EBA CLEARING

Real-time transaction monitoring: The future of fraud fighting

How FPAD will support European PSPs' fraud prevention and compliance with the Payment Services Regulation requirements

Based on PSR final compromise text

Executive summary

Fraud levels in European payments are rising sharply, driven by well-resourced criminal networks leveraging the latest technology. Fraudsters are taking advantage of the 24/7 immediacy of instant payment rails and exploiting whichever channel presents the weakest defences.

Regulators are acting to close any weak links targeted by criminals, with the mandatory introduction of verification of payee (VOP) for all SEPA Credit Transfers having marked an important first step. VOP implementation has driven widespread integration of application programming interfaces (APIs) in the payment initiation process, enabling payment service providers (PSPs) to request and consume input from external sources to prevent fraud across the ecosystem.

Building on this, the Payment Services Regulation (PSR) is setting the stage for taking fraud detection and prevention capabilities to the next level: [1]

- Art. 83 requires each PSP to perform transaction monitoring on all incoming and outgoing payment transactions. The Article also specifically requires PSPs to base their transaction monitoring mechanisms on the analysis of historical transaction data and support it with input from information sharing arrangements. It further clarifies that where one PSP carries out transaction monitoring and the other does not, liability rests with the latter.
- Art. 83a requires PSPs to participate in information sharing arrangements and to exchange pseudonymised data with other PSPs for fraud prevention and detection purposes in case of known or suspected fraudulent behaviour by a payment service user.

Transaction monitoring is most effectively done at the network level, where a much broader data view can be taken into account than each individual PSP has on its own. The statistical indicators and signals generated from this network view can be used to enrich each individual PSP's anti-fraud engines with additional intelligence. Importantly, because such monitoring can be performed in real time at the network level, it avoids the delays inherent in end-to-end information sharing models, where suspicious accounts must first be identified and validated before the information can be exchanged and action can be taken.

EBA CLEARING's user community recognised the value of this network-level approach several years ago and joined forces in 2023 to unlock these capabilities through the development of a Fraud Pattern and Anomaly Detection (FPAD) functionality. FPAD enables real-time transaction monitoring for its SEPA payment systems at pan-European scale.

FPAD provides PSPs with a powerful fraud-fighting toolset that can help them meet their PSR-related fraud-fighting obligations. The fraud indicators that FPAD feeds to PSPs cover most of the data elements they must process as part of the required transaction monitoring mechanisms. In particular, FPAD enables PSPs to assess fraud risks based on network-wide transaction history. PSPs should also consider leveraging FPAD as an information-sharing arrangement, which generates a network view based on the analysis of the passive and active feeds received from PSPs. Importantly, FPAD's set-up ensures a level of security and confidentiality proportionate to the nature and extent of the information exchanged.

1 The lay of the land in European payments: Threats and defences

1.1 The dark side of payments

According to the latest available data from the European Banking Authority and the European Central Bank (ECB), in 2024 the total value of fraudulent credit transfers sent by PSPs in the European Union (EU) / European Economic Area (EEA) amounted to €2.5 billion, representing a fraud rate of 0.001%. Comparatively, the value of fraudulent card transactions in the EU/EEA amounted to €1.3 billion.[2]

For the SEPA Credit Transfers (SCT) and SEPA Instant Credit Transfers (SCT Inst) processed by its STEP2 and RT1 Systems, EBA CLEARING witnessed a similar trend.

The sophistication of fraud

The challenge lies not only in the rising volume of fraud, but in the accelerating sophistication of the organisations and techniques behind it. While many still imagine scams as the work of isolated individuals or small groups on the margins of society, the reality is very different. Today's fraud is driven by highly coordinated, well-resourced operations functioning with corporate-like scale and discipline, estimated to command a workforce of close to 1.5 million – making fraud globally a substantial and very complex threat to detect, disrupt and deter.[3]

Criminal networks driving this industrialisation generate tens of billions of dollars through fraud factories, combining professional management structures with forced labour. Compounding this trend is the shifting geopolitical environment, with many organised fraud operations linked to – or even endorsed and supported by – rival power blocs.[4]

Mimicking trends seen in large institutions, these criminal organisations command substantial budgets to be spent on advertisements linked to scams or banned goods. As a result, users of major social and technology platforms are exposed to an estimated 15 billion scam ads every day.[5]

Many also have highly efficient tools at their disposal: from generative artificial intelligence (AI) that translates and sustains conversations, to deepfake video calls and mirrored websites that convincingly imitate legitimate financial institutions (FIs). In one high-profile case, a finance employee at a multinational company was duped into transferring $25 million (€21.3 million) after fraudsters used deepfake technology to impersonate the chief financial officer (CFO) and other colleagues on a video call – all of whom were AI-generated fabrications.[6]

