ECRI IN-DEPTH ANALYSIS

SHARING FRAUD INTELLIGENCE UNDER THE PAYMENT SERVICES REGULATION: MIND THE GAP

Judith Arnal

August
2026 - 02

SUMMARY

The EU Payment Services Regulation (PSR) represents a significant improvement in the EU's response to payment fraud. It moves beyond a model centred mainly on identity and controls on individual payment service providers (PSPs), and recognises that modern fraud prevention requires shared intelligence.

Even so, the PSR leaves two major implementation problems unresolved. The first is internal to the payment sector. The Regulation gives PSPs a clearer legal and data protection basis for sharing fraud-related information. But this legal certainty also instils rigidity: the categories of data that can be safely shared are set by statute, without provision for a dynamic mechanism to adapt them as fraud typologies evolve.

At the same time, national arrangements are emerging, along with sector-led, private and pan-European ones. If these schemes develop different data models, taxonomies, suspicion thresholds, alert formats and governance rules, PSPs may face overlapping obligations in siloed systems. This could weaken the overall network approach to fraud that the PSR is meant to enable.

The second problem concerns the wider fraud chain. The PSR recognises that many scams originate outside the payment layer, involving platforms, hosting providers, search engines or electronic communications providers. Yet, the obligation for non-PSP actors to cooperate is not as strong, systematic or complete as that imposed on PSPs. Fraud prevention cannot rely solely on PSPs or users reporting fraud after it has materialised; it also requires *ex ante* measures by upstream actors capable of detecting and disrupting scam infrastructure before a fraudulent payment is executed.

This analysis argues against both fragmentation and centralisation. The EU does not need a single, mandatory fraud database. It needs interoperability by design, which would entail the following:

- common operational requirements for PSP-to-PSP information sharing;
- a federated FRIDA (fraud information) layer, led by the European Payments Council, to connect national, private and sectoral arrangements across SEPA and EPC payment schemes;
- model protocols for cooperation with non-PSP actors; and
- a first PSR review focused on whether the framework has produced a genuinely interoperable ecosystem of fraud intelligence.

The central claim is that the PSR has opened the legal gateways for fraud intelligence to flow. But its success will depend on whether implementation turns those gateways into a connected, operationally usable and preventive network.

The European Credit Research Institute (ECRI) is an independent, non-profit research institute that provides in-depth analysis and insight into the structure, evolution, and regulation of retail financial services markets in Europe. ECRI's operations and staff are managed by the Centre for European Policy Studies (CEPS).

Judith Arnal is Associate Senior Research Fellow at ECRI and CEPS. The author would like to thank Mathilde Bonneau and Iván Burillo for helpful comments to a previous draft.

PAYMENT FRAUD AS A MACROECONOMIC AND INSTITUTIONAL PROBLEM

Retail payment fraud is no longer a marginal operational risk on the edge of payments law. It has become a structural challenge for the digital economy. In the European Economic Area, the total reported value of payment fraud increased from EUR 3.5 billion in 2023 to EUR 4.2 billion in 2024, while the overall fraud rate remained stable at approximately 0.002% of the total value of payment transactions. This aggregate rate may appear low, but the economic and institutional impact is much broader than the direct amount stolen.

Payment fraud undermines confidence in digital payments, increases the cost of compliance and reimbursement, and burdens dispute-resolution and law enforcement systems. It threatens the policy objective of making instant and cross-border payments safe, trusted and widely used. Fraud is increasingly not only a matter of unauthorised access or weak authentication; it is also a matter of deception, manipulation and misuse of the wider digital ecosystem.

The Payment Services Regulation (PSR) should therefore be read against this background. The PSR does more than simply update the security model of the Payment Services Directive 2. **It reflects a broader shift from identity-based fraud prevention towards intelligence-led fraud prevention.**

The gap exposed by scams is not that identity verification necessarily fails, but that it is not enough: a payer may be correctly identified and the payment technically authorised, yet the payer has nevertheless been manipulated into making the payment. The PSR responds to this by imposing transaction-monitoring obligations, requiring payment service providers (PSPs) to share information and creating legal gateways for cross-sector cooperation. It also introduces governance mechanisms for fraud trends and mitigation measures.

All the same, fraud data sharing should not be treated as a complete fraud-prevention strategy. It is a necessary tool for detecting patterns that no single PSP can see, but it cannot substitute for prevention of fraud by upstream actors that design, host, transmit or monetise the infrastructure through which scams reach consumers. A fraud chain may begin with fraudulent advertising, AI-enabled impersonation, spoofed communications, phishing infrastructure or mule-account networks, and only later materialise as a payment transaction.

This In-Depth Analysis argues that the PSR's most important innovation, the shift towards shared fraud intelligence, is also its most fragile. Although the Regulation builds a solid legal basis for PSP-to-PSP information sharing and channel obligations for cooperation with upstream actors, two distinct aspects make it fragile. The first concerns the architecture for mandatory PSP-to-PSP cooperation. Even where cooperation is required, the PSR does not itself establish the operational infrastructure through which intelligence will circulate. It leaves data models, technical interfaces, common vocabulary, suspicion thresholds and governance arrangements largely to private schemes, national initiatives and future technical standards.

The second concerns the scope of cross-sector cooperation. The PSR recognises that fraud often originates outside the payment transaction itself, but it does not impose on upstream actors a full duty to contribute fraud intelligence across the scam chain comparable to the duty imposed on PSPs. The implementation risk is twofold: a governance risk of mandatory PSP cooperation developing through fragmented and non-interoperable arrangements; and an

incompleteness risk of wider actors that generate or observe crucial fraud signals remaining only partially integrated into the intelligence network.

Both risks are real but avoidable. The EU can address them with instruments it already has, by ensuring that emerging arrangements converge on common standards and by operationalising cross-sector cooperation more deliberately, rather than by building a single central platform.

