Cybercrime Brief 2024*, supra Fn 78.
[152] Monetary Authority of Singapore (MAS), "E-Payments User Protection Guidelines" (revised 25 October 2024), https://www.mas.gov.sg/regulation/guidelines/e-payments-user-protection-guidelines, accessed 31 August 2025.

Services Act 2019 (No. 2 of 2019).[153] Their scope is limited to "protected accounts," defined as non-business retail accounts capable of sending or receiving payment instructions, held with regulated entities within Singapore.

The EUPG introduces a quasi-objective reimbursement regime for unauthorised payment transactions: if a consumer did not act fraudulently or with gross negligence and promptly reports an unauthorised transaction, the payment service provider (PSP) is expected to reimburse the loss entirely.[154] MAS defines an "unauthorised transaction" as one that the account holder did not initiate, authorise, or benefit from. In such cases, the burden of investigation and decision rests with the PSP, which must conclude its internal review within 21 business days for straightforward cases and within 45 business days for complex or cross-border matters.[155] The institution must communicate its findings in writing, including specific reasons if the claim is rejected in part or in whole.

The EUPG also establishes minimum technical and procedural standards that PSPs must meet. These include the provision of 24/7 reporting hotlines, real-time transaction alerts, user-configurable transaction limits, and two-factor authentication by default. Since the 2024 revision, all covered institutions are additionally required to implement a user-accessible kill switch[156] that can instantly suspend all outgoing transactions. This requirement applies to banks as well as to non-bank MPIs, such as YouTrip and Revolut, provided they offer protected accounts within the meaning of the Guidelines.

Singapore's regime also specifies a set of enumerated user duties[157] under EUPG, so consumers and users of payment services have clearly defined responsibilities to protect their credentials and notify service providers promptly of unauthorised transactions. These enumerated duties include safeguarding login credentials, not sharing OTPs or passwords, and swiftly reporting fraudulent transactions to limit liability.

Within the European Union, the EUPG's principles resemble, in part, the liability provisions of Article 73 of PSD2. However, PSD2 introduces a strict timeline (no later than the end of the next business day) for refunds. It provides a limited consumer liability cap of EUR 50 under Article 74(1), a feature absent in the Singaporean model. Additionally, PSD2 assigns the burden of proof to the PSPs, which must demonstrate that the transaction was authenticated, recorded, and not affected by a technical breakdown. The EUPG reflects similar logic but falls short of providing an explicit right to reimbursement or judicial enforceability, due to its soft-law status.

[153] Monetary Authority of Singapore (MAS), Response to Consultation on Proposed Revisions to E-Payments User Protection Guidelines (September 2023), https://www.mas.gov.sg/publications/consultations/2023/consultation-on-proposed-revisions-to-e-payments-user-protection-guidelines, last accessed 25 August 2025.
[154] E-Payments User Protection Guidelines (MAS), § 4.1: "A responsible financial institution shall provide a full reimbursement … if the user did not act fraudulently or with gross negligence.
[155] Ibid., § 5.3 and § 5.6: 21 or 45 business days depending on complexity.
[156] Montey Authority of Singapore (MAS), "Circular on Anti-Scam Measures by Major Payment Institutions Providing Personal Payment Accounts that contain E-money" (MAS Circular PD 25 October 2024), https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/pd/circular-on-anti-scam-measures/circular-on-anti-scam-measures-by-mpis.pdf, last accessed 25 August 2025.
[157] Hong Leong Finance, "Let's Work Together To Protect Your Account", https://www.hlf.com.sg/site-services/eupg.html, last accessed 3 August 2025.

Dispute resolution under the EUPG is left primarily to internal complaint processes; optional escalation is offered to the Financial Industry Disputes Resolution Centre (FIDReC).[158] Although FIDReC's decisions are binding on financial institutions if accepted by the consumer, it has a claim limit of S$100,000.

As a reply to the surge in online fraud, several major reform initiatives were set recently:

A Shared Responsibility Framework (SRF) was introduced in 2023 and formally implemented in December 2024.[159] This framework created a liability-sharing model between banks and telecommunications companies for phishing-related scams. Banks were required to implement technical safeguards such as "kill switches" allowing consumers to freeze compromised accounts instantly. At the same time, telcos were obliged to block fraudulent SMS sender IDs and strengthen anti-spoofing filters. Under the SRF, liability for consumer losses for unauthorised payment transactions is apportioned depending on which institution failed to meet prescribed duties. Still, the absence of a statutory cap means banks and telcos face theoretically unlimited exposure if they are negligent, creating a powerful incentive to invest in preventive controls. Under the SRF, banks must deploy layered real-time fraud-surveillance engines that combine device fingerprinting, behavioural biometrics, and velocity checks. Transactions flagged by these systems must trigger "step-up authentication" and can be suspended until the customer re-verifies intent. It has further mandated a 12-hour cooling-off period for high-risk changes, such as payee additions on a new device. The guidance explicitly forbids the inclusion of clickable hyperlinks in system-generated SMS messages. However, even the SRF is restricted to phishing-based unauthorised transactions and does not cover APP fraud or any other malware-based unauthorised payments.

Instead of having banks absorb the entirety of the liability that originates through spoofed SMS traffic, the regulatory framework identifies the telecommunications layer as the least cost avoider for that portion of the threat. It therefore places affirmative obligations, and ultimately liability, on network operators. This principle was first articulated in the Infocomm Media Development Authority's (IMDA) 2022 consultation on a whole mandatory SMS Sender-ID regime, which noted that spoofing fell by nearly 70 per cent within three months of pilot implementation.[160]

Interestingly, financial institutions responded with proprietary innovations that often exceed the minimum standard. Overseas Chinese Banking Corporation (OCBC) released its "Money Lock" feature in November 2023,[161] allowing customers to sequester funds within sub-accounts

[158] Singapore Management University, "Mediating consumer financial disputes: Financial Industry Disputes Resolution Centre's unique house style,"
"https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?params=/context/sol_research/article/5235/&path_info=Mediating_Consumer_Financial_Disputes___FIDReC_Unique_House_Style.pdf, last accessed 31 August 2025.
[159] Monetary Authority of Singapore, "Guidelines on Shared Responsibility Framework" (published 24 October 2024), https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework, last accessed 31 August 2025.
[160] Financial Times, „Rich and Naive – why Singapore is engulfed in a scamdemic", https://www.ft.com/content/3299cf7e-67bd-4654-8aa9-55fc24a66b63, last accessed 30 May 2025
[161] OCBC, "OCBC rolls out Money Lock anti-scam security feature" (press release 27 November 2023), https://www.ocbc.com/group/media/release/2023/ocbc-rolls-out-money-lock-anti-scam-security-feature.page, last accessed 31 August 2025.

that cannot be moved digitally and can be unlocked only in person at an ATM or branch. According to media reports, by 2024, 245,000 customers placed more than S$20 billion under lock, illustrating the demand for user-controlled indemnification tools.[162]

Singapore currently does not impose a statutory or regulatory duty to reimburse victims of APP fraud, even where the deception was apparent, and instead relies on discretionary goodwill payments and some other initiatives rolled out during the past months:

The Anti-Scam Command (ASCom)[163] is a specialised unit formed under the Singapore Police Force (SPF), operational since March 2022. It centralises efforts for scam detection, investigation, incident response, enforcement, and collaboration with banks and other partners. ASCom operates as a joint unit of the Singapore Police Force and major banks. ASCom operates as a centralised hub for the rapid detection and freezing of fraudulent transfers. By mid-2024, ASCom had frozen more than 10,300 bank accounts and recovered S$54 million in scam proceeds[164].

