How to ensure a safer future for retail payments: Aligning fraud prevention and accountability in the EU

Judith Arnal

Policy Brief

Summary

Retail payment fraud is a structural challenge that no longer falls solely within the remit of payment service providers (PSPs). As transactions flow through increasingly fragmented digital ecosystems, the mismatch between where fraud occurs and where liability falls is becoming unsustainable.

This ECRI Policy Brief examines how modern fraud exploits institutional asymmetries and identifies why a realignment of preventive duties and financial responsibility is needed. Drawing on international experiences – from Singapore's cascading liability model to the UK's reimbursement regime – it argues that effective fraud prevention requires proportional accountability across the full value chain. It then turns to the evolving European regulatory framework, highlighting its ambition but also its structural and legal constraints.

Finally, three policy recommendations are provided, specifically to foster meaningful cross-sectoral cooperation, to clarify data-sharing rules and to institutionalise shared accountability mechanisms.

The key message is that fraud prevention and accountability aren't separate goals and shouldn't be treated as such – instead, they're really two sides of the same coin.

The growing threat of fraud in retail payments – evidence and typologies

Few issues illustrate the tension between digital efficiency and systemic vulnerability more clearly than fraud in retail payments. What was once considered a marginal problem within the financial sector has become a structural challenge at the intersection of technology, regulation and trust. As new actors and platforms enable ever faster and more seamless transactions, they also create new opportunities for manipulation, deception and abuse. The integrity of digital payments is no longer a narrow concern for payment service providers (PSPs) alone – it's an essential condition for economic security and institutional credibility in an increasingly cashless world.

The scale of the challenge is difficult to ignore. In 2022, retail payment fraud across the EU amounted to an estimated EUR 4.3 billion. By the first half of 2023, losses had already reached EUR 2 billion. The

growing use of instant credit transfers and their irreversibility has increased systemic exposure, especially in cases where the user is deceived into making a payment. Fraud is also more common in cross-border transactions, particularly those initiated by consumers, which are often harder to monitor and prosecute due to fragmented jurisdictional and supervisory frameworks.

The rise of fraud has been accompanied by a shift in its *modus operandi*. Broadly, retail payment fraud can be classified into two main categories. The first involves unauthorised transactions – cases where the user/payer hasn't consented to the transfer of funds, often due to stolen personal details, malware or technical breaches. These situations usually fall within the scope of existing liability frameworks, which requires the PSP to reimburse the user unless the user had acted fraudulently themselves – which does happen, where a customer purposely deceives their bank by pretending to be a victim of fraud.

The second and increasingly dominant category is authorised push payment (APP) fraud, where the user initiates the transaction voluntarily but does so under false pretences. Unlike unauthorised fraud, APP fraud relies not on technical intrusion but on psychological manipulation – victims are deceived into believing that they're interacting with a legitimate party and approve the transaction themselves. APP frauds take many forms: the impersonation of trusted institutions such as banks or public authorities; fraudulent investment schemes promising high returns; online marketplace scams where goods or services are advertised but never delivered; emotionally manipulative tactics often deployed via social media or online dating platforms; and redirection fraud targeting businesses, where invoice details are subtly altered to divert payments to fraudulent accounts.

These scenarios reveal a common pattern: the fraudster uses technology and institutional interfaces to exploit online vulnerabilities in human perception and trust. It also points to a broader truth – namely that modern fraud is no longer confined to the finance sector. **Fraud now flows through a multi-layered ecosystem of digital platforms, telecommunications networks and outsourced service providers – many of which remain outside the scope of financial regulation**.

The fragmentation of the retail payments value chain

The transformation of the retail payments landscape over the past decade has brought undeniable gains in efficiency, competition and user experience. However, it has also introduced significant structural vulnerabilities that are often underestimated in the policy debate. Central among these is the value chain's growing fragmentation: a shift away from a linear, bank-dominated process towards a multi-actor ecosystem where numerous entities – many of them unregulated or regulated under different sectoral regimes – now play essential roles in initiating, processing and executing payments.

In the traditional model, most stages of a retail payment transaction were controlled by a single PSP, which was then well placed to monitor for anomalies, implement customer authentication and assume financial responsibility in the event of fraud. Regulation reflected this structure, placing the bulk of compliance and liability obligations on PSPs. Alas, this architecture no longer reflects the reality of how payments operate today.