The argument proceeds in four steps. Section 2 sets out the PSR's anti-fraud framework and distinguishes between its main weaknesses – the absence of a sufficiently specified operational system for mandatory PSP-to-PSP information sharing, and the more limited integration of upstream actors into the fraud intelligence framework. Section 3 examines the ecosystem of information-sharing arrangements now appearing in the EU and the resulting governance risk of fragmentation across Member States, between public and private schemes, and between payment- and cross-sector channels. Section 4 draws lessons from two jurisdictions that have gone further in different directions – the UK on standardised intelligence sharing within the payment sector and Australia on mandatory cooperation across sectors.

Section 5 sets out the policy recommendations that follow, addressed to the actors and instruments that can realistically deliver common operational standards for PSP-to-PSP sharing and a more deliberate framework for cross-sector cooperation. Section 6 concludes.

THE PSR MODEL IN THE EU: FROM INDIVIDUAL SECURITY TO COLLECTIVE INTELLIGENCE

The PSR's anti-fraud architecture is based on a simple but important insight: no single PSP sees the whole fraud chain. The payer's PSP may observe the customer's behaviour, authentication process, device data and transaction history. The payee's PSP may observe mule-account activity, abnormal inflows, rapid onward transfers and patterns across receiving accounts. Platforms may observe fraudulent advertising or suspicious seller behaviour. Hosting providers may host phishing websites or fraudulent content. Electronic communications service providers may observe spoofing, smishing or manipulation of calling-line identification. Effective fraud prevention therefore requires a networked intelligence model.

The PSR does not, however, create a single EU fraud-intelligence utility or a public central database. Its approach is decentralised. It creates legal duties, legal gateways and institutional incentives, but leaves much of the operational infrastructure to private-sector arrangements, payment infrastructures, national initiatives, future technical standards and soft-law coordination by the European Banking Authority (EBA). This is the core tension in the Regulation: it recognises that fraud prevention requires collective intelligence, but it does not itself build a fully harmonised European network for fraud intelligence.

Table 1 summarises the PSR's approach to fraud intelligence.

Table 1: The PSR's fraud intelligence architecture

PSR component	Function in the fraud intelligence architecture	Nature of the obligation	Public policy assessment
Article 83 – Transaction monitoring	Internal analytical layer within each PSP.	Mandatory.	Foundational fraud-control layer for PSPs, covering traditional unauthorised fraud as well as APP/scam typologies. Essential, but not itself a network; its value under the PSR depends on the external fraud intelligence that can be fed into it.
Article 83(a) – PSP-to-PSP fraud information sharing	Core PSP-to-PSP fraud intelligence mechanism.	Mandatory where objective suspicion exists.	Strong privacy-law gateway for PSP-to-PSP fraud data sharing, but decentralised and potentially fragmented. Its limitation to specified PSR data categories improves legal certainty but may reduce flexibility as fraud typologies evolve.
Article 59(a) – Cross-sector cooperation	Cooperation with hosting providers, electronic communications providers, very large online platforms (VLOPs) and very large online search engines (VLOSEs).	Hybrid: mandatory notification and channels; conditional data exchange.	Recognises that payment fraud often originates outside the payment layer, but falls short of a mandatory regime for cross-sector intelligence sharing. Cooperation may therefore remain bilateral, uneven and dependent on voluntary initiative or goodwill.
Article 59(b) – Financial services advertising	Preventive due diligence against scam advertising.	Mandatory for VLOPs and VLOSEs.	Important upstream due-diligence measure against scam advertising, but insufficient on its own: effective real-time intelligence depends on whether upstream actors collect, retain and structure the fraud-relevant signals needed for cross-sector sharing.
Article 82 and Article 89 – Reporting and Regulatory Technical Standards (RTS)	Statistical fraud reporting and technical standards for transaction monitoring.	Mandatory reporting; EBA Level 2 mandates.	Useful return flow of supervisory intelligence through EBA/ECB fraud reporting. Further value would come from greater transparency on how supervisors use the reported data. Still not a complete, operational data-sharing rulebook.
Article 83(b) – Platform on combating fraud	Commission-led public-private forum.	Governance and coordination mechanism.	Useful for policy learning and soft-law convergence, but not an operational intelligence hub and does not mandate participation by upstream firms.

Source: Author's elaboration based on the PSR.

TRANSACTION MONITORING AND PSP-TO-PSP INFORMATION SHARING

The starting point is Article 83, which requires every PSP to operate transaction monitoring mechanisms to support Strong Customer Authentication (SCA) and detect potentially fraudulent transactions. Transaction monitoring is the basic fraud-control layer within each PSP. It is not new as a supervisory or operational expectation, but the PSR gives it a different role by linking it expressly to shared fraud intelligence. This obligation is two-sided. The payer's PSP must monitor the transaction before execution, and the payee's PSP must monitor it

before making the funds available. Each PSP therefore sees only its own half of the payment chain, so monitoring on its own cannot capture the full picture.

Article 83 anticipates this. The data a PSP may use includes the payer, payee, account, transaction, session and device information it observes itself, but it also expressly includes information obtained through information-sharing arrangements. This is the link to Article 83(a), which is the provision enabling that shared information. Article 83 is the monitoring layer; Article 83(a) triggers its main external input.

Article 83(a) is the central provision for PSP-to-PSP fraud information sharing. It requires PSPs to participate in information-sharing arrangements with other PSPs and to exchange data where this is necessary to comply with transaction monitoring obligations and where there are objectively justified reasons to suspect fraudulent behaviour by a payment service user. This is not framed as a merely voluntary arrangement. The wording is mandatory: PSPs 'shall participate' and 'shall exchange data' where the relevant conditions are met.

At the same time, the obligation is conditional, purpose-limited and decentralised. The PSR does not create a single EU-wide platform. Instead, PSPs must participate in arrangements whose operational features, including the possible use of dedicated IT platforms, are to be specified by the arrangements themselves. That decentralised choice is not problematic in itself. The problem is that the PSR does not specify how decentralised arrangements are to remain mutually connected. The key implementation question is therefore not whether the EU should build a single platform, but whether multiple arrangements can be made interoperable.