The sophistication extends beyond technology deployed to the time being invested in individual scams. Romance scams, for example, involve criminals cultivating online relationships over months before coercing victims into fraudulent investments, often in cryptocurrency. One survey found average losses of $155,000 (€132,900), with many victims reporting that more than half of their net worth had been wiped out.[7]

1.2 Building up further defences

The rise of highly sophisticated fraud networks means criminals have become adept at navigating around cyber defences, shifting their activity across payment instruments as controls tighten and new weak points emerge. In response, there are growing obligations for PSPs from regulators, as well as emerging pan-European industry initiatives aimed at creating a more resilient, coordinated approach to preventing fraud.

Instant Payments Regulation and VOP

While instant payments bring significant benefits for end users, these same benefits have opened fresh avenues for criminal exploitation. With funds able to move within seconds, 24/7, victims and providers have only a narrow window to intervene – a vulnerability that criminals are increasingly exploiting as money-mule networks expand and diversify.

Both knowing mules (who intentionally support organised crime) and unwitting individuals (recruited through fake job advertisements, phishing schemes or romance scams) are being used to move illicit funds across multiple payment accounts within seconds, making it extremely difficult for PSPs to interfere and recover the funds. Reflecting the scale of this challenge, fraud-related recalls for instant payments are now 10 times higher than for standard credit transfers.

A central pillar of the framework is, therefore, fraud defence – coming in the form of VOP, which checks whether the name and International Bank Account Number (IBAN) of a recipient match before a payment is authorised. By providing greater certainty to the payer, VOP targets misdirected payments and authorised push-payment (APP) fraud – though ultimately it is always the payer who decides whether to proceed.

The early lessons in Europe reflect what has been seen in other markets that have similar initiatives in place. VOP is highly effective at stopping genuine mistakes: typos, incorrectly entered details or outdated beneficiary information. Its value in preventing fraud, however, is limited, because many scams involve accounts where the name superficially matches, or where fraudsters co-opt legitimate accounts ('mule accounts') that pass the name check.

In parallel, fraudsters are also shifting back into traditional SEPA Credit Transfers, pushing fraud values in non-instant products to their highest levels on record. Even SEPA Direct Debits, historically low-risk, are now being actively targeted.

Payment Services Regulation

While VOP has proven effective in certain use cases, its limitations make it clear that fraud defences must go further. The PSR represents that next step, making real-time transaction monitoring an obligation for PSPs.

Concretely, the amended Payment Services Directive 2 (now PSD3) and the new PSR, introduce a reform package that, among its objectives, aims to better contain payment fraud and strengthen overall consumer security.[8]

Under the PSR, PSPs on both sides of the transaction must put in place effective transaction-monitoring mechanisms to prevent and detect fraud. Crucially, Art. 83 makes this an explicit legal obligation: the payer PSP must carry

out transaction monitoring checks before a payment is executed, while the payee PSP must carry out transaction monitoring before the funds are made available to the payee. In this context, existing controls – such as strong customer authentication – are no longer sufficient in isolation to demonstrate that a transaction was authorised and/or legitimate. The controls required by the regulation must also keep pace with increasingly adaptive fraud, with the PSR emphasising that transaction monitoring must be continuously improved, making full use of technologies such as AI and increasingly rich, up-to-date fraud intelligence.

Where the required transaction monitoring checks are not carried out in accordance with the PSR, or where a PSP cannot demonstrate that such checks have been performed, the PSP will be liable for any resulting losses from fraudulent transactions, unless the payer has acted fraudulently. Compliance by only one of the PSPs involved in a transaction is not sufficient. Where one PSP performs the required transaction monitoring and the other does not (or cannot evidence that it has done so), the PSP that failed to apply or demonstrate the required controls will bear liability for any financial losses incurred by the payer. It is important to note that the burden of proof falls on the PSPs and not the end user.

PSPs should base their transaction monitoring mechanisms on the "analysis of previous payment transactions". In practice, this encompasses any payment data up to the current moment. Importantly, tools to support PSPs with this monitoring are already available as a standard feature within the pan-European infrastructures STEP2 and RT1 *(see Box: Real-time transaction monitoring with FPAD)*.

The PSR also explicitly states that the transaction monitoring outlined in Art. 83 should rely, among others, on information sharing arrangements. This means that PSPs are required to exchange data where there are justified suspicions of fraud.