In the current ecosystem, payment processes often begin and end far from the regulated banking sector. A transaction may originate from a digital marketplace or social media platform, where a fraudulent offer is placed. It may be routed through a payment initiation service provider (PISP) or other fintech intermediary that facilitates the payment without holding client funds. It may rely on authentication mechanisms delivered through telecoms infrastructure – such as SMS-based codes or mobile number verification – which are vulnerable to attacks like SIM swapping. And it may depend on

technical service providers (TSPs) that host interfaces, manage APIs or offer behavioural analytics, all being critical for detecting anomalies but often lie beyond the consumer's awareness or direct control.

Each of these actors plays a different role in facilitating the transaction, yet few of them face obligations equivalent to those imposed on PSPs under financial regulation. Consequently, fraud can be enabled by actions or omissions at any point in the chain, while liability remains concentrated at the end, within the financial sector.

This structural lopsidedness creates a fundamental misalignment of incentives. The party most exposed to financial risk – the PSP – may not be the one best positioned to prevent the fraud from happening in the first place. Conversely, actors who play a key role in enabling fraudulent activity – by hosting content, delivering credentials or controlling user interfaces – may suffer no consequences at all when that activity results in financial loss. Without clearly allocating preventive duties and financial liability across the full range of actors involved, the system encourages only a partial response that isn't effective at countering fraud, as well as underinvestment in fraud detection and limited cooperation.

The value chain's fragmentation also makes information sharing more difficult. Different actors operate under different regulatory frameworks, with varying levels of supervision, compliance capacity and legal clarity. Data sharing across sectors is often inhibited by fears of breaching privacy laws or revealing trade secrets. **There's no common infrastructure for the real-time exchange of fraud indicators or behavioural signals, and voluntary initiatives remain isolated and insufficiently coordinated.**

Moreover, the increasing use of outsourcing and modular infrastructure – where PSPs rely on third-party providers for authentication, data analysis or user interaction – has created further governance blind spots. This weakens the ability to implement end-to-end preventive strategies and to identify points of failure with sufficient speed and precision.

The cumulative effect is a system where technical progress and the regulatory architecture have diverged. Without adjusting how liabilities are distributed and without a regulatory framework that reflects the payment chain's true structure, fraud will continue to target and exploit the weakest links – with many of them lying outside the scope of existing financial regulation.

To better understand how to correct this incentive misalignment, **we need to look at how other jurisdictions have responded to similar challenges – specifically, Singapore, Australia and the UK**, to see how they've allocated preventive duties and financial liability across an increasingly complex payments ecosystem.

International approaches to fraud in retail payments – prevention and liability

The structural vulnerabilities described above are not unique to the EU. Across advanced economies, the rise of complex, multi-actor payment ecosystems has challenged traditional assumptions about how fraud can be prevented and who should bear the consequences when prevention fails. Yet the regulatory responses have varied significantly.

Singapore has developed the most structured and legally binding model of shared accountability to date. Its Shared Responsibility Framework (SRF), launched jointly by the Monetary Authority of Singapore (MAS) and the Infocomm Media Development Authority (IMDA), recognises that fraud prevention requires coordination across sectors. The SRF sets out specific preventive duties for both financial institutions and telecoms operators. If a financial institution fails to fulfil its obligations – such as issuing real-time alerts or enabling robust authentication – it's required to reimburse the consumer for any losses. However, if the institution has complied and the fraud occurred due to vulnerabilities in

the telecoms layer (such as a SIM swap attack), then liability may shift to the telecoms provider. This cascading model of liability links financial responsibility to preventive performance and distributes exposure according to where the failure occurred.

Importantly, the SRF doesn't cover all forms of fraud. Its scope is currently limited to unauthorised digital payments due to phishing scams. Other common forms – such as malware-enabled fraud or APP scams that directly deceive the user – remain outside the framework. Nonetheless, the Singaporean model stands out for its ability to embed preventive incentives across the system and to institutionalise a logical trail of proportional accountability.

Australia has taken a different route, placing the emphasis on prevention through regulation and deterrence. Its Scam Prevention Framework, launched in 2025 and coordinated by the Australian Competition and Consumer Commission (ACCC), imposes legally binding obligations on financial institutions, telecoms operators and major digital platforms to implement fraud detection systems, share risk information and respond swiftly to emerging threats. The framework doesn't mandate reimbursement in fraud cases, nor does it establish formal rules for apportioning financial liability between actors. Instead, it uses a compliance-based logic, relying on administrative penalties and reputational consequences to drive behavioural change.