The data-sharing power is not unlimited. The shareable data are linked to data that may be processed for transaction monitoring under Article 83. PSPs may share information concerning the suspected fraudulent behaviour, the relevant payment account or transaction, and the objectively justified reasons giving rise to the suspicion. Where the suspected fraud is connected to fraudulent content hosted online, the PSP may also share information on notifications made to hosting providers through the notice-and-action procedure of the Digital Services Act.

Notably, the PSR expressly excludes the sharing of environmental and behavioural characteristics typical of the payer's normal use of personalised security credentials. This exclusion is important: the Regulation permits fraud intelligence, but it does not authorise the unrestricted circulation of behavioural profiles. It also reveals a rigidity risk. By tying PSP-to-PSP sharing to a statutorily delimited set of Article 83 data categories, Article 83(a) strengthens legal certainty and data minimisation, but it may also make the legally safe scope of fraud intelligence difficult to adapt as fraud typologies evolve. New fraud-relevant signals may become operationally important without fitting neatly within the existing categories. Unless these signals can be interpreted as falling within the bounds of Article 83, their systematic sharing between PSPs will require further regulatory clarification or, ultimately, legislative amendment through the PSR review process. The PSR therefore protects against over-sharing, but it does not create an express dynamic mechanism for expanding the Article 83(a) data limits.

Article 83(a) also contains safeguards that are essential to the legitimacy of the regime. PSPs must implement technical and organisational security measures, including measures enabling pseudonymisation. Data obtained through an information-sharing arrangement may be retained only for as long as necessary and, in any event, for no longer than five years after the

suspected fraudulent transaction. Before concluding an arrangement, PSPs must jointly conduct a data protection impact assessment and, where the GDPR requires it, consult the competent data protection supervisory authority. The arrangement must also address the allocation of roles and responsibilities under data protection law. Finally, PSPs may not terminate a business relationship or negatively affect future onboarding solely on the basis of information received from another PSP without assessing that information. This is designed to prevent fraud intelligence from becoming an unreviewed private blacklist.

The policy logic is clear. Article 83(a) gives PSPs a legal basis to share fraud-relevant information, but it attempts to contain the risks of over-sharing, false positives, unjustified exclusion from payment services and disproportionate processing of personal data. Shared fraud intelligence is meant to improve monitoring and detection; it is not meant to operate as an automatic de-risking mechanism.

CROSS-SECTOR COOPERATION: PLATFORMS, HOSTING PROVIDERS AND ELECTRONIC COMMUNICATIONS PROVIDERS

Article 59(a) extends the PSR beyond the payment sector. This is one of the most innovative parts of the Regulation, because it recognises that the origin of payment fraud often lies outside the payment transaction itself. A scam may begin with a fraudulent advertisement, a fake investment website, a phishing page, a spoofed telephone call, a manipulated email address or social-engineering activity on a digital platform.

The first element of Article 59(a) is mandatory notification. Where payment fraud originates in fraudulent content published online, PSPs must inform hosting providers without undue delay through the notice-and-action mechanism of the Digital Services Act (DSA) or, where applicable, the trusted-flagger mechanism. This connects the PSR anti-fraud framework to the DSA's content-governance infrastructure. The DSA link is useful, but it should not be overstated. The DSA notice-and-action mechanism provides a route for reporting specific items of allegedly illegal content and requires hosting providers to process notices in a timely, diligent, non-arbitrary and objective manner. It does not, however, turn each PSR notification into a fixed-time takedown order, nor does it create a payment-fraud liability regime for platforms or hosting providers. For payment fraud, the practical question is therefore not only whether illegal content can be notified, but whether the upstream actor has systems capable of detecting, prioritising and disrupting scam infrastructure before a fraudulent payment is executed.

The second element is a communication-channel obligation. Electronic communications service providers, very large online platforms and very large online search engines must establish dedicated communication channels with PSPs. Alternatively, they must participate in an effective communication system or information-sharing mechanism to enable faster and more effective exchanges. **This measure is stronger than a purely voluntary model, but it remains less detailed than Article 83(a).**

The PSR does not specify a common Application Programming Interface (API), a minimum data payload, a response-time standard, a confidence-scoring model, a fraud taxonomy or an escalation protocol for cross-sector information sharing. This under-specification matters because the channel model may remain bilateral rather than networked. A dedicated PSP-to-platform, PSP-to-hosting-provider or PSP-to-telecommunications channel can accelerate an individual exchange, but it does not by itself ensure that a signal generated in one relationship

becomes available to the wider ecosystem. A scam campaign using the same online infrastructure to target customers of several PSPs should generate a reusable system-wide signal, not a sequence of disconnected one-to-one notifications.

The third element is conditional data exchange. Article 59(a) allows data to be exchanged between PSPs and hosting providers, and between PSPs and electronic communications service providers, where this is necessary to prevent and detect potentially fraudulent payment transactions and where there are objectively justified grounds to suspect fraudulent behaviour by a user of the relevant service. This creates a legal gateway for cross-sector fraud intelligence, but it does not impose a general obligation on platforms, hosting providers or electronic communications providers to disclose all relevant fraud data in every case.

The conditional nature of the gateway also creates a detection circularity. An upstream actor may not know that particular content, account activity or communication is linked to a potentially fraudulent payment without intelligence from PSPs, while a PSP may not see the broader scam context without platform, hosting-provider or telecommunications intelligence. Article 59(a) therefore enables exchange once suspicion exists, but it does less to organise the earlier, recursive intelligence process through which suspicion is generated in the first place.