This is supported by Art. 83a of the PSR, which pushes institutions toward more active cooperation by requiring stronger information sharing on known or suspected fraudulent accounts and mule networks. Information is to be exchanged through information sharing arrangements as defined by the PSR and used to the extent necessary for PSPs to prevent and detect potentially fraudulent payment transactions. This new legal requirement aims to close the gaps exploited by organised criminals, who often move funds quickly across multiple PSPs to avoid detection.

Further legal comfort is provided by Art. 75 of the EU Anti-Money Laundering Regulation (AMLR), which explicitly permits the sharing of customer and transaction data where necessary to comply with AML and countering the financing of terrorism (CFT) obligations – as well as to detect, prevent and investigate related offences, including fraud-related activity, subject to strict data-protection safeguards.[9]

Nevertheless, despite a certain and solid legal basis for PSPs to rely on, direct and end-to-end data sharing will likely remain cautious, controlled and constrained by liability considerations and data protection requirements, since any future model must balance this enhanced information exchange with necessary safeguards that prevent unintended harm to customers or payment flows. As a consequence, the effectiveness of this data sharing approach is further constrained by time lags.

In this context, EBA CLEARING's FPAD functionality provides a practical example of an information sharing arrangement in which PSPs can participate and leverage shared risk indicators and models that support these regulatory objectives *(see 2.2 How PSPs can leverage FPAD to comply with the PSR)*.

Pan-European industry initiatives

Pan-European collaboration has become central to strengthening Europe's fraud-prevention capabilities with the understanding that improving each stakeholder's fraud prevention and detection capabilities will have a multiplying effect across the ecosystem, and thus benefit each player individually. For example, the European Payments Council (EPC)'s Malware Information Sharing Platform (MISP) provides a SEPA-wide mechanism for PSPs to share fraud-related intelligence. The Fraud Information Distribution Arrangement Task Force (FRIDA TF), established in 2025, goes further by creating a structured arrangement for exchanging fraud information, supporting interoperability between national schemes and advising on fraud-prevention measures across EPC-managed SEPA payment schemes.[10]

Complementing these efforts is EBA CLEARING's FPAD, which enriches the risk views of individual PSPs with insights for fraud prevention and detection that only a network-wide perspective can provide. The network view provided by FPAD is based on the payment transactions processed by the pan-European STEP2 and RT1 payment systems operated by the Company, which is a European-owned, European-governed and European-regulated provider of payment infrastructure services. The processing of STEP2 and RT1 payment transactions and FPAD data takes place in the EU and in accordance with EU laws.

FPAD can help PSPs fulfil their obligations for transaction monitoring, in particular by assessing risks based on transaction history, including transaction information on both the payer and payee, the payment instrument, currency, date and time of execution, as well as the unique identifier of the payee, information on the payee and information received through information sharing arrangements.

Completing the picture is the fraud taxonomy by the Euro Banking Association (EBA), which equips fraud fighters with a harmonised pan-European vocabulary and categorisation approach for naming and organising fraud types for payments. By harmonising definitions across markets and making data more comparable, it aims to improve the quality of fraud monitoring, reporting and information sharing – supporting the overall shift towards coordinated, pan-European fraud-fighting by helping to classify the data shared through the EPC's MISP or used by EBA CLEARING's FPAD.

In Art. 83 (2b)(c), the regulation stipulates that transaction monitoring mechanisms take into account known fraud scenarios. In order to keep pace with the evolving fraud threat landscape, the EBA Fraud Taxonomy, which was developed with PSPs across Europe, is updated on an annual basis.[11] PSPs can apply this taxonomy in their active feeds back to FPAD, including feedback as well as transaction and account insight notifications. This means that when PSPs use FPAD for their transaction monitoring, their active and passive (fraud recalls) feeds can be leveraged for training FPAD's models with more granular information on known fraud scenarios.