The Australian model represents an ambitious attempt to foster cross-sectoral cooperation – but it reveals the limits of prevention if there's no financial accountability. Institutions may comply with formal obligations without necessarily internalising the costs of failure. In this context, deterrence substitutes for direct liability and the framework's effectiveness depends on the regulator's credibility and enforcement capacity.

The *UK* has opted for a more consumer-centric approach. A mandatory reimbursement regime for APP fraud was introduced in October 2024. Under this system, PSPs are required to refund victims within five business days, unless the customer has acted with gross negligence. The reimbursement cost is shared equally between the payer's and payee's PSPs. The scheme is administered by the Payment Systems Regulator and applies to all firms participating in the Faster Payments System.

This model provides a strong safety net for users and creates incentives for PSPs to invest in fraud detection, consumer education and risk profiling. However, it doesn't extend to non-financial actors. Telecoms operators, social media platforms and online marketplaces are not subject to specific preventive duties, nor are they required to financially contribute to reimbursements. As a result, responsibility remains concentrated in the financial sector, even when the fraud originates elsewhere in the digital ecosystem.

The model is relatively simple to enforce and delivers rapid redress but it reinforces a structural imbalance – those best positioned to detect and block fraud in its early stages don't participate and nor are they held financially accountable. The result is a limited form of incentive alignment, effective within the financial space but not enough to address the broader architecture of fraud enablement.

Taken together, these three cases offer valuable insights into the interaction between regulatory design, incentive structures and systemic resilience when a partial approach to fraud prevention and liability is taken.

Singapore shows the potential of aligning liability with preventive capability through a legally binding cascade model. Australia highlights the promise and limitations of prevention without direct compensation. The UK demonstrates the benefits of mandatory reimbursement but also the

constraints of confining responsibility to PSPs. **Still, none of the three models offers a holistic approach to fraud prevention and liability**.

These three examples make one point abundantly clear – effective fraud prevention in a fragmented environment requires not only better technology or tighter compliance **but a realignment of liability that reflects the distributed nature of risk**.

The EU – evolving ambitions, structural constraints

The EU has traditionally placed the burden of fraud prevention and redress squarely on PSPs, especially under the second Payment Services Directive (PSD2). While this functioned relatively well in a more centralised ecosystem, the increasing complexity of the retail payments environment has exposed its limitations.

Yet the proposed measures remain shaped by the same institutional asymmetries and encounter longstanding obstacles that could limit how effective they are in addressing the root causes of systemic vulnerability.

A multi-pillar strategy for fraud prevention

One of the most notable developments in the European Commission's PSR proposal is the recognition that fraud prevention cannot be the responsibility of PSPs alone. The new framework articulates a more holistic approach, built around four strategic pillars designed to address both the behavioural and structural drivers of fraud.

The *first pillar* focuses on enhancing user awareness and decision-making. PSPs are expected to provide more and better information to users – such as clearly identifying payees through verification tools and real-time warnings about common fraud typologies. This isn't limited to customer interfaces but also includes broader efforts, such as participating in public awareness campaigns and education initiatives that work towards making users more resistant to manipulation.

The *second pillar* centres on enabling PSPs to access and process better quality data for fraud detection. The proposal clarifies how fraud-related data can be processed, aligning it with the General Data Protection Regulation (GDPR) and affirming that data sharing for fraud prevention constitutes a legitimate interest. The intention is to remove a key legal uncertainty that has hindered cooperation between institutions and to facilitate the creation of shared detection systems and fraud intelligence networks.

The *third pillar* introduces a novel liability mechanism for impersonation-based fraud, granting victims a right to reimbursement in cases where they've been deceived by a third party posing as a trusted institution. The scope of this rule is narrow – it covers only a subset of APP frauds – but it represents an important shift towards recognising that informed consent may not always be a meaningful defence in the face of sophisticated deception.

To mitigate moral hazard and ensure user accountability, the right to reimbursement is conditional only if the payer hasn't committed gross negligence themselves. This preserves the incentive for users to remain vigilant and take reasonable precautions against fraud, striking a balance between enhanced consumer protection and the need to avoid complacency. By incorporating this, the proposal acknowledges that not all victims of impersonation-based fraud are equally blameless and that fairly allocating responsibility remains essential.

Finally, the *fourth pillar* acknowledges that PSPs cannot act alone and explicitly calls for cross-sectoral cooperation, particularly from telecoms operators. The regulation proposes that electronic communication service providers should support fraud prevention by securing access channels and responding promptly to PSPs' requests when fraud is suspected. While the obligations are still relatively general, this is an important departure from the assumption that fraud is purely a financial sector issue.