This asymmetry is particularly visible when Article 59(a) is read alongside the PSR's liability rule on impersonation fraud. Where a consumer is manipulated by a third party pretending to be the consumer's PSP through communication channels attributed to that PSP, Article 59 gives the consumer a refund claim against the PSP, subject to the conditions set out in that provision. Article 59(a), by contrast, recognises that the fraud may have been enabled through online content, hosting infrastructure or electronic communications services, but it does not impose an equivalent customer-facing liability or a fully specified prevention regime on those upstream actors.

Electronic communications service providers also acquire a specific anti-impersonation role. They must take appropriate organisational and technical measures to detect and prevent the use of their services for impersonation fraud. This includes manipulation of calling-line identification or email addresses where the purpose is to induce a payment service user to make a payment or compromise account security. This reflects the fact that many modern fraud typologies exploit the communications layer rather than the payment interface itself.

National experience suggests that more granular anti-spoofing obligations can produce operational results. Spain's Order TDF/149/2025 introduced measures to combat identity-impersonation scams through fraudulent calls and text messages, including obligations for operators to block certain calls and messages using unassigned numbers or international-origin communications that simulate Spanish numbering. The Spanish Government later reported that, between the entry into force of the first measures on 7 March 2025 and 30 November 2025, operators had blocked almost 135 million calls and more than 5 million SMS with fraudulent intent.

Finland's Traficom regime points in the same direction. After obligations to prevent caller-ID spoofing came fully into effect, Traficom reported that spoofing of Finnish phone numbers had 'come to an end in practice' and that the mobile-number measures had prevented more than 200 000 scam calls per day during the initial period.

These examples suggest that the general anti-impersonation language of Article 59(a) could usefully be complemented, at the EU level, by more concrete technical expectations for electronic communications providers.

Article 59(b) adds a further preventive measure. Very large online platforms and very large online search engines must request authorisation, registration or equivalent information from advertisers of regulated financial services. They must make best efforts to verify that information using official registers where appropriate, and refuse the advertisement where the required information has not been obtained. This is not a real-time fraud intelligence mechanism, but it is relevant to the same ecosystem logic – platforms are required to reduce the upstream circulation of fraudulent financial promotions.

This logic points to a further limitation. Article 59(a) remains heavily notice-led: fraudulent content, communications or advertising are addressed once they have been detected by a PSP, a user or another actor. Article 59(b) introduces a more preventive duty of due diligence for financial services advertising, but it remains narrower than a general upstream fraud-prevention regime. In scam advertising and spoofing cases, delay is itself part of the harm. A fraudulent advert, website, caller ID or sender ID can be replicated and reused at scale before any individual victim reports the fraud to a PSP. Cross-sector intelligence sharing is therefore only as effective as the *ex ante* measures adopted by upstream actors, and as the underlying data that those actors collect, retain and structure.

A more resilient framework would need to identify, subject to necessity, proportionality and data protection safeguards, and the categories of upstream signals most relevant to fraud prevention. These include URLs and advertising links, fraudulent websites, advertiser or seller identifiers, payment and financial-instrument details linked to scam activity, profile or subscriber data, device and IP signals, application signatures and communications metadata relevant to smishing or spoofing.

GOVERNANCE, LEVEL 2 MEASURES AND THE LIMITS OF HARMONISATION

The PSR also creates a supervisory and governance layer. Article 82 requires PSPs to report statistical fraud data to competent authorities, which then provide aggregated data to the EBA and the ECB. The EBA and ECB must publish an annual joint report analysing fraud trends. The EBA is also mandated to develop regulatory technical standards on the statistical fraud data to be reported and implementing technical standards on customary forms and templates.

Article 89 requires the EBA to develop regulatory technical standards on authentication, secure communication and transaction monitoring mechanisms, including the technical requirements for the transaction monitoring mechanisms referred to in Article 83. These Level 2 mandates will matter, especially for the design of PSPs' monitoring systems. However, they do not appear to create a complete operational rulebook for Article 83(a) fraud information-sharing arrangements or Article 59(a) cross-sector cooperation. The PSR does not expressly require the EBA to specify a common data model, fraud taxonomy, API, response-time requirements, confidence scores, feedback mechanisms or interoperability standards for PSP-to-PSP or PSP-to-platform/telecoms intelligence sharing.

Article 83(b) establishes a Commission-led platform on combating fraud in the area of payment services. The platform is to bring together public and private actors with knowledge of payment fraud. Its functions include advising the Commission, issuing recommendations for the

voluntary code of conduct, sharing and analysing fraud trends, exchanging information on mitigation measures and identifying ways to improve cross-border and cross-sector cooperation. This is a useful governance mechanism, but it is not an operational hub for fraud intelligence.

The result is a partial harmonisation model. The PSR harmonises the legal basis for sharing, the obligation to participate in PSP-to-PSP arrangements, the basic conditions for sharing and several safeguards. It does not fully harmonise the operational infrastructure through which fraud intelligence will circulate.

THE EMERGING ECOSYSTEM OF ARRANGEMENTS FOR FRAUD INFORMATION SHARING IN THE EU: THE RISK OF FRAGMENTATION

The main implementation risk under the PSR is not the same for the two branches of its fraud intelligence architecture. For PSP-to-PSP information sharing, the Regulation goes furthest towards solving the legal basis problem. Article 83(a) creates a mandatory, purpose-limited sharing regime between PSPs. Article 80 reinforces the data protection basis for payment systems, payment schemes, processing entities and PSPs to process special categories of personal data where necessary for payment services and PSR compliance, subject to appropriate safeguards. The remaining weakness in this branch is therefore primarily architectural: the PSR requires PSPs to participate in information-sharing arrangements, but leaves the operational design of those arrangements largely open.

For cross-sector cooperation, the weakness is different. Article 59(a) creates notification duties, dedicated channels and a legal gateway for conditional data exchange with upstream actors. But it does not impose a general, symmetric duty on hosting providers, electronic communications providers, very large online platforms or very large online search engines to contribute fraud intelligence to a common network. The cross-sector layer may therefore remain bilateral, uneven and, in practical terms, dependent on voluntary initiative, goodwill and the incentives of individual upstream actors. The PSR thus reduces legal uncertainty most clearly within the payment sector, but it does not fully solve either the governance problem of PSP-to-PSP sharing or the completeness problem of cross-sector intelligence.