The Online Criminal Harms Act (OCHA) (2023), a legislative measure,[165] authorised regulators to order the immediate removal of fraudulent websites, advertisements, or online accounts within a maximum of two hours, thereby targeting the infrastructure fraudsters use to lure victims.

The Protection from Scams Act (2025)**[166]** grants law enforcement and financial institutions the power to impose 30-day freezes on suspicious transactions. This measure is particularly significant in a jurisdiction where most transfers settle instantly, as it introduces a legally sanctioned cooling-off mechanism to block suspected scams before funds disappear into international laundering networks. Complementary proposals have also focused on consumer awareness, with MAS requiring banks to deploy persistent fraud warnings at the transaction interface and to strengthen behavioural monitoring systems.

Taken together, Singapore illustrates both the promise and limitations of a multi-sectoral response to the scam crisis. The alignment of liability with functional control, making banks responsible for payment monitoring and telcos for communication integrity, has spurred technical investment and operational reforms. Yet the absence of a statutory reimbursement duty for APP fraud victims continues to represent a major structural weakness. Unless Singapore extends the logic of the SRF to the broader landscape of APP fraud, it will remain a jurisdiction with strong

[162] The Star, OCBC Malaysia launches Money Lock feature to curb scams (2 September 2025), https://www.thestar.com.my/business/business-news/2025/09/02/ocbc-malaysia-launches-money-lock-feature-to-curb-scams, last accessed 3 September 2025.
[163] Singapore Police Force, "Opening of the Anti-Scam Command Office", https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scam_command_office, last accessed 3 September 2025.
[164] Channel News Asia, "Banks, telcos and scam victims to share liability for losses under new framework to kick in on Dec 16", https://www.channelnewsasia.com/singapore/phishing-scams-banks-telcos-shared-responsibility-framework-dec-16-responsibilities-duties-4699236, last accessed 3 September 2025.

[165] Singapore Police Force, "Introduction to OCHA), https://www.police.gov.sg/Advisories/Online-Criminal-Harms-Act/Introduction-to-OCHA, last accessed 3 September 2025.
[166] ReedSmith, "Singapore introduces Protection from Scams Bill and offences for the misuse of SIM cards" (Client Alerts 17 January 2025), https://www.reedsmith.com/en/perspectives/2025/01/singapore-protection-scams-bill-offences-misuse-sim-cards, last accessed 3 September 2025.

preventive measures but insufficient victim compensation, despite its otherwise sophisticated enforcement architecture.

9.5 Australia's Evolving Multi-Sector Approach

Australia combines very high digital payments adoption with a dense mix of bank, telecom, and platform intermediaries, which has made the country a significant target for deception-based fraud. In 2024, reported consumer scam losses fell to AU$2.03 billion, a decline of roughly 26% from 2023. Outside the scams lens, CNP fraud has surged: total card fraud reached AU$762 million in 2023 (about 70.2 cents per AU$1,000 spent), with over 90% now attributable to CNP transactions and overseas CNP losses rising steeply again in 2024.[167] At the communications layer, the national regulator reports hundreds of millions of scam calls and SMS blocked annually under enforceable industry codes; by mid-2025, providers reported more than 936 million blocked scam SMS since July 2022,[168] illustrating both the scale of malicious traffic and the preventive capacity of upstream filtering. Taken together, these figures reflect a two-track risk landscape: large, persistent losses from sophisticated investment and redirection scams, and a parallel rise in merchant-side and scheme-level card fraud that exploits remote channels.

Protection against unauthorised electronic payments is governed by the Australian Securities and Investments Commission´s (ASIC) ePayments Code (EPC). Although the EPC is a voluntary code, the major banks and most retail payment providers subscribe to and must incorporate the code in their customer terms. The EPC places the default loss on the provider unless the institution can prove consumer fraud, breach of passcode-security obligations, or unreasonable delay in reporting; where a passcode was required and none of the "full liability" scenarios apply, the account-holder's exposure is capped at the least of AU$150, the available balance, or the applicable transaction limit(s).[169]

The code defines "extreme carelessness" (for example, keeping username and password together in an unsecured manner). It puts the burden of proof on the PSP to show a relevant consumer breach. It also stipulates investigation and response timeframes and provides a distinct "mistaken internet payments" regime that obliges sending and receiving institutions to trace, freeze where available, and return funds when payers misaddress transfers. Disputes can be escalated to the Australian Financial Complaints Authority (AFCA),[170] the national external dispute resolution (EDR) body, which applies the EPC's liability logic and can order compensation (binding orders for the PSPs); providers are required to share evidence if they allege consumer contribution. In aggregate, this architecture produces strong, technology-neutral protection for unauthorised withdrawals, broadly analogous to PSD2's regime in the EU.

[167] Australians Payment Network, "Fraud Statistic Jan – Dec 2024," https://auspaynet.com.au/resources/fraud-statistics, last accessed 25 August 2025.
[168]Bird&Bird, "Revised code targets scam SMS traffic," https://www.twobirds.com/en/insights/2023/australia/revised-code-targets-scam-sms-traffic, last accessed 3 September 2025.
[169] Australian Securities & Investments Commission (ASIC), "ePayments Code" (published 02 Juni 2022), https://download.asic.gov.au/media/lloeicwb/epayments-code-published-02-june-2022.pdf, last accessed 25 August 2025.
[170] Australian Financial Complaints Authority, "The process we follow," https://www.afca.org.au/what-to-expect/the-process-we-follow, last accessed 3 September 2025.

Australia has not yet adopted a general statutory right to reimbursement for APP fraud. Instead of a UK-style reimbursement duty, the country has enacted an ecosystem-wide Scams Prevention Framework (SPF)[171] that came into force on 21 February 2025 (by inserting Part IVF into the Competition and Consumer Act 2010). The SPF empowers the Minister to designate sectors, initially banks, telecommunications carriers, and digital platforms (social-media, paid search, and direct-messaging services), and to make binding sector codes and SPF rules that require reasonable steps to prevent, detect, report, disrupt, and respond to scams, with civil penalties up to AU$50 million for non-compliance. Crucially, the SPF[172] allows authorisation of a single EDR pathway (the Government has signalled AFCA for the initial sectors) to determine consumer complaints about how regulated entities responded to scams and to award monetary redress on the facts of each case. Still, it does not create a blanket, statutory presumption of reimbursement for APP losses.[173] In practice, AFCA has begun to shape outcomes at the margin. In a notable line of determinations, the authority has rejected provider arguments that a customer "voluntarily disclosed" one-time passcodes where the disclosure occurred under bank impersonation scripts, thereby applying the EPC's unauthorised transaction logic and limiting consumer contribution to AU$150 in those specific fact patterns. Even so, these EDR-based remedies remain case-by-case and fall short of a universal APP reimbursement rule.