Together, these four pillars point to a more dynamic and distributed model of prevention. **However, how they'll be implemented remains uncertain**. Many of the obligations placed on non-financial actors are expressed in soft language or rely on future cooperation mechanisms that remain undefined. Moreover, without a corresponding adjustment to liability rules, these preventive efforts may lack the incentives necessary to produce sustained behavioural change.

The limits of current responsibility rules

The proposed reforms include partial steps to address the misaligned responsibility identified in previous sections. Most notably, the Commission has proposed a mandatory reimbursement mechanism in cases of impersonation fraud, with the PSP required to refund the victim under specified conditions. However, responsibility continues to rest solely with the PSP, even when other actors played a material role in enabling the fraud. This perpetuates unequal levels of exposure and does little to address the incentive problems caused by fragmented accountability.

Recognising these shortcomings, the European Parliament (EP) has proposed a more ambitious model. While maintaining the user's right to be reimbursed promptly, the EP's draft amendments include a limited right of redress for payment service providers. Specifically, the EP's proposal stipulates that electronic communications service providers (ECSPs) may be required to refund PSPs the full amount of a fraudulent authorised transaction if they fail to remove fraudulent or illegal content after being notified and provided that the consumer reports the fraud to the police and notifies the PSP without delay. While this provision introduces a form of shared accountability, it applies to a narrow set of circumstances and doesn't establish a general principle of proportional responsibility across the fraud chain.

The proposal reflects the logic adopted in Singapore's cascading liability model and aims to anchor financial responsibility where preventive capacity resides. It also includes a mechanism to operationalise this logic through formal cooperation channels, including those established under the Digital Services Act, such as Article 16 obligations for the timely removal of illegal content. While such levels of coordination remain largely aspirational, it marks a shift towards a more integrated regulatory framework capable of addressing the reality of multi-actor fraud schemes.

Nonetheless, this approach raises questions about evidence, causality and enforceability. Proving that a non-financial actor failed to meet its duties may require access to information that's difficult to obtain or subject to confidentiality. Determining which actor should ultimately bear full liability in practice could also lead to disputes and litigation.

Moreover, the EP's solution only makes digital platforms liable when they fail to take down fraudulent websites after being notified by the PSP – without setting a removal deadline or establishing a fast and straightforward procedure for PSPs to claim redress. It doesn't cover any other type of APP scam. Without clear evidentiary standards and institutional mechanisms to adjudicate claims, the liability-shift mechanism could remain nothing more than a pipe dream.

Structural barriers to effective cooperation

Even where regulatory ambition exists, structural barriers still hinder effective cross-sector coordination. One of the most frequently cited concerns is the perceived tension between fraud prevention and data protection. Although the GDPR allows the processing of personal data based on legitimate interest, many institutions remain hesitant to engage in real-time data sharing, fearing enforcement action or reputational damage. With the lack of consistent guidance from data protection authorities, particularly regarding the scope of permissible cooperation, uncertainty prevails and risk aversion dominates.

In parallel, competitive considerations and the protection of trade secrets present further obstacles. Fraud detection systems, behavioural analytics and internal risk models are often considered commercially sensitive. Firms may be reluctant to share information that could reveal their security architecture or be interpreted as an admission of weakness. This is particularly true for large digital platforms, whose core business models depend on proprietary algorithms and user data, and for telecoms operators, whose technical infrastructure may be vulnerable to enhanced scrutiny.

Finally, the institutional landscape itself is ill-suited to cross-sectoral governance. While the European Banking Authority (EBA) and Eurosystem authorities have well-established mechanisms for coordinating with PSPs, no equivalent platform exists to facilitate collaboration with telecoms or digital service providers. Consequently, cooperation depends heavily on goodwill and informal networks, which are insufficient in the face of increasingly sophisticated and transnational fraud schemes.

Policy recommendations – towards a more coherent framework of shared accountability

As the EU finalises the next generation of its payment services framework, it must recognise that fraud is no longer confined to the domain of PSPs and cannot be effectively addressed through sector-specific rules alone.

A first priority is to rebalance the distribution of financial responsibility within the payment ecosystem.

The underlying principle should remain clear – actors should bear liability in line with their capacity to prevent the specific fraud in question. In practice, this implies that reimbursing consumers – particularly in cases of deception-based fraud – should be swift and guaranteed but the financial burden of that reimbursement should not fall solely on PSPs.