This fragmentation risk operates along two axes that should be kept analytically distinct. The first is *horizontal*: arrangements emerging at Member State level may diverge from one another, so that a large cross-border PSP must connect to several national schemes simultaneously. The second is *vertical*: alongside these public or nationally coordinated schemes, a parallel set of private and often transnational arrangements is emerging outside the national logic altogether. The result is not a single fragmented network but a layered ecosystem in which PSP-to-PSP arrangements (Article 83(a)), cross-sector arrangements (Article 59(a)), and the semantic and governance layers that should connect them, do not yet align.

PSP-TO-PSP ARRANGEMENTS UNDER ARTICLE 83(A)

France illustrates the horizontal trajectory most clearly. The FNC-RF, managed by the Banque de France, is a national platform for centralising and sharing fraud-related account information, allowing PSPs to declare and consult alerts on accounts suspected of being linked to payment fraud. The information shared focuses on account identifiers and fraud-related

metadata rather than on the identity of the account holder. The significance of the French model is not that every Member State will replicate it in identical terms, but that it shows how Article 83(a)-style intelligence emerges first through national systems.

France is not an isolated case. In **the Netherlands**, the sector-level Incident Alert System enables institutions to share post-suspicion information on confirmed or suspected fraud incidents.

Germany reflects the same trend, although at an earlier and more coordination-oriented stage. In December 2025, the Deutsche Bundesbank published a joint statement from a Roundtable Betrugsbekämpfung aimed at identifying concrete measures to combat payment fraud across sectors. The Bundesbank's own account describes participation by banks and other PSPs, telecommunications companies, social platforms such as Meta, retailers, ministries, BaFin, the Federal Criminal Police Office and data- and consumer-protection actors.

Spain now provides a further example of sector-led PSP-to-PSP cooperation. In June 2026, CaixaBank, Banco Santander and BBVA launched FrauDfense Check, the first operational service of their jointly owned company FrauDfense, open to participation by the wider Spanish financial sector. The service is presented as a secure information-sharing mechanism designed to prevent fraud before it occurs, with its pilot phase demonstrating its capacity to detect fraud worth millions of euros.

Crucially, however, the most advanced arrangements are not always national. Salv Bridge operates as a cross-border collaboration network that allows PSPs to launch joint investigations as soon as a suspicion is established, explicitly targeting the delays that render funds unrecoverable in instant-payment environments. EuroDaT, structured as a data-trustee model, goes further still by enabling pre-suspicion information sharing between banks in a secure environment. These private and transnational arrangements are the vertical dimension of the fragmentation problem: they cut across borders without passing through the national schemes that the PSR's decentralised model implicitly assumes.

For a large PSP, the cumulative operational burden could therefore be substantial: joining several national schemes, adapting to multiple APIs, maintaining different impact assessments on data protection, applying different retention periods, and reconciling different rules on when an alert must be created, corrected, withdrawn or acted upon. **Smaller PSPs will most likely lack the resources to participate effectively in all relevant arrangements at once.**

This is the gap that the European Payments Council (EPC) seeks to close with the FRIDA (Fraud Information Distribution Arrangement) initiative. FRIDA is described as an arrangement enabling PSPs, and potentially other stakeholders, to share fraud-related information across SEPA and EPC schemes, with the possible use of a central hub based on the Malware Information Sharing Platform (MISP) or another solution. Importantly, it would involve a preferred *federated* approach that leverages existing national platforms.

FRIDA is the closest European candidate for coordinating Article 83(a) implementation, but it should not be presented as 'the' EU fraud intelligence system. That federated approach is precisely where the difficulty lies – connecting systems is not the same as harmonising the intelligence they contain. A suspicious-IBAN alert in one country is not equivalent to a suspicious-IBAN alert in another if the evidence threshold, fraud classification, confidence level, feedback process and legal consequences differ.

A further design question concerns access. If FRIDA were to operate only through national arrangements, PSPs established or operating in Member States without a mature national framework could face a practical entry barrier. That would be particularly problematic for cross-border PSPs whose fraud exposure is not neatly aligned with a single domestic scheme. A federated model should therefore avoid turning the absence of a national platform into exclusion from the European intelligence layer.

CROSS-SECTOR ARRANGEMENTS UNDER ARTICLE 59(A)

Article 59(a) extends the logic of information sharing beyond the payment sector, in recognition that the origin of payment fraud often lies in fraudulent advertising, phishing pages, spoofed communications or social-engineering activity on digital platforms. Yet the cross-sector arrangements emerging in practice are even less mature, and more dependent on voluntary initiative, than their PSP-to-PSP counterparts.

The clearest live examples are no longer limited to platform- and bank-specific channels such as Meta's Fraud Intelligence Reciprocal Exchange (FIRE). Although FIRE is important, it is limited: it is a UK bank-platform channel in partnership with Meta, not a general EU infrastructure. Its value for this analysis is therefore illustrative rather than institutional. Even so, it shows that direct PSP-to-platform channels can emerge voluntarily, ahead of regulation, while also confirming why platform-specific channels cannot replace a neutral cross-sector framework.

The Global Signal Exchange (GSE) is a closer analogue to the kind of neutral, cross-sector system for signal sharing that Article 59(a) leaves underdeveloped. GSE presents itself as a mechanism for generating real-time insights into the supply chains delivering scams, fraud and other forms of cybercrime by merging multiple data sources and making cybercrime facilitators more visible. The same direction is visible in Cifas' Scamlink initiative, which links member organisations with partners including Meta and GSE so that scam signals can be shared, investigated and used to disrupt online criminal networks.