REAL-TIME TRANSACTION MONITORING WITH FPAD

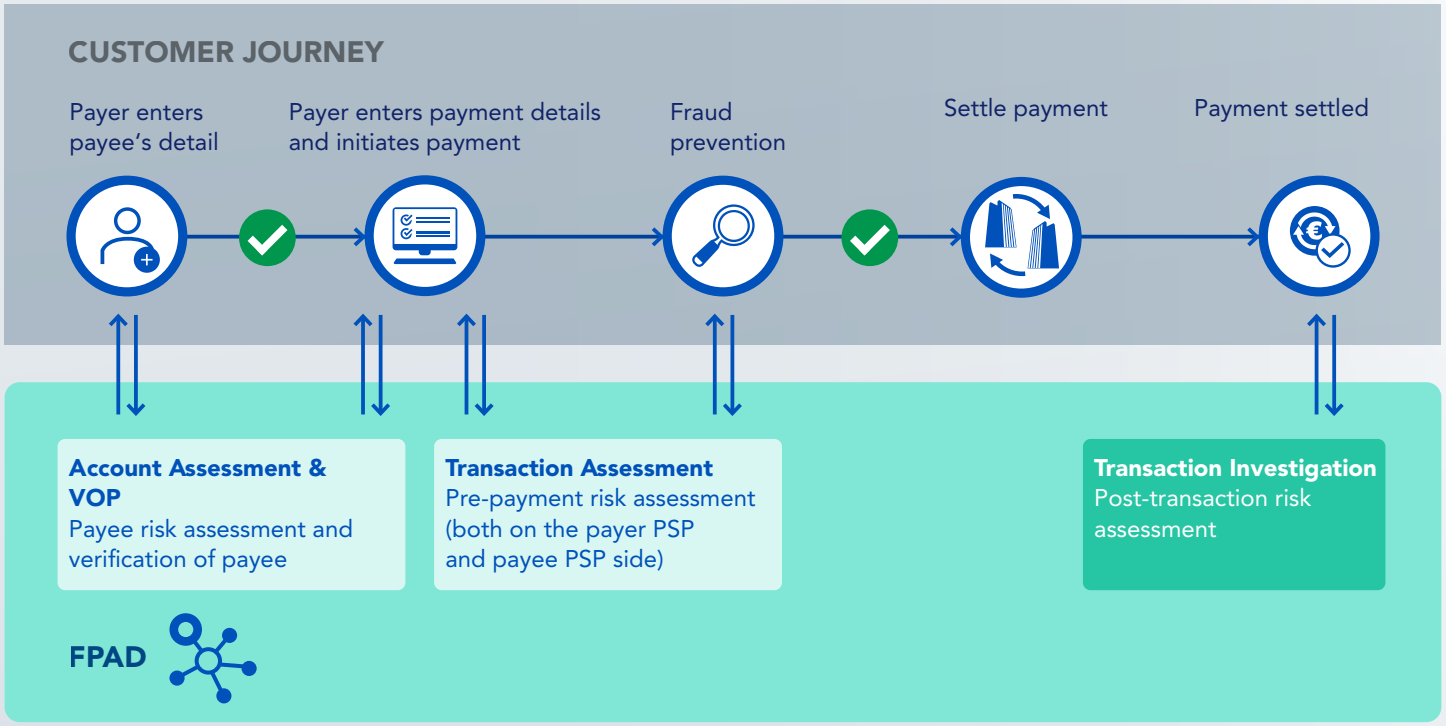
FPAD is a real-time transaction monitoring functionality, which gives STEP2 SCT and RT1 SCT Inst Participants access to a wide range of fraud prevention and detection tools. It was developed at the request, and with the active involvement, of fraud experts from across the user community of EBA CLEARING's SEPA Credit Transfer services.

FPAD enables STEP2 and RT1 Participants to take the fight against payment fraud to the next level by enriching their individual risk views with insights that only a network view can provide. FPAD offers several modules, which cover the whole range of fraud fighting: from fraud prevention (before a transaction is sent) to fraud detection (after clearing and settlement). Based on its pan-European view of the payment activity in the STEP2 SCT and RT1 SCT Inst Services, FPAD identifies patterns of known fraud and anomalous payment behaviours, and provides insights into payment and beneficiary account behaviours unavailable to any individual PSP.

FPAD also offers a VOP function, supporting PSPs in meeting the requirements of the IPR. The use of historical data for transaction monitoring, as demonstrated by FPAD, becomes a regulatory requirement under the PSR – and is already available today to all participants in EBA CLEARING's SEPA Credit Transfer services.

The different FPAD modules were designed to be easily integrated to enhance PSPs' existing payment, fraud prevention and investigation systems and processes.

Figure 1
HOW DOES FPAD WORK?



2 The future of fraud fighting in European payments

2.1 Why building out transaction monitoring is most promising

Network-level analytics are already possible today, grounded in a PSP's legitimate interest to protect its customers from fraud. The PSR requirements will provide additional legal comfort, clarifying the basis for using such insights. By making the liabilities for PSPs dependent on the amount of work done to prevent fraud, the PSR creates powerful incentives for banks and other PSPs to invest in more robust detection and prevention capabilities.

Real-time transaction monitoring sits at the centre of this approach. It observes patterns and anomalies as they emerge, dynamically tuning the underlying statistical models based on the transactions flowing through the system. By working at the level of indicators, rather than raw transaction data, including personal data, a framework such as FPAD enables its user community to generate collective intelligence across the network without disclosing sensitive information – delivering stronger defences built on a solid, privacy-by-design foundation.