Consumer groups advocated for including a presumption of reimbursement in the SPF, but the final Act opted for obligations, penalties, and EDR, rather than a UK-style liability split. The Senate record and Treasury FOI material confirm the government's rationale: avoid concentrating costs solely on banks and create prevention incentives across the whole scam chain (banks, telcos, platforms).

Australia's enforcement actions and policy proposals over the past two years have been deliberately multi-sectoral and prevention-led.

The National Anti-Scam Centre (NASC)[174] was established in July 2023 within the Australian Competition and Consumer Commission (ACCC) as a central coordination hub for government, industry, and civil society, accelerating intelligence sharing and joint interventions.

On the banking side, the Australian Banking Association's "Scam-Safe Accord[175]" (compelling from late 2023) committed major banks to a package of controls: stronger biometric checks, risk-based friction on high-risk payments, exchange-level controls for transfers to cryptocurrency venues, enhanced inter-bank intel-sharing, and, critically, the staged roll-out (from July 2025) of CoP/VoP (Confirmation/Verification of Payee, a name-checking control on account-to-account payments designed to prevent misdirection and specific APP scams).

---

[171] Australia, *Scams Prevention Framework Act 2025* (No. 15 of 2025), https://www.legislation.gov.au/Details/C2025A00015, last accessed 1 September 2025.

[172] Corrs Chambers Westgarth, "The new Scams Prevention Framework: key considerations for regulated entities" (21 February 2025), https://www.corrs.com.au/insights/the-new-scams-prevention-framework-key-considerations-for-regulated-entities, last accessed 25 August 2025.

[173] Australian Treasury, "Scams Prevention Framework – Summary of Reforms" (September 2024), https://treasury.gov.au/sites/default/files/2024-09/c2024-573813-summary.pdf, last accessed on 25 August 2025.

[174] National Anti Scam Centre, "Together we are an unstoppable force", https://www.nasc.gov.au/, last accessed on 25 August 2025.

[175] Gilbert+Tobin, "Australia's whole-of-ecosystem approach to combating the scourge of scams" (blog post 30 August 2024), https://www.gtlaw.com.au/insights/australias-whole-of-ecosystem-approach-to-combatting-the-scourge-of-scams, last accessed on 3 September 2025.

At the telecoms layer, enforceable codes registered by the Australian Communications and Media Authority (ACMA)[176] require carriers to identify, trace, and block scam calls and SMS at scale; by late 2024, the Government had also announced a mandatory SMS Sender ID Register to curb brand impersonation ("alpha tags") in text messages.

On the platform layer, sector codes under the SPF are being developed to impose ad-buyer verification, takedown service-level agreements, scam-content blocking, and data-sharing duties on social-media, search, and messaging services that have become dominant first-mile vectors for investment scams and purchase fraud.

These measures have produced mixed but visible results. On the positive side, headline scam losses fell by about one-quarter in 2024, consistent with the effect of upstream filtering, coordinated takedowns, and bank-side frictions. ACMA's codes have sustained very high-volume blocking of malicious traffic, which reduces exposure to first-contact lures, and the early EDR jurisprudence has narrowed a frequent institutional defence in impersonation contexts. At the same time, investment scams continue to dominate total losses, reflecting displacement towards higher-value targets and the ability of criminal networks to recruit and funnel victims via social-platform advertising and encrypted messaging.

Consumer advocates and parts of the press have criticized the SPF as "lacking teeth" because it raises duties and penalties without guaranteeing compensation; the Government's rationale, set out in parliamentary materials, is to avoid concentrating costs solely on banks and to create prevention incentives across the whole scam chain, banks, telcos, and platforms, while leaving redress to EDR where entities fall short of their obligations.

In sum, Australia now operates a whole-of-ecosystem prevention regime with penalties and centralised EDR, rather than a statutory reimbursement right for all APP victims. Compared to the EU's current position, Australia goes further in codifying cross-sector responsibilities and in empowering regulators to set and enforce sector codes. Still, it remains behind the UK's mandatory reimbursement model. The trajectory for 2025/26: CoP roll-out,[177] a compulsory Sender ID register[178], platform-sector codes under the SPF, and continued AFCA jurisprudence, will determine whether the prevention-first approach can deliver sustained reductions in APP losses and more predictable redress, or whether pressure will build for a UK-style presumption of reimbursement.

ACMA reports hundreds of millions of blocked scam calls/SMS per year under the Scam Calls/SMS codes, an essential "first-mile" mitigation given that many APP scams start with spoofed bank/government messages and a fake ad funnel.[179]

---

[176] Austelco, "Communications Alliance Ltd; REDUCING SCAM CALLS and SCAM SMS", https://www.austelco.org.au/wp-content/uploads/2025/06/C661_2022.pdf, last accessed 3 September 205.

[177] Confirmation of Payee (CoP) is scheduled for roll-out starting July 2025 across Australian banks, providing a name-checking control on account-to-account payments aimed at preventing misdirected payments and APP scams.

[178] The mandatory SMS Sender ID Register is expected to come into effect by December 2025, requiring all alphanumeric SMS sender IDs to be registered and approved by ACMA to reduce brand impersonation scams ("alpha tags")

[179] ACCC, "Scamwatch/National Anti-Scam Centre), Targeting Scams Report 2024" (published on 11 March 2025), https://www.scamwatch.gov.au/sites/default/files/targeting-scams-report-2024.pdf, last accessed 25 August 2025.

9.6 Comparative analysis: United Kingdom, Australia, and Singapore

The three most developed responses to APP fraud show distinct choices in scope, liability allocation, enforcement architecture, and consumer-conduct standards.

The UK adopts a reimbursement-first model on FPS with a mandatory 50:50 PSP split and a narrow gross-negligence carve-out for PSUs. Coverage is channel-specific; cards, BACS, CHAPS, and cross-border transfers are excluded, and FOS anchors enforcement as a binding ADR. The model directly addresses induced-consent losses on covered rails but leaves residual exposure on non-covered rails (see Section 9.2).

Singapore runs a prevention-first design. SRF allocates phishing-vector duties across banks and telcos, while EUPG governs unauthorised transactions; there is no general APP reimbursement right for investment or purchase scams. An operational hub (ASCom) accelerates freezes and recalls, which hardens the first mile yet can leave induced-consent victims without ex post compensation (see Section 9.4).

Australia´s SPF imposes enforceable codes and controls on banks, telecoms, and platforms (e.g., sender/recipient screening, name-checking roll-outs, scam-ad filtering). AFCA provides external dispute resolution on a case-by-case basis; no blanket APP reimbursement exists. The framework prioritises upstream risk reduction and penalties for weak controls, with compensation routed through EDR rather than statutory reimbursement (details in Section 9.5).