THE CONNECTIVE TISSUE THAT DOES NOT MOVE DATA

A coherent ecosystem of sharing arrangements would require two further layers that are not themselves arrangements but are preconditions for them to interoperate. **The first is semantic. Fraud intelligence loses most of its value if one PSP classifies an event as impersonation fraud, another as authorised push payment fraud, and still another as mule-account activity.** The Euro Banking Association Fraud Taxonomy and the EPC's own taxonomy work address this by providing a common vocabulary, but a taxonomy moves no data and helps only if operational schemes actually adopt it. Nor should the ambition be purely EU-wide. Scam campaigns, online infrastructure and financial flows are cross-border by design. A European fraud taxonomy would be more valuable if it were compatible with global signal-sharing standards and with comparable taxonomy work in jurisdictions such as the UK, Singapore and Australia.

The second is governance. The Euro Retail Payments Board (ERPB) Working Group on fraud prevention and the Commission-led platform on combating fraud established under Article 83(b) can identify gaps, promote common practices and support soft-law convergence, yet they are coordination fora rather than operational hubs, and they do not themselves impose technical interoperability.

The status of these two layers is therefore the crux of the problem. The arrangements inventoried above will only cohere into a functioning European fraud intelligence network if a common semantic layer is genuinely adopted and a governance layer is empowered to mandate interoperability. At present, both remain largely voluntary. The PSR has built the legal gateways through which fraud intelligence may flow, and the market is building the arrangements that will carry it, but the EU has not yet added the connective tissue that would make these arrangements speak to one another.

Table 2 reorganises the emerging ecosystem according to this functional logic.

Table 2: Emerging ecosystem of arrangements for sharing information on fraud

Initiative	Type	Function	Why it matters	Why it does not solve the whole problem
National schemes (e.g. France's FNC-RF)	Art. 83(a) – PSP-to-PSP	Domestic infrastructure for sharing suspicious-account and fraud-event data.	May be the first concrete Article 83(a) arrangements to operate in practice.	If each Member State builds its own model, PSPs face multiple, non-harmonised, participation obligations (horizontal fragmentation).
Incident Alert System (Netherlands)	Art. 83(a) – PSP-to-PSP	Sector-level sharing of post-suspicion fraud-incident information.	Shows the French model is not isolated.	Another national variant with its own design choices.
Salv Bridge	Art. 83(a) – PSP-to-PSP (transnational, private)	Cross-border real-time collaborative investigation between PSPs.	Closest live example of what Art. 83(a) aims to enable.	Private and transnational; sits outside the national-scheme logic (vertical fragmentation).
EuroDaT	Art. 83(a)-adjacent (data-trustee)	Pre-suspicion, private-private data sharing.	Addresses the pre-suspicion gap that the Art. 83(a) threshold leaves open.	Operates at or beyond the statutory suspicion threshold; governance uncertain.
EPC FRIDA / MISP	Art. 83(a) – federating layer	Pan-European distribution arrangement leveraging national platforms.	The leading candidate to coordinate Art. 83(a) implementation.	Federating is not harmonising; success depends on genuine interoperability of the schemes it connects.
Meta FIRE / GSE / Scamlink	Art. 59(a)-adjacent – cross-sector signal sharing	PSP-platform and broader cross-sector exchange of scam-related signals.	Shows that platform-specific channels and broader signal-sharing systems can emerge before regulation.	Voluntary, uneven and not embedded in a harmonised EU standard; platform-specific channels remain narrower than neutral cross-sector frameworks.
DSA notice-and-action / telecoms channels	Art. 59(a) – cross-sector (PSP–hosting / PSP–ECS)	Legal gateways and channels for hosting and communications providers.	Connect the anti-fraud framework to content and communications layers.	Under-specified: no common API, payload, response-time or escalation standard.

Initiative	Type	Function	Why it matters	Why it does not solve the whole problem
EBA / EPC Fraud Taxonomy	Connective tissue – semantic	Common vocabulary for classifying fraud typologies.	Precondition for semantic interoperability across schemes.	Moves no data; effective only if arrangements adopt it.
ERPB / Platform on combatting fraud (Art. 83(b))	Connective tissue – governance	Policy coordination and soft-law convergence.	Can identify gaps and promote common practice.	Not an operational hub; does not impose interoperability.

Source: Author's elaboration.

COMPARATIVE LESSONS: FRAUD INTELLIGENCE IN OTHER JURISDICTIONS

Section 3 examined the EU's emerging arrangements along the two tracks the PSR distinguishes: the sharing of intelligence between PSPs within the payment sector (Article 83(a)), and cooperation across the other sectors in which fraud originates (Article 59(a)).

Two jurisdictions show, more clearly than the EU's current arrangements, what a more developed approach to each track looks like. The UK is the more advanced example of intra-payment fraud intelligence, with a standardised model of fraud data and a network-level analytical overlay built on its domestic instant-payment rail. It is also moving towards cross-sector disruption through initiatives such as the Online Crime Centre, Stop Scams UK, GSE and Cifas' Scamlink, although much of that layer remains voluntary and industry-led. Australia is the more advanced example of mandatory cross-sector intelligence on fraud, with a whole-of-ecosystem framework coordinated through a public-private operational hub.

Neither is a finished system, and neither is institutionally identical to the EU. They are selected because each isolates a transferable practice that addresses a specific gap in the PSR model: the absence of a common data model and a network view in the first case, and the under-specification of cross-sector cooperation and the lack of an operational hub in the second.

A final qualification is that the UK model is no longer purely intra-payment. The Online Crime Centre and initiatives such as GSE and Scamlink show a move towards cross-sector disruption, linking financial institutions, technology firms, telecommunications actors, law enforcement and government. For the purposes of this analysis, however, the UK remains most relevant for its payment-sector lesson: the standardisation of fraud data and the possibility of a network-level analytical overlay. Its cross-sector layer is important, but it remains more voluntary and less legally integrated than the Australian framework discussed below.