Why does transaction monitoring matter? Fraudsters may use different instruments, such as wallets, crypto assets or alternative transfer channels, to obscure the trail or move funds across borders. But they need to use traditional payment rails to get the money out of their victim's account. That is the moment when patterns, behaviours and anomalies become visible, allowing PSPs to detect suspicious activity and intervene.

The foundations are already here

One significant advantage for the industry is that VOP has become a crucial enabler for transaction monitoring. Before its introduction, the absence of real-time name checking was a clear weak link in the chain, as PSPs often had limited ability to validate beneficiary details or draw on external intelligence before executing a payment.

The mandatory rollout of VOP under the IPR changed that – and went one step further. By forcing widespread adoption of APIs and technical connectivity for real-time name checks across the ecosystem, it prepared PSPs – both technologically and operationally – for the exchange of a larger fraud-relevant dataset in real time.

These same capabilities can now underpin transaction monitoring. PSPs can enrich front-end checks with deeper network-level indica-

tors and consume external signals before releasing funds (see Box: The power of transaction monitoring: Enhancing VOP results and customer experience).

Just as importantly, this connectivity allows PSPs to feed back anomalies they detect, helping others tune their fraud-fighting models and improving the collective intelligence of the ecosystem. In this way, VOP has acted as a stepping stone: a regulatory requirement that has not only strengthened APP-fraud defences, but also created the infrastructure and readiness needed for the far more advanced, network-wide transaction-monitoring approach mandated by the PSR.

European PSPs already started to move in this direction ahead of formal PSR/PSD3 implementation. To further strengthen customer protection and trust, as well as curb fraud losses, they have been working collectively to build fraud-fighting capabilities that outperform anything they would be able to achieve on their own.

Tackling the weakest links

By allowing PSPs to ingest network indicators and statistical signals into their anti-fraud tools, transaction monitoring makes it possible to analyse patterns and anomalies across the network using statistical models and machine learning. This matters because fraudsters operate across networks, not within the boundaries of a single PSP – meaning that an indicator which appears benign in one institution can become highly meaningful when viewed alongside signals from others.

And by analysing behaviour on the beneficiary account side – not just on the payer account side – PSPs can more effectively identify mule accounts, which often display recognisable patterns of incoming and outgoing flows.

THE POWER OF TRANSACTION MONITORING: Enhancing VOP results and customer experience

When a customer performs a VOP check, their subsequent payment steps will be guided by the VOP result, with the payment either sent or withheld. The figure below shows how FPAD Account Assessment risk indicators can be used to improve VOP check outcomes.

FPAD VOP supports both of the challenges outlined below. The solution goes beyond the basic IBAN/name check by layering in a broad range of network-based fraud risk indicators, which helps PSPs strengthen their defences against a wider spectrum of threats, and to reduce unintended VOP friction for their customers.