In short, the UK is channel-specific and reimbursement-first; SG is vector-specific and prevention-first; Australia is sector-specific and prevention/EDR-first. Enforcement architectures differ, FOS (UK), EDR-centric pathways (AU), and an operational police–bank hub (ASCom, Singapore), as do consumer standards (UK's narrow gross-negligence, Singapore´s enumerated user duties, Australia´s code-based obligations). Reimbursement models deliver predictable redress on covered rails but risk displacement to excluded channels, while prevention-first models reduce attack surfaces but can under-compensate victims.

Effective policy, therefore, combines reimbursement for induced-consent losses on core rails with complex upstream duties across the fraud/scam chain, including inbound risk scoring, mule-account controls, and ad-funnel and telecom filtering.

10. The PSR Proposal: Progress and Blind Spots in Europe's Response to Payment Fraud

Chapters 7–9 traced the evolution from PSD1/PSD2 to today's APP fraud gap and compared international responses. This chapter evaluates how far the PSR/PSD3 package intends to close Europe's gap, focusing on Article 59's trigger, prevention tooling, and the trilogue choices that determine consumer outcomes.

The Payment Services Regulation (PSR) is now the Union's principal instrument for repairing PSD2's enforcement gap: while PSD2 foresees redress rules for unauthorised fraud, victims of fraudulently induced, but technically authorised, transfers remain largely unprotected, and national divergences erode both harmonisation and market confidence. The Commission's proposal of 28 June 2023[180] acknowledged the problem but kept a narrow, technique-based trigger focused on bank impersonation. Parliament's text broadened protection to the economic reality of deception and experiments with shared liability across sectors. The Council's approach, published as of 18 June 2025,[181] retreats to the Commission's narrow scope while layering in useful prevention tools.

10.1 The Legislative Genesis: From Crisis Recognition to Policy Response

PSR's rationale is threefold. First, APP losses persist despite SCA and risk-based monitoring; criminals have shifted from credential theft to psychological manipulation. Second, redress and supervision remain fragmented: national authorities apply divergent standards and victims face uneven outcomes, undermining the promise of the single market. Third, market entry for innovative PSPs is impeded by inconsistent consumer protection, which raises the cost of compliance and depresses user trust. The Commission recognised these failures in its Impact Assessment,[182] but the architecture still relies on the PSR for directly applicable user rights while PSD3 modernises supervisory scaffolding. In practice, durable improvement in consumer protection against scams must be delivered in the PSR text itself. Whether the PSR succeeds turns on a single threshold question: will reimbursement remain limited to PSP Impersonation cases, or shift to an outcome-based standard of "fraudulently induced payment" that treats consent obtained through deception as invalid, and thus reclassifies the transaction as unauthorised, paired with explicit liability and prevention duties for PSPs, electronic communications service providers (ECSPs), and online platforms.

---

[180] 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 COM/2023/367 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0367.

[181] European Council, "Council agrees its position on a more modern payment service framework in the EU" (press release 18 June 2025), https://www.consilium.europa.eu/en/press/press-releases/2025/06/18/council-agrees-its-position-on-a-more-modern-payment-service-framework-in-the-eu/, last accessed 3 September 2025.

[182] European Commission, *Commission Staff Working Document: Impact Assessment Report* accompanying the Proposal for a Regulation on payment services in the internal market and amending Regulation (EU) No 1093/2010 and the Proposal for a Directive on payment services and electronic money services in the internal market (Brussels, 28 June 2023) SWD(2023) 231 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023SC0231.

10.2 Parliamentary Expansion: The Belka Report

The European Parliament's response to the Commission proposal, led by Marek Belka (Rapporteur, S&D, Poland), represented a significant improvement in consumer protection. The Parliament's amendments, adopted by the Economic and Monetary Affairs Committee on 14 February 2024 and confirmed by the full Parliament on 23 April 2024,[183][184] transformed the PSR from a technical adjustment into a comprehensive reform attempt.

The Parliament significantly expanded fraud coverage beyond the Commission's narrow focus on institutional impersonation. This expansion encompassed a definitional broadening through the extension of reimbursement rights to fraud involving "any relevant public or private entity".

The Parliament's most controversial innovation was the introduction of a shared liability framework extending beyond payment service providers to include Electronic Communications Service Providers (ECSPs) and online platforms. This framework established multi-sector responsibility and recognised that modern fraud operations exploit vulnerabilities across multiple industries. It proposed functional liability allocation by distributing responsibility based on control over fraud vectors, rather than traditional sectoral boundaries. This approach aimed at creating prevention incentives by establishing financial incentives for fraud prevention across the scam chain.

10.3 Article 59: The Core Provision Analysis

Article 59 of the Parliament's version represents the heart of the PSR's approach to APP fraud protection. The provision applies exclusively to "impersonation fraud" with specific definitional requirements that encompass institutional impersonation where fraudsters must unlawfully use the name, email address, or telephone number of the consumer's payment service provider, public authority impersonation requiring fraudsters to impersonate government agencies, law enforcement, or regulatory authorities, and private entity impersonation where, in the Parliament's expanded version, fraudsters must impersonate any relevant private entity. The framework includes an attribution requirement mandating that contact details must be "attributed to such entity," creating potential for definitional manipulation, alongside a causation standard requiring consumers to authorise payments they would not have authorised without the deception.

This definitional approach creates several problematic outcomes. The framework establishes arbitrary distinctions where protection depends on criminal technique rather than victim harm or deception sophistication, while simultaneously creating criminal adaptation incentives by providing clear guidance for criminals on how to structure schemes to avoid liability. The approach generates victim confusion through identical victim experiences receiving different

[183] European Parliament, Report of the ECON-Committee (Rapporteur: Marek Belka) zum PSR-Entwurf (A9-0281/2023 dated 24 October 2023), OEIL-Document 1784188, https://oeil.secure.europarl.europa.eu/oeil/en/document-summary?id=1784188, last accessed 25 August 2025.
[184] European Parliament legislative resolution of 23 April 2024 on the 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 (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD))

treatment based on technical distinctions, and produces enforcement complexity through complex definitional requirements that enable institutional manipulation and avoidance.

10.4 Council's General Approach (GA) (18 June 2025): what changed, and what didn't

On 18 June 2025, the Council of the EU adopted its negotiating mandate on the PSR/PSD3 package. The Council's press release[185] stresses three priorities: (i) tackling fraud (with a specific nod to "spoofing" of banks), (ii) rolling out EU-wide name/IBAN checks (Confirmation/Verification of Payee), and (iii) more transparency on card-scheme fees and ATM pricing. It also brings electronic communications service providers (ECSPs) explicitly into the *prevention* perimeter, information-sharing, liaison channels, and a voluntary code, while pointedly *not* making them liable to reimburse victims.

Substantively, the Council narrows Parliament's consumer protection ambition on APP fraud and aligns much more closely with the Commission's original proposal:

- Article 59 remains limited to PSP Impersonation ("spoofing") only: The Council rejects Parliament's expansion to impersonation of "any relevant public or private entity." In other words, reimbursement duties in the PSR would attach only where the fraudster impersonated the customer's PSP,[186] not the police, a tax authority, or a private firm.