THE UK: A COMMON DATA MODEL AND A NETWORK-LEVEL OVERLAY

The UK's most transferable contribution is not a single platform but a standardised foundation for sharing fraud data. Working with the UK Finance's Enhanced Fraud Data Working Group, Pay.UK – the operator of the country's retail payment systems – developed a logical data model. It categorises the customer and transaction data relevant to fraud, so that both the sending and the receiving PSP can more readily identify a suspect transaction. Pay.UK made its first iteration of the model available through its standards portal.

The model is intended as the basis for a long-term industry standard for how customer data are structured and exchanged. Its significance for the present argument is conceptual rather than technical: it shows that the standardisation of fraud data semantics – the common operational object that the PSR leaves to future arrangements – can be achieved within a decentralised, multi-PSP system, without a single central operator.

The second UK contribution operationalises the network insight that underpins Article 83. Between 2023 and 2024, Pay.UK piloted a fraud-detection overlay service, developed with Visa, Synectics Solutions and Featurespace, in which participating banks and PSPs contributed historical Faster Payments transaction data under a data-sharing agreement. This allowed predictive models to analyse money flows across institutions rather than within the four walls of a single PSP. The pilot reported an average uplift in fraud detection of around 40% at a five-to-one false-positive ratio, equivalent to over GPB 112 million in fraud detected annually, and was designed to be extended to all UK banks and building societies. The overlay is the conceptual successor to the earlier Mule Insights Tactical Solution, which already traced the movement of funds through mule accounts across institutions; it generalises that logic from tracing to prediction.

Two qualifications matter. First, the overlay remains an advanced proof of concept oriented towards deployment, not a fully operational national service. UK industry representatives continue to argue that existing data-sharing initiatives still operate largely in silos and need to be 'industrialised' into a real-time, comprehensive picture of fraudulent activity (Innovate Finance, 2025). Even the most advanced jurisdiction, in other words, has not resolved the problem. Second, and precisely for that reason, the transferable lesson is not 'adopt the UK overlay' but the more durable point that both a common data model and a network-level analytical layer are attainable through industry standards under regulatory steer. The EU's Article 83(a) arrangements will deliver comparable intelligence only if they are built upon the former and oriented towards the latter.

AUSTRALIA: A MANDATORY CROSS-SECTOR FRAMEWORK AND AN OPERATIONAL HUB

Australia addresses the transversal dimension of the problem more directly than any other jurisdiction. The Scams Prevention Framework, passed by both houses of the federal parliament in February 2025, establishes what its regulator describes as world-first, mandatory anti-scam legislation. **Rather than confining anti-fraud obligations to PSPs, it adopts a whole-of-ecosystem approach. The principles-based duties – to prevent, detect, disrupt and respond to scams – apply across designated sectors.** They are underpinned by sector-specific, enforceable codes, with banks, telecommunications providers and certain digital platforms (initially social-media, instant-messaging and search services) designated as the first regulated sectors.

Implementation is now being specified through draft rules and sector codes released for consultation in late May 2026. The first designated sectors – banking, telecommunications and digital platforms – are expected to be subject to the stronger operational duties from 31 March 2027, so the framework remains under construction rather than fully in force (Australian Government, 2026).

For the purposes of fraud intelligence, the framework's defining feature is that information sharing is mandatory and routed through an operational hub. **Designated businesses must share the scam intelligence they gather with the Australian Competition and Consumer**

Commission (ACCC), acting through the National Anti-Scam Centre (NASC), which can then redistribute it across sectors. In the Treasury's own illustration, a digital platform that blocks a fraudulent advertisement may pass the associated telephone number to the ACCC, which forwards it to telecommunications providers so that they can block the same number (Australian Treasury, 2025). This routing function is performed by the NASC, housed within the ACCC, as a public-private fusion capability that had already begun operating ahead of the framework, and which complements the industry-led – and previously voluntary – Australian Financial Crimes Exchange (ACCC, 2025).

The contrast with the EU is precise. Article 59(a) of the PSR creates legal gateways and channel obligations for cross-sector cooperation but, as Section 2.2 noted, leaves the operational substance – the common data, the response times, the escalation paths – unspecified. The platform on combatting fraud established under Article 83(b) is a coordination forum, not an operational hub. The Australian framework supplies exactly the two features the EU model lacks at the transversal level. It has a mandatory cross-sector obligation to share, rather than a conditional gateway, and an institution that actually moves intelligence between sectors, rather than one that merely convenes them. The transferable lesson is therefore institutional: effective cross-sector fraud intelligence appears to require both a binding duty to share intelligence and an operational node empowered to route it, neither of which the PSR currently provides.

POLICY RECOMMENDATIONS: FROM LEGAL PERMISSION TO INTEROPERABILITY

The PSR represents an important shift in EU policy on payment fraud. It recognises that fraud prevention can no longer rely solely on SCA, bilateral controls and *ex post* reimbursement. It creates legal gateways for PSP-to-PSP information sharing and for cooperation with platforms, hosting providers and electronic communications service providers. The remaining challenge is implementation. The EU should now ensure that these legal gateways do not produce a fragmented ecosystem of non-interoperable arrangements. Four policy priorities follow.

First, the EBA should set out common requirements for interoperability in arrangements for PSP-to-PSP information sharing under Article 83(a). This should be done through regulatory technical standards where the PSR mandate allows it and through guidelines where it does not. The objective should not be to impose a single European fraud database or a single mandatory platform. Rather, it should seek to ensure that all Article 83(a) arrangements operate on the basis of a common fraud taxonomy, a standard data model, core alert fields, confidence indicators, time stamps, correction and withdrawal procedures. It should also include feedback loops and generic rules for documenting the objectively justified grounds for suspicion.

Individual arrangements could retain different institutional designs and add further functionalities, but they should not diverge from this common operational layer. Without such unifying requirements, PSPs may be legally required to participate in information-sharing arrangements that remain too heterogeneous to support effective cross-border fraud prevention.