REDUCING RISK WITH FPAD

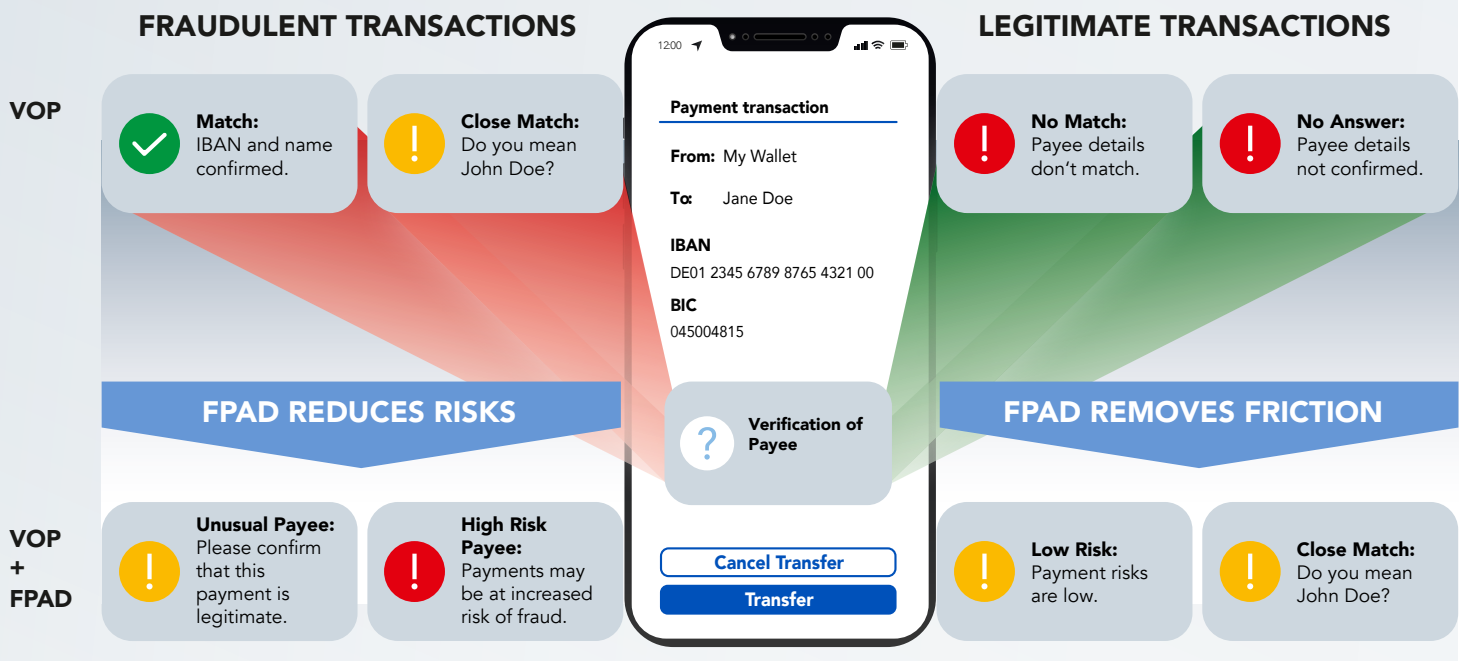
When a VOP check returns a match or close match, it can create a false sense of security about the payment. Yet successful VOP checks provide no guarantees that the transaction itself or the payee involved is not fraudulent. FPAD reduces fraud risk by identifying unusual, high-risk and known fraudulent payee accounts – giving context that a name match alone cannot provide. FPAD risk indicators can trigger additional warnings, helping to reduce the risk of fraud.

REMOVING FRICTION WITH FPAD

When a VOP check fails, this can create unnecessary friction – leading to a legitimate payment being stopped or abandoned. For example, a "No Match" result might wrongly indicate that the account details are incorrect because of minor issues.

FPAD indicators help PSPs reduce this friction by assessing payee risk using the network-wide view of activity. It can support a qualified alternative to a strict name match and can also extend VOP coverage when a counterparty PSP is temporarily unavailable. By combining these indicators, PSPs can give customers clearer, risk-based feedback – allowing them to authorise low-risk payments with confidence, rather than rejecting them.

Figure 2
IMPROVING VOP EXPERIENCE WITH FPAD RISK INDICATORS



2.2 How PSPs can leverage FPAD to comply with the PSR

The PSR stipulates in Art. 83 (1b) that PSPs' transaction monitoring mechanisms shall be based on the analysis of previous payment transactions and access to payment accounts online. Art. 83 (2) and (2a) specify the data that the payer PSP's and the payee PSP's processing should be limited; this includes information received through information sharing arrangements.

PSPs can fulfil many of these fraud prevention and detection obligations by feeding their transaction monitoring mechanisms with FPAD output. Among other things, FPAD supports PSPs in meeting the requirement to take into account the payment history of the involved payment accounts. FPAD provides PSPs with risk indicators based on patterns and anomalies of previous transactions, without sharing the underlying data of those transactions. This is underpinned by robust technical and organisational safeguards, including pseudonymisation, ensuring a high level of security and confidentiality. Based on the indicators provided by FPAD, PSPs will decide whether to process a payment transaction or not. The decision and control will always remain with the PSP.

PSPs may also obtain from FPAD transaction information on both the payer and payee, the payment instrument, currency, date and time of execution, as well as the unique identifier of and information on the payee, and the name of the payer. To this extent, FPAD could be considered by PSPs as one of their information sharing arrangements. What makes information sharing through FPAD particularly powerful is that it enables PSPs to continuously enhance data quality through passive feeds (fraud recalls) and active feeds (feedback, transaction and account insight notifications) – enabling FPAD's models to be trained with known fraud scenarios in the provision of payment services.