- Refund clock: 15 business days: The Council lengthens the refund deadline for in-scope Article 59 cases from 10 to 15 business days. It clarifies that consumers must provide their PSP with the relevant information they can reasonably be expected to have about the events leading to the payment.[187]

- For ECSPs' cooperation, not reimbursement is laid out. Unlike Parliament's text (which contemplated ECSP liability where illegal content wasn't removed after notice), the Council Article 59a would oblige ECSPs to set up dedicated PSP communication channels and participate in information-sharing or a Union-level voluntary code of conduct to prevent/fight scams. National authorities may require ECSPs to block access to numbers/services used for fraud (aligned with the EECC), but stop short of imposing reimbursement duties on them.[188]

- Confirmation/Verification of Payee across *all* credit transfers: The Council would leverage the recent SEPA amendments and extend the "name-matches-IBAN" check beyond SEPA-euro transfers to *all* credit transfers in the Union.

[185] EU Council, Press release, „Council agrees its position on a more modern payment service framework in the EU" (18 June 2025), https://www.consilium.europa.eu/en/press/press-releases/2025/06/18/council-agrees-its-position-on-a-more-modern-payment-service-framework-in-the-eu, last accessed 25 August 2025.
[186] Hogan Lovells, "PSD3: COREPER approves Council of EU's amended PSD3 and PSR texts, paving the way for inter-institutional negotiations on final texts" (News from 23 June 2025), https://www.hoganlovells.com/en/publications/psd3-coreper-approves-council-of-eus-amended-psd3-and-psr-texts-paving-the-way, lad accessed 24 August 2025.
[187] Hogan Lovells, idbd, F,n 99.
[188] Hogan Lovells, *idbd,* Fn 99.

- Blocking suspicious payments: The Council mandate adds/clarifies the ability for the payer's and payee's PSPs to block or reject payments on fraud grounds (Articles 65 and 69), while also adding that an "unusual" payment alone isn't enough to suspect fraud.

- More on fraud/data sharing & platform (Article 83, Article 83a, 83b) and fees: The mandate strengthens timely cross-industry fraud information sharing (with data-protection guardrails)and requires greater transparency around card-scheme/processing fees and ATM charges presented to users *before* a transaction.

10.5 Critical Limitations and Blind Spots

The Council's PSR GA suffers from several critical limitations that undermine its effectiveness in addressing the consumer protection crisis.

The Council narrows Article 59 back to PSP Impersonation only. It stops short of imposing reimbursement duties on ECSPs or platforms in any circumstance, confining them to cooperation-only roles. The Council kept "gross negligence" out of the binding Articles and instead added Recital-level guidance. Stating that Gross Negligence (GN) "means more than mere negligence," assessment should generally follow national law, and a non-exhaustive list of factors/examples may be considered (such as ignoring a clear, case-specific PSP warning; storing credentials with the instrument, etc.). The PSR proposal does not create an EU-level binding ADR requirement and leaves Member State redress heterogeneity largely intact. In short, the Council's PSR proposal may improve prevention tooling, but leaves the reimbursement perimeter tight and the redress architecture weak, precisely where PSD2 already struggled.

The regulatory framework prioritises technical criminal categorisation over victim experience relevance, while simultaneously facilitating criminal adaptation by providing clear guidance on structuring schemes to avoid regulatory coverage. This creates a violation of justice principles where identical victim harm receives different treatment based on arbitrary technical distinctions.

Without installing a working European-wide ADR scheme and not narrowly defining gross negligence, the PSR perpetuates the fragmented enforcement structure that has proven systematically inadequate under PSD2. The proposal preserves existing alternative dispute resolution systems despite their proven structural inadequacy and lacks automated systems for monitoring institutional compliance with consumer protection obligations.

10.6 "van Praag's model" / "Council's approach vs. van Praag's" Proposal (EBI WP 190, May 2025).

As Emanuel van Praag and co-authors have noted in their paper[189] *Authorised Push Payment Fraud: Suggestions for the Draft Payment Services Regulation,* extending EU-level APP fraud liability beyond narrow PSP Impersonation to scams that abuse public trust in the payment

[189] Emanuel van Praag, "Authorised Push Payment Fraud: Suggestions for the Draft Payment Services Regulation" (EBI Working Paper No. 190, 05 May 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5241100, last accessed 25 August 2025.

system, such as impersonation of a regulator, central bank, supervisor or police, because these attacks undermine confidence in banking itself, while leaving other scenarios (WhatsApp, investment scams, romance scams, invoice scams) to Member-State discretion via national duty-of-care rules. They favour implementing this by creating a distinct PSR liability ground (rather than redefining "authorised"), coupled with a narrow gross-negligence exception that the PSP must prove, ideally articulated in Article 59 and illustrated in the Recitals, so that GN remains a very narrow carve-out. Beyond scope, they urge the PSR to codify operational prevention duties, precise monitoring and warning obligations, proportionate frictions (temporary suspension, configurable/default limits for high-value instant transfers), and ceilings on intervention to avoid paternalistic blocking and undue privacy intrusions, plus a "sufficient action" standard under which, after adequate warnings and justified frictions, continued customer insistence may flip liability to the payer (broadly aligned with the UK model). They also address "moral hazard", finding it overstated, mainly given the trauma, uncertainty, and effort involved in reimbursement, with only narrow exceptions (such as non-delivery in online purchases).

By contrast, Council's 18 June 2025 GA keeps Article 59 limited to PSP Impersonation, lengthens the refund clock to 15 business days, adds a consumer cooperation duty, expands IBAN–name checks beyond SEPA-euro transfers, strengthens fraud-data sharing, and brings ECSPs into cooperation channels/voluntary codes, but not into reimbursement liability. It does not adopt van Praag's broader liability perimeter,[190] does not define a narrow GN standard in the operative text, and does not codify an explicit "sufficient action" safe harbour; GN guidance appears only in Recitals and application is mainly left to national law (unlike the Parliament's call for EBA guidance). In short, the Council essentially adds prevention tooling while retaining a tight reimbursement perimeter, diverging from van Praag's systemic alignment of incentives.

10.7 Trilogue outlook: two viable landings and their consumer protection delta

Two coherent compromises are visible. A narrow landing would look like the Council's text: reimbursement only for PSP Impersonation; PSP-ECSP cooperation without liability; EU-wide CoP; stronger SCA and supervision; fifteen-day refund clocks.

A broad landing would follow Parliament on substance: an outcome-based trigger for fraudulently induced payments; default PSP loss-sharing with calibrated rights of recourse; conditional duties for ECSPs/platforms tied to functional control over first-mile vectors; EBA to issue guidelines on the definition of "gross negligence" within 12 months, and binding ADR (FIN-NET 2.0) enforcement. The consumer protection delta between these landings is substantial. The narrow landing hardens rails but leaves most APP victims outside reimbursement and preserves uneven redress. The broad landing aligns incentives across the scam chain and creates predictable victim outcomes, with prevention and liability mutually reinforcing.