While the EP's proposal introduces a first step in this direction by establishing limited liability for digital platforms in specific scenarios, its scope is too narrow and its enforcement mechanisms underdeveloped. For shared accountability to become effective, the regulatory framework should go further – **liability should extend to all actors who failed to act, thus enabling the fraud, supported by clear timelines, procedural clarity and effective redress mechanisms**. Only then will all relevant actors – digital platforms, telecoms operators, and technical intermediaries – have the appropriate incentives to invest in meaningful prevention and cooperate with PSPs.

Second, cooperation should be enhanced by creating an institutionalised, cross-sectoral platform for fraud intelligence sharing at EU level.

This body should bring together not only payment service providers but also telecoms operators, digital platforms, cybersecurity authorities, law enforcement and relevant regulators across sectors, reflecting the multidimensional nature of modern fraud schemes. **Its core tasks would include exchanging**

intelligence on fraud typologies, coordinating incident response protocols, and developing interoperable technical standards for detection and prevention.

To be effective, **the platform must be supported by a robust legal mandate and enforceable data-sharing obligations, with safeguards to ensure compliance with data protection rules**. Importantly, its scope must go beyond payments legislation to address the broader regulatory and technical enablers of fraud. Voluntary initiatives, however well intentioned, won't be sufficient in the face of increasingly sophisticated and transnational fraud networks.

In parallel, regulatory clarity on data sharing remains a critical enabler of effective fraud prevention. The proposed PSR takes an important step forward by recognising that PSPs may exchange fraud-related data in compliance with the GDPR, thus removing longstanding legal uncertainty. However, this exchange should not be left up to discretion – it must be made mandatory among PSPs, to ensure timely and comprehensive information flows across the financial system.

This principle should also be extended beyond the financial sector. Telecoms providers and digital platforms are often key for early fraud detection, being able to intercept, for example, information on spoofed communications or compromised domains. To facilitate meaningful cooperation, data sharing with these actors should be structured through coordinated mechanisms at national level – rather than on a case-by-case basis – ensuring both operational efficiency and legal certainty.

Finally, the EU should leverage its supervisory infrastructure to reinforce consistency and accountability across borders. In short, cross-border fraud requires cross-border solutions.

The EBA, national competent authorities and European data protection authorities should be empowered to conduct joint supervisory actions, issue coordinated warnings and oversee compliance with shared accountability principles

Conclusions

What emerges from this analysis is a simple but demanding truth – complex problems cannot be solved through fragmented solutions. And as retail payment fraud becomes more complex and more international, such solutions just won't cut it anymore,

Such fraud is no longer a marginal or incidental risk; it's a structural challenge that impacts not only the credibility of the entire digital economy but also the financial system's overall legitimacy. Meeting this challenge will require a new regulatory logic that recognises interdependence and distributes responsibility accordingly.

The EU, through the Commission's PSR proposal and the ongoing work to reach a final agreement, has indeed made some positive steps in the right direction – but more will be needed.

The three recommendations advocated for in this ECRI Policy Brief will help chart a course forward for more ambitious ideas and solutions.

European Credit Research Institute

The European Credit Research Institute (ECRI) is an independent, non-profit research institute that develops its expertise from an interdisciplinary team and networks of academic cooperation partners. It was founded in 1999 by a consortium of European banking and financial institutions. ECRI's operations and staff are managed by the Centre for European Policy Studies. ECRI provides in-depth analysis and insight into the structure, evolution, and regulation of retail financial services markets in Europe. Through its research activities, publications and conferences, ECRI keeps its members up to date on a variety of topics in the area of retail financial services at the European level, such as consumer credit and housing loans, credit reporting, consumer protection and electronic payments. ECRI also provides a venue for its members to participate in the EU level policy discussion.

For further information, visit the website: www.ecri.eu.

Centre for European Policy Studies

CEPS is one of Europe's leading think tanks and forums for debate on EU affairs, with an exceptionally strong in-house research capacity and an extensive network of partner institutes throughout the world. As an organisation, CEPS is committed to carrying out state-of-the-art policy research that addresses the challenges facing Europe and maintaining high standards of academic excellence and unqualified independence and impartiality. It provides a forum for discussion among all stakeholders in the European policy process and works to build collaborative networks of researchers, policymakers and business representatives across Europe.

For further information, visit the website: www.ceps.eu.