Figure 3

Data to be processed <u>by the payer PSP's</u> transaction monitoring mechanism, PSR Art. 83 (2)

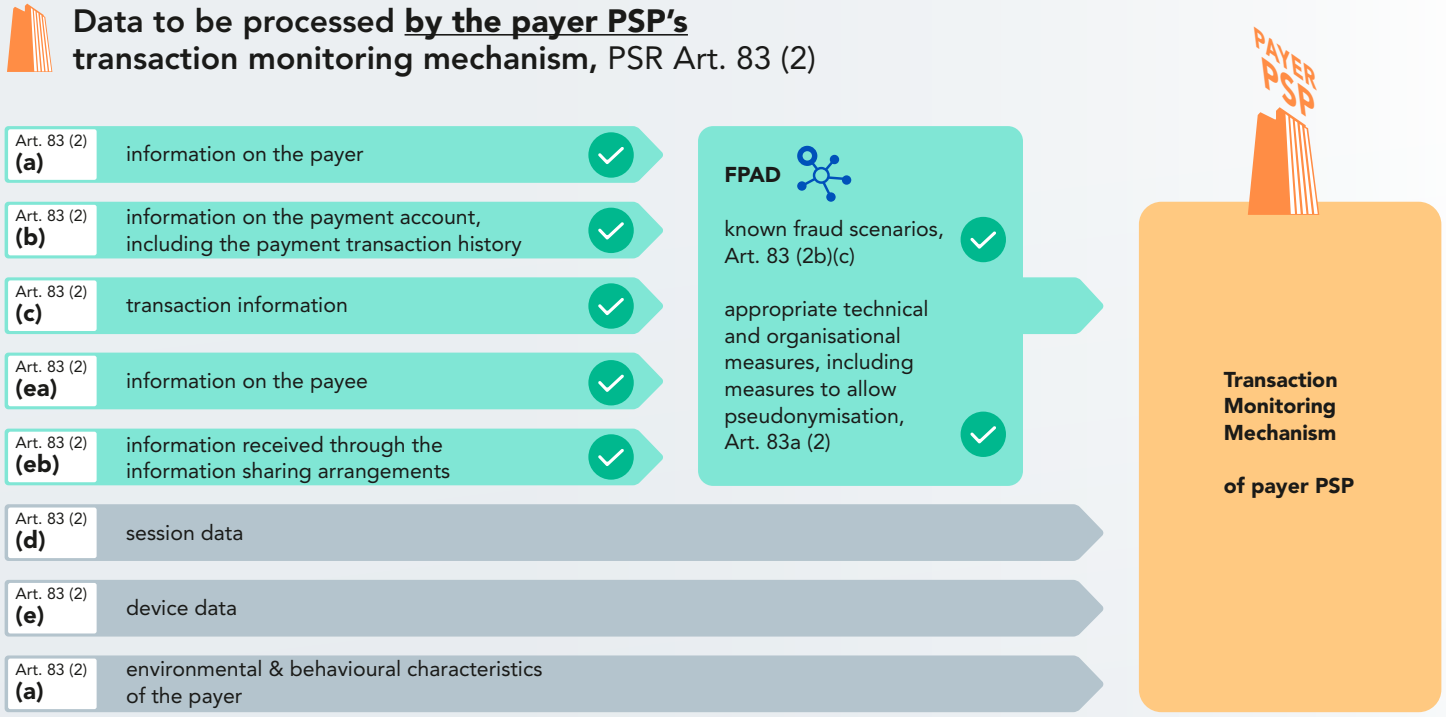
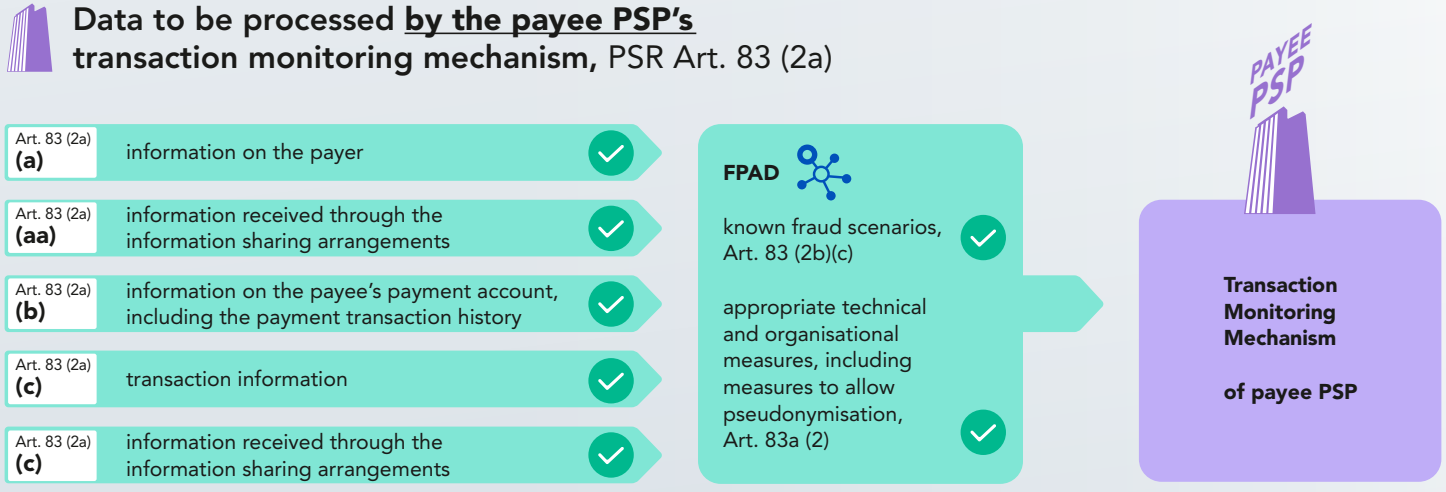