190

11. Conclusion: Restoring Trust in Europe´s Payment Rails

Europe is confronting a genuine public-interest crisis in online fraud. Central banks, consumer authorities, and law-enforcement bodies now widely recognise large-scale digital fraud as a systemic threat to society. Yet the single market remains highly exploitable for scammers because corrective measures, while underway, remain fragmented and insufficiently coordinated. A central gap is the absence of an EU-level fraud data-sharing framework, leaving policymakers and supervisors without comparable, timely evidence. As instant payments move into mass adoption in Europe and irrevocability will become the norm, fraud losses will accelerate in both speed and scale.

Crucially, online fraud always depends on payment channels to turn deception into profit; every scam ultimately needs a pathway for stolen funds to get laundered and to reach the offender. This dependency creates the strongest opportunity for intervention: payment service providers, with their information, technical capacity, and real-time controls, are uniquely positioned to tackle fraud at the point where it becomes financial, from detection and interdiction to recovery.

11.1 The Payment Paradox Identified

From the outset, the European Union made a clear promise: modernising and harmonising payment rails would not diminish consumer protection but enhance it. PSD1 as well as PSD2 enshrined the principle that payment service providers PSPs, **as system designers and operators,** must bear the risks of fraud and execution failure. The Digital Finance Strategy (September 2020)[191] reiterated this principle, stressing that innovation and competition in the payments market must go hand in hand with consumer trust, and that digital finance would only succeed if users were guaranteed the same level of protection as in traditional finance.

PSD1 codified this principle explicitly:

- *Article 60(1)* required PSPs to refund unauthorised transactions “without delay,” restoring the account to its prior state.
- *Article 61* capped the consumer’s liability for losses due to lost, stolen, or misappropriated instruments at €150, save for fraud or gross negligence.
- *Article 59* placed the burden of proof on the PSP to show that a disputed transaction was authenticated, accurately recorded, and not affected by technical failure.
- *Recital 34* emphasised that trust in electronic payment instruments requires limiting payer liability, and that Member States could reduce the cap further to strengthen consumer confidence.

PSD2 reaffirmed and strengthened this consumer protection baseline:

[191] European Commission, Digital Finance Strategy (COM(2020) 591 final 24 September 2020); European Commission, Retail Payments Strategy (COM(2020) 592 final 24 September 2020).

- *Recital 85* makes explicit that execution risk belongs to the PSP, since "the payment service provider is responsible for the correct execution of the payment transaction," including the organisation of intermediaries and recall procedures.

- *Recitals 95–96* further imposed risk-proportionate security duties on PSPs, requiring authentication measures that "dynamically link" the user to the payee and amount.

- *Articles 72 and 74* imposed a harmonised €50 liability cap on consumers and mandated immediate refund of unauthorised transactions, except where the PSP can prove payer fraud or gross negligence.

- *Article 72(2)* confirmed that the *use of payment credentials alone does not prove authorisation,* thereby rejecting formalistic arguments that mere technical authentication suffices to shift liability.

Both directives thus articulated a technology-neutral consumer protection framework. Regardless of the channel or instrument, PSPs were to bear liability for unauthorised or improperly executed payments, save for narrow exceptions. This allocation was not incidental; it was designed to ensure public trust in payment rails and to prevent consumers from being the residual risk-bearers of systemic vulnerabilities.

The paradox emerges in the present crisis.

While the EU has succeeded in constructing one of the world's most advanced electronic and real-time payment infrastructures, it has become evident that it has failed to establish an adequate liability framework and an effective enforcement architecture. Victims deceived into authorising transfers are left to bear the full loss, even though PSD1 and PSD2 intended payment service providers, who operate and control the payment rails, to absorb fraud risks. Worse still, even victims of clearly unauthorised transactions often fail to obtain refunds because providers deny claims, dispute resolution is ineffective, and supervisors rarely enforce the rules.

The result is a double failure: a liability gap for APP fraud and an enforcement gap for unauthorised fraud. Together, these gaps amount to a reversal of the very promise on which Europe's electronic and digital payments framework is built. Instead of upholding consumer protection as the cornerstone of trust, the current regime abandons it at the moment of greatest vulnerability.

11.2 The Reform Imperative: Fundamental Principles for Change

Resolving the paradox identified in 11.1 requires more than incremental adjustments as proposed in the Council's PSR proposal; it requires re-anchoring European payment law in the foundational principles that justify liability allocation in the first place.

Four principles are decisive.

First, **consumer protection** must be the cornerstone of European payment regulation. From PSD1 through PSD2, and as crystallised in the 2020 Digital Finance and Retail Payments

Strategies, the EU has pursued a technology-neutral framework that is supposed to ensure a high level of consumer protection for electronic (and, by extension, digital) payment services, comparable to traditional channels. This baseline is what sustains trust in digitalisation.

Second, **liability must follow functional control over risk.** Payment service providers are not only the parties who benefit from digitalisation; they are the only actors who can meaningfully prevent and mitigate fraud. As system operators, PSPs design authentication procedures, deploy monitoring systems, onboard merchants, control the execution, organise intermediaries, and have the ability to freeze or recall transfers. Consumers possess none of these capacities. They cannot run anomaly detection, verify IBAN ownership, or suspend suspicious flows; their role is structurally limited to providing consent at the interface. For this reason, Recital 85 of PSD2 explicitly recognises that "the payment service provider is responsible for the correct execution of the payment transaction" precisely because it designs and controls the system and its intermediaries. Liability must therefore track the actor who controls risk and is best placed to prevent loss, the PSP.

Third, **liability must also reflect a fair and economic justice**. PSPs have captured unprecedented efficiency gains from the government-led modernisation of payment rails, reduced processing costs, increased profitability, and streamlined operations. Yet at the same time, consumers have been forced to absorb the downside risks of digitalisation, particularly in cases of APP fraud. This inversion violates the principle of *qui bono, cui malum*: those who reap the benefits must also bear the corresponding risks. Functional control and economic justice thus result in the same conclusion: PSPs must internalise fraud risks rather than externalise them onto deceived consumers.

Fourth, **rights must be enforceable.** PSD2 already codified strong duties, immediate reimbursement for unauthorised transactions (Art 73), liability caps (Art 74), and a clear burden of proof on PSPs (Art 72). Yet the enforcement gap has rendered these rights illusory: PSPs routinely deny refunds, supervisors decline to intervene, and ADR mechanisms fail to deliver outcomes. Rights without credible enforcement are not rights at all, but abstractions. Reform must therefore equip supervisory and redress bodies with binding powers, resources, and timelines sufficient to ensure that consumer protection duties are observed in practice.

Together, these principles define the reform imperative. They make clear that consumer protection is not an obstacle to innovation, but rather its precondition. Liability must follow both functional control and economic benefit, and rights must be backed by enforcement capable of delivering results. Without re-embedding these principles, Europe's Digital Finance Strategy will continue to rest on unstable foundations: technological sophistication coupled with institutional abandonment**.**

11.3 Consent given under Deception is not Consent: Fraud is Fraud.

The current European approach to fraud protection still lacks a reasoned justification. PSD2 defines a payment transaction as "authorised" when the payer consents in the manner agreed with the provider (Art 64(1)), and imposes strict refund duties only for "unauthorised" transactions (Art 72–74).