Second, these general interoperability requirements also need a vehicle for implementation. The European Payments Council is the natural candidate for this role: it manages the SEPA scheme rulebooks and coordinates the FRIDA initiative, which is designed to enable fraud-related information sharing across SEPA and EPC schemes. The EPC should embed the

requirements set at the EU level into FRIDA, making the common taxonomy, data model and alert procedures binding conditions for participation in the FRIDA framework.

FRIDA should not be a single mandatory database. Nor should the policy choice be framed as a binary one between a single central platform and fragmentation. **A more resilient model is interoperability by design**: multiple information-sharing arrangements may coexist, but participation in one of them should provide meaningful connectivity to the broader ecosystem.

The architecture should be federated but permeable, connecting national schemes, private arrangements and, where appropriate, PSPs directly. It should include common standards, mutual-recognition rules and routing mechanisms that prevent PSPs from being walled off from intelligence generated elsewhere. Direct or equivalent access will be particularly important for PSPs operating in Member States without a mature national arrangement. This would help to prevent the proliferation of schemes resulting in fragmentation. The problem is not that several schemes may exist, but that they may fail to interoperate.

This interoperability logic should not stop at PSP-to-PSP connectivity. A well-designed EU framework should allow Article 83(a) arrangements to connect, where lawful, necessary and proportionate, with appropriately governed cross-sector mechanisms for sharing signals. Instead of a closed payment-sector loop, the relevant model is a payment-sector intelligence layer that can exchange usable signals with the wider fraud intelligence ecosystem. The UK experience with Cifas' Scamlink and GSE illustrates how a fraud-prevention network can act as an intermediary between financial sector participants and a broader system for signal sharing across sectors.

Third, cross-sector cooperation and intelligence/signal sharing under Article 59(a) should be operationalised through a Commission-led convergence process rather than left entirely to bilateral arrangements. The PSR requires dedicated communication channels between PSPs and relevant actors, such as hosting providers, electronic communications service providers, very large online platforms and very large online search engines. But it does not itself specify the operational content of those channels.

The Commission should therefore use the platform on combating fraud under Article 83(b) to develop model protocols for cross-sector cooperation on intelligence and signal sharing. These should include input from the EBA, the ECB, data protection authorities, digital-services regulators and telecommunications regulators. The protocols should set common expectations on the type of information to be exchanged, alert formats, acknowledgement of notifications, escalation procedures, response-time benchmarks and feedback after action is taken.

For electronic communications providers, the model protocols should also assess whether the general Article 59(a) obligation to detect and prevent impersonation fraud should be translated into more concrete technical expectations at the EU level. Examples can be drawn from national anti-spoofing models such as those adopted in Spain and Finland (Orden TDF/149/2025, 2025; Finnish Transport and Communications Agency Traficom, 2023). This approach would not pretend that the PSR already contains a full technical-standardisation mandate for Article 59(a). Rather, it would use the governance tools available under the Regulation to reduce fragmentation and build a common operational practice. If voluntary convergence proves insufficient, the first review of the PSR should consider introducing a more explicit mandate for binding, cross-sector technical standards.

Fourth, the first review of the PSR should assess whether Articles 83(a) and 59(a) have produced an interoperable ecosystem of fraud intelligence in practice. This review should not be limited to formal compliance with participation duties or the creation of communication channels. It should examine whether PSP-to-PSP arrangements provide a genuine network view of fraud across institutions and borders, and whether cross-sector cooperation enables intelligence to move effectively between PSPs, platforms, hosting providers and electronic communications service providers.

The UK experience shows the importance of a common fraud data model and network-level analysis, while the Australian experience shows the value of an operational public-private node for routing scam intelligence across sectors. If the PSR framework proves too fragmented, the Commission should consider targeted amendments or additional mandates to establish core data standards, stronger cross-sector procedures and, where necessary, an EU-level coordination function for fraud intelligence.

CONCLUSION

The PSR marks a real change in how the EU approaches payment fraud. It accepts that fraud is now driven by deception and manipulation as much as by unauthorised access, and that no single PSP can see the whole fraud chain. Its response is to move from individual security towards collective intelligence, by requiring PSPs to share information with one another and to cooperate with the sectors in which fraud originates. This is the right direction.

Yet, the Regulation stops at the legal basis. It permits and requires sharing without prescribing how that sharing should work in practice, leaving the data models, common vocabulary and governance of the arrangements to the market and to future standards. The central question is therefore not whether PSPs are allowed to share intelligence, but whether the intelligence they share will be interoperable.

This approach risks fragmentation. If each Member State and private provider develops its own scheme, with its own data model, suspicion threshold and rules, PSPs will be obliged to participate in disconnected arrangements and the collective intelligence ambition of the Regulation will be lost.

Comparative experience shows that this outcome is avoidable. The UK demonstrates that fraud data standards and a network-level view of fraud can be achieved across a decentralised system without a single central operator. Australia demonstrates that cross-sector intelligence works only when a binding duty to share is matched by an institution that actively routes that intelligence across sectors. Neither requires the EU to build a mandatory platform. But both point to the same conclusion: the way to avoid fragmentation is to converge on common standards and interoperability by design, not centralisation.

The instruments needed to achieve this already exist. The EBA can specify the common requirements that arrangements must meet. The European Payments Council can embed them in FRIDA and turn federation into harmonisation. The Commission can use the platform on combatting fraud to build standard cross-sector practice. Then, the first review of the Regulation can close any gaps that voluntary convergence leaves open.

What matters now is that these instruments are used deliberately and in good time. The success of the PSR will not be measured by the legal gateways it has opened, but by whether

fraud intelligence actually flows through them in an interconnected, operationally usable form. That will be determined during implementation, where European and national authorities should now concentrate their efforts.

www.ecri.eu

ECRI - European Credit Research Institute

@ECRI_CEPS

EUROPEAN CREDIT RESEARCH INSTITUTE