Figure 4

Data to be processed <u>by the payee PSP's</u> transaction monitoring mechanism, PSR Art. 83 (2a)



3 Conclusion

Regulators are intensifying pressure on PSPs to strengthen their fraud detection and prevention defences, introducing new obligations with tight timelines. With these regulatory changes, the burden of proof and liability of fraud losses is shifted entirely to PSPs. These efforts are well founded. Fraud levels continue to rise, with bad actors exploiting weaknesses in the payment chain, and regulators – and the wider industry – progressively looking to close these gaps as they emerge.

The next phase in this journey will be defined by the expansion of real-time transaction monitoring, underpinned by the PSR. Fortunately, the industry is not starting from scratch. VOP has driven the widespread integration of APIs into the payment-initiation process, which can now be repurposed for transaction monitoring, while community-driven initiatives such as FPAD already provide an effective, live solution. Together, these developments have established strong foundations for more advanced fraud defences and puts PSPs in a strong position to address the new compliance requirements stemming from the PSR.

As the ecosystem evolves, a fundamental reality remains: the defence of the network is defined by the weakest link in the chain. The effectiveness of real-time transaction monitoring will depend on broad and consistent adoption. Even the most advanced capabilities will have limited impact if participation is partial – and where PSPs do not consume indicators and act on insights, those gaps may become the next points of criminal exploitation.

Effective fraud fighting at scale requires coordinated action at a pan-European level. Only through collective action can the industry reduce systemic vulnerabilities and strengthen the resilience of the payments ecosystem for the benefit of the European economy and its stakeholders.

1 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulations (EU) No 1093/2010, (EU) No 260/2012, (EU) 2017/2394, (EU) 2021/1230 and (EU) 2023/1114 – Confirmation of the final compromise text with a view to agreement (17 April 2026 – ST 8221 2026 INIT – NOTE), available at: Council of the European Union (accessed 5 June 2026).

2 European Banking Authority and European Central Bank, Report on Payment Fraud, December 2025, available at: European Banking Authority (accessed 5 June 2026).

3 The Economist, 'The vast and sophisticated global enterprise that is Scam Inc', The Economist, 6 February 2025, available at: The Economist (accessed 5 June 2026).

4 Council of the European Union, Organised Crime Report 2025, July 2025, available at: Council of the European Union (accessed 5 June 2026).

5 Reuters, 'Meta is earning a fortune from deluge of fraudulent ads, documents show', Reuters, 6 November 2025, available at: Reuters (accessed 5 June 2026).

6 CNN, 'Deepfake CFO scam in Hong Kong', CNN, 4 February 2024, available at: CNN (accessed 5 June 2026).

7 The Guardian, 'Scam state: the multi-billion-dollar industry in South East Asia', The Guardian, 2 December 2025, available at: The Guardian (accessed 5 June 2026).

8 PSR final compromise text (see endnote 1)

9 The Financial Crime News, 'EU Article 75: Pan-EU information sharing is coming, but will it be enough?', The Financial Crime News, available at: The Financial Crime News (accessed 5 June 2026).

10 European Payments Council, 'Fraud Prevention and Payment Security', available at: European Payments Council (accessed 5 June 2026).

11 Euro Banking Association, EBA Fraud Taxonomy – Management Summary, June 2025, available at: Euro Banking Association (accessed 5 June 2026).

Imprint

ABE CLEARING S.A.S. À CAPITAL VARIABLE (EBA CLEARING)
Authorised share capital: EUR 200,000
40 rue de Courcelles, F-75008 Paris
VAT n°: FR 52419020193
RCS Paris 419 020 193
WWW.EBACLEARING.EU

CONCEPT AND TEXT
EBA CLEARING
40 rue de Courcelles
F-75008 Paris

GRAPHIC DESIGN & ILLUSTRATION
formfellows
Kommunikations-Design
Frankfurt am Main

CONTACT
clearing@ebaclearing.eu

PUBLICATION DATE
9 June 2026