This distinction undermines the technology-neutral design of PSD1 and PSD2. Both directives were crafted to ensure that protection applies regardless of instrument or channel. PSD1 Recital 34 stressed that trust in electronic payments requires liability limitations independent of the instrument's form. PSD2 Recital 85 explained that liability rests with providers because they design and control execution, not because of the technical path by which fraud occurs. By treating deception-induced consent as legally equivalent to genuine consent, the current framework abandons this principle of neutrality and creates arbitrary disparities in victim protection.

The proposed Article 59 exacerbates this problem by limiting reimbursement to PSP Impersonation fraud, where the criminal unlawfully uses the name, contact details, or brand of the consumer's bank. This categorical limitation excludes the majority of APP fraud cases, including investment scams, romance scams, and false authority scams.

We propose treating fraud-induced payments as unauthorised transactions, effectively redefining "authorisation" in current payment law. This change restores technology-neutral consumer protection by recognising that **consent given under deception is not genuine consent**. It allows the full use of existing PSD2 remedies, such as shifting the burden of proof, immediate refunds, and narrow grounds for refusal. It aligns with recent research highlighting inconsistent national practices. Combined with precise monitoring and warning duties, proportionate friction measures, and a "sufficient action" standard, this approach creates aligned incentives throughout the payment chain without resorting to paternalistic blocking or invading privacy. Unlike the Council's narrow definition focused on PSP Impersonation, this reclassification ensures predictable remedies across all payment methods and fulfils the EU's goal of equal protection for payment channels.

Full reimbursement for fraud-induced payments does not create reckless moral hazard; it corrects asymmetric risk allocation and fulfils the Union's promise of equivalent or better protection. As van Praag observes[192], moral hazard is unlikely in most scenarios, given the trauma of victimisation and the uncertainty and effort required to obtain compensation.

11.4 Detailed Fraud Data as a Precondition for Liability Frameworks

Any comprehensive liability framework presupposes a robust empirical foundation. Europe cannot credibly protect consumers while operating in what amounts to a statistical vacuum. Unlike the UK, Singapore, the US and Australia, where detailed taxonomies of fraud categories underpin both prevention strategies and liability rules, the EU still relies on highly aggregated figures that obscure which scams drive the majority of losses. The absence of harmonised typologies and mandatory, comparable reporting across Member States means that thousands of victims remain statistically invisible, while policymakers are left without a reliable evidence base.

To address this structural gap, a European Fraud Data Framework is required. Such a framework should: (i) establish standardised fraud categories (investment, romance, impersonation, purchase scams); (ii) oblige payment service providers and law enforcement bodies to report consistently against these categories; and (iii) require Member States to provide accessible

[192] Emanuel van Praag, ibid, 14-16

digital portals for fraud reporting. Only based on transparent, harmonised, and credible data, liability rules can be designed reasonably, enforced consistently, and adapted to the evolving methodologies of organised crime. Without this empirical foundation, even the most ambitious reforms risk remaining arbitrary, unbalanced, and vulnerable to industry pushback.

11.5 Institutional Reform: Building Effective Enforcement Architecture

Even the most comprehensive liability rules are meaningless if they are not enforced. The experience under PSD2 demonstrates this with stark clarity. Despite unequivocal statutory duties, such as the obligation to refund unauthorised transactions without undue delay (Article 73 PSD2) and to cap consumer liability at €50 (Article 74 PSD2), victims routinely fail to obtain redress. Banks reject claims on spurious grounds, national competent authorities (NCAs) decline to intervene, and alternative dispute resolution (ADR) mechanisms prove inaccessible or ineffective. In practice, rights have remained primarily on paper.

Rights without remedies are illusory. This principle, adequate judicial protection and Member-State liability for breaches of EU law, was articulated in *Francovich* (C-6/90 and C-9/90)[193] and consistently reaffirmed across consumer protection jurisprudence. Where Member States fail to ensure effective enforcement of EU rights, the Union's legal order is undermined. Payment services regulation cannot be an exception: if PSPs are obliged to reimburse victims, institutions must exist to ensure compliance.

Mandates for the different enforcement authorities must be clarified so that consumer protection obligations are binding, not aspirational. Performance standards for enforcement authorities should be codified in law, with measurable indicators (reimbursement rates, resolution times, enforcement actions). National Competent Authorities must publish regular reports enabling democratic oversight, and non-compliance must trigger automatic penalties. Supervisory independence must be strengthened to curb industry capture, with governance that reduces reliance on industry consultation and embeds formal roles for consumer representatives.

Consumer protection authorities need sanctioning powers that exceed the gains from non-compliance, ensuring negligence becomes a financial liability. Automated supervisory monitoring using real-time transaction data should detect patterns of institutional negligence rather than relying solely on individual complaints.

Europe requires a two-pillar enforcement architecture: The EBA, or a new Union body, must be vested with direct powers to investigate, sanction, and remedy consumer protection breaches. This includes authority to impose binding obligations, levy penalties, and require restitution for systemic failures. Reliance on national discretion has proven untenable in a cross-border payments market. A (cross-border) European Financial Ombudsman with binding authority (FIN-NET 2.0): For Scammers, there are no borders in Europe; let us address them accordingly. Consumers need a direct, accessible channel for redress with decisions that PSPs cannot ignore. Such an ombudsperson should be industry-funded, staffed with specialised expertise in fraud and digital payments, and empowered to handle cross-border cases efficiently. Binding

[193] https://curia.europa.eu/juris/showPdf.jsf?docid=97223&doclang=EN, accessed 3 September 2025.

authority and statutory deadlines for resolution (e.g., 90 days) are essential to prevent victim exhaustion and restore trust.

A strong enforcement architecture is not merely complementary to liability reform; it is indispensable. Expanding liability coverage without enforcement creates false expectations and deepens disillusionment. Conversely, robust enforcement ensures that liability rules function as intended, incentivising PSPs to invest heavily in prevention and in exposing the ones who fail their high standards.

11.6 Multi-Stakeholder Liability Framework

Modern fraud operations exploit not only the financial system but the entire digital ecosystem in which consumers operate. A liability framework that focuses exclusively on PSPs, therefore, misses critical actors whose infrastructures are exploited at scale.

Accordingly, liability should not be shared mechanically but allocated according to the degree of functional control and risk exercised by each actor. The institution or organisation that failed to act where it had the clearest prevention duty must bear the liability.

EFRI´s dataset evidence that where PSPs rigorously apply KYC/EDD, merchant monitoring, and MCC governance, they are largely absent from the fraud chains or appear only at the margins. Where standards are relaxed, or high-risk business is consciously pursued, PSPs become the monetisation engine for scams. Liability should therefore follow risk acceptance and functional control: institutions that choose to board high-risk merchants, tolerate MCC camouflage, or ignore monitoring alerts should bear a default reimbursement duty for victims whose payments were processed over their rails, with appropriately calibrated rights of recourse upstream or downstream.

The United Kingdom's new reimbursement regime splits liability 50:50 between sending and receiving PSPs, regardless of which party failed. While simple, this model weakens incentives: if both actors know their maximum exposure is capped at half, they may underinvest in prevention. Moreover, it produces inequitable outcomes, as seen in cases like Payvision BV or Københavns Andelskasse, where a single institution's compliance failures were decisive; an equal split would dilute responsibility rather than enforce it.

Based on our research, we think that liability should be:

Fault-based and control-driven: The party whose failure to discharge its regulatory duties (e.g., KYC/EDD, transaction monitoring, anomaly detection, blocking, or recall duties) enabled the fraud must bear the loss.

Joint and several liability applies when multiple failures occur: If both the sending and receiving sides demonstrably breached duties, they should be jointly and severally liable, leaving allocation between them to recourse actions.

Rebuttable presumption. Where it is unclear which party failed, liability should fall on both by default, unless one can demonstrate compliance with its obligations. This ensures that no victim is left uncompensated.

Extending liability beyond banks: Telecoms and digital platforms must be included in this framework. Caller-ID spoofing, fraudulent SMS, and social-media advertising are critical first-mile enablers of fraud. Where these providers fail to implement adequate preventive controls, such as sender-ID verification, ad-buyer screening, or timely takedowns, they too should bear liability for resulting losses. The same principle applies: control entails responsibility; failure involves liability.

The consumer-facing PSP as reimbursement anchor: On grounds of efficiency and fairness, the payer´s PSP should be the reimbursement anchor. Victims cannot reasonably be expected to identify or litigate against foreign beneficiary institutions, acquirers, telecom operators, or social media giants. The ASPSP is responsible for the customer relationship and is accessible; once it has reimbursed the victim, it can pursue recourse against the failing actor(s) in the chain. This mirrors the card-scheme trust architecture, issuers reimburse cardholders and recover from acquirers/merchants, delivering rapid redress while internalising costs within the industry, which has the information and capacity to allocate liability efficiently.

Where chain opacity precludes timely attribution of the control failure, the reimbursement anchor remains the payer's PSP (with recourse preserved); otherwise, industry-created information deficits are converted into default consumer losses. This approach aligns with the principle that liability follows functional control and that recourse is resolved within the industry rather than by individual victims.

The decisive feature of this framework is that liability allocation occurs *behind the scenes*. Victims must receive reimbursement swiftly from their PSP; disputes about ultimate responsibility are resolved among providers afterwards. This creates certainty for consumers while ensuring that financial and technological institutions retain strong incentives to monitor and mitigate fraud risks proactively.

Our proposed Shared Liability Framework also requires a narrow, evidence-based Consumer Standard of Caution definition, due-process guardrails, prompt reporting (filing criminal complaints), and cooperation duties so that opportunistic claims are deterred and calls for a narrow definition of gross negligence (PSP bears the proof; vulnerable users excluded).

11.7 Embedding Technology and Innovation Obligations

Liability and enforcement mechanisms alone are insufficient if the technological architecture of payments does not incorporate robust preventive capacities. A comprehensive European response must therefore embed state-of-the-art technology obligations into the liability framework, ensuring that fraud prevention becomes a mandatory feature of digital finance.

The central weakness of PSD2's technical framework was its static design. Accordingly, a sustainable framework requires outcome-based technology duties: PSPs and other actors must be obliged to deploy fraud-prevention systems commensurate with the risk, adapting continuously as threats evolve. This principle already appears in PSD2 Recital 96, which requires security measures to be "compatible with the level of risk," but it has not been operationalised into enforceable standards.

Core technology obligations for a reformed Framework should be

1. Real-time transaction monitoring and anomaly detection. PSPs must deploy systems capable of identifying transactions inconsistent with a customer's behavioural profile (e.g., sudden large transfers abroad, unusual payment references, new high-risk beneficiaries).

2. Risk-based intervention tools. Systems must not only detect but also respond, through step-up authentication, cooling-off periods for high-risk payees, or mandatory manual review. Consumers should be clearly warned where anomalies indicate elevated fraud risk.

3. AI-enhanced fraud analytics. Criminal networks already employ machine learning to optimise victim targeting. PSPs and platforms must be required to invest in equivalent or superior technologies for fraud detection, pattern recognition, and predictive analysis.

4. Cross-sectoral data-sharing. Fraud is often detected only when multiple incidents across institutions are aggregated. EU law must mandate structured, privacy-compliant sharing of fraud intelligence between PSPs, telecom operators, and platforms, overcoming the silos that criminals exploit.

5. User-empowering tools. Consumers must be given control mechanisms such as configurable transaction limits, "kill switches" to block outgoing transfers, and transparent alerts that communicate risk in clear, non-technical language.

The Union's future framework must embed technological innovation as a regulatory obligation, not an optional investment. Fraud prevention cannot be left to the goodwill of providers but must be enforced as a legal duty proportionate to risk. Outcome-based standards, binding monitoring requirements, AI-enabled detection, and consumer-empowering tools must become core features of the European payment architecture. Only by integrating liability with technological obligation can Europe prevent fraud effectively while sustaining consumer trust in digital finance.

11.8 The Crisis of Trust and Its Far-Reaching Consequences

The most profound consequence of institutional failure is not the scale of financial loss but the erosion of trust. Trust is the foundation upon which financial systems, democratic governance, and economic innovation depend. When consumers are systematically abandoned after fraud, the damage extends far beyond individual victims to the very legitimacy of Europe's digital art.

The data reveal that institutional betrayal is often more traumatic than the fraud itself. Whereas the criminal deception undermines personal judgment, the denial of redress by trusted institutions destroys confidence in the very systems meant to provide protection.

We disagree with van Praag's premise[194] that abuse of trust in the payment system consists chiefly of PSP Impersonation or impersonation of public authorities. Trust collapses when victims are left without assistance by their ASPSPs and other institutions after they seek

[194] Emanual van Praag, ibid, 3–4 (key concl. (iv)), 9–12 (sect. 4).

warnings, intervention, and recovery. The core breach lies not only in the deception but in the institutional failure to protect and remediate.

Institutional abandonment does not remain confined to individual victims. The loss of trust is communicated to family members, peers, and professional networks, creating collective scepticism toward digital innovation.

The trust crisis generates significant direct and indirect costs. Direct costs include healthcare expenses linked to trauma, legal costs from forced individual litigation, and social services expenditures for those financially devastated by fraud. Indirect costs include reduced willingness to adopt new financial technologies, diminished competitiveness of European PSPs compared to international providers offering superior protection, and capital flight toward jurisdictions with more predictable frameworks. In aggregate, these effects threaten the economic rationale for Europe's digital finance strategy: technological investment without corresponding consumer trust produces declining returns.

11.9 Final Call: Fundamental Reform Imperative

The choice before European policymakers is stark. Either they undertake fundamental reform that restores accountability and makes consumer protection enforceable, or they allow the present system of institutional abandonment to persist. The latter path guarantees the continuation of widespread fraud victimisation, further erosion of public trust, and long-term damage to Europe's economic and democratic foundations. The urgency is not abstract: every day without reform transfers the costs of digitalisation from institutions onto vulnerable consumers, while criminal enterprises strengthen their hold on Europe's financial infrastructure.