AMLYZE

WHITE PAPER · PAYMENTS & FINANCIAL CRIME

Fraud, redrawn

Real-time, ecosystem-wide fraud defense

By Eglė Kontautaitė

AMLYZE Head of Client Solutions

Published August 2026 · Basis: PSR published text, Council doc 8221/26

ABOUT THIS PAPER

How the EU Payment Services Regulation moves payment-fraud prevention from post-transaction reimbursement to real-time, ecosystem-wide, AML-adjacent defense.

A white paper for payments, fraud, AML and compliance leaders – and the senior business readers who own the risk.

The Payment Services Regulation (PSR) reshapes how payment fraud is prevented and remedied across the EU. This paper sets out the four paradigm shifts the PSR introduces, what they require of payment service providers (PSPs), and how fraud prevention and anti-money-laundering (AML) controls become operationally interdependent. It is written for a mixed audience: rigorous on the law, but each section opens with a plain read on why it matters. Where the law is explained, so is the reasoning behind it – the European Commission's own impact assessment supplies the evidence the legislator acted on.

Content

	Executive summary	3
1	The framework shift: one rulebook, full harmonisation	4
2	Four paradigm shifts in fraud prevention	6
3	Reimbursement redrawn	8
4	Fraud prevention – from siloed towards ecosystem	11
	Box No. 1 · Checklist for assessing the fraud-prevention vendor	13
5	AML and fraud convergence within payment service regulation	17
6	Conclusion: from regulation to implementation	20
	Box No. 2 · Practical readiness check	22

This paper reflects the author's own analysis and views. It is provided for information only and does not constitute legal advice; readers should seek their own professional advice on how the PSR applies to their circumstances.

Executive summary

THE PSR DOES NOT MERELY ADD CONTROLS – IT CHANGES THE PHILOSOPHY OF PAYMENT-FRAUD REGULATION

Under PSD2, the regulatory approach to payment fraud remained comparatively reactive: prevention centered largely on Strong Customer Authentication (SCA), while the liability framework operated primarily after fraud had occurred, through reimbursement of unauthorized payment transactions.. The PSR reorders that logic around prevention. Four shifts define it:

1. **Reimbursement is redrawn:** a new, harmonized duty to refund victims of PSP-impersonation fraud extends liability beyond unauthorized transactions and extends the burden of proof onto the PSP.
2. **Prevention replaces siloed SCA with a lifecycle of statutory controls –** Verification of Payee (VoP), customer-defined limits, transaction monitoring and the power to refuse or suspend execution.
3. **Responsibility widens from a single PSP to an ecosystem –** the payee's PSP, telecoms, online platforms and hosting providers all acquire duties.
4. **Fraud prevention and AML become operationally interdependent,** sharing the same intervention mechanism for overlapping but distinct objectives – protecting the victim, pursuing the perpetrator.

For PSPs, the practical consequence is that liability now turns on proving the whole prevention framework was in place – not just that a transaction was authorized. The framework is agreed but not yet published in the Official Journal; once it is, the clock runs to general applicability in 2028, with the PSR's Verification of Payee provisions following six months later. On VoP, though, the clock has already run. The Instant Payments Regulation has required euro-area PSPs to offer verification of payee on every SEPA credit transfer – instant or not – since 9 October 2025, with PSPs outside the euro area following on 9 July 2027.[1] Which makes 2028 a poor planning anchor: part of the framework is already running, and the institutions that fare best will be the ones already operating fraud, AML, legal and operations as a single connected capability – not assembling one against a deadline.

The evidence behind that reordering explains the shape of the rules. The Commission's own impact assessment found that strong customer authentication worked: it stripped out most of the card fraud where the customer never approved the payment. But it cannot reach the fraud that took its place. In a scam the customer is tricked first and authenticates second, so the check passes – the right person really did approve the payment. The deception is complete before authentication begins. On EBA data, credit transfers carried the lowest fraud rate of any instrument and the highest aggregate fraud value, and 43% of that value came from manipulating the payer into authorizing the payment themselves. That is a prevention problem wearing the clothes of an authorization problem, and prevention is what the PSR legislates.[2]

[1] Regulation (EU) 2024/886 (Instant Payments Regulation), amending Regulation (EU) No 260/2012 (SEPA Regulation). The verification-of-payee obligation applies to all SEPA credit transfers, standard and instant, from 9 October 2025 for PSPs in Member States whose currency is the euro and from 9 July 2027 for those outside the euro area.

[2] European Commission, Impact Assessment accompanying the proposals for a Payment Services Regulation and a recast Payment Services Directive (PSD3), SWD(2023) 231 final, 28 June 2023, pp. 8–10. Strong customer authentication is credited there with substantially reducing unauthorised fraud, while authorized push payment (APP) fraud is found to be beyond its reach because the transaction is authorized by the payer.

1 The framework shift: one rulebook, full harmonisation

WHY IT MATTERS *A regulation applies directly and identically in every member state – there is no national transposition to wait for, and no room to gold-plate or diverge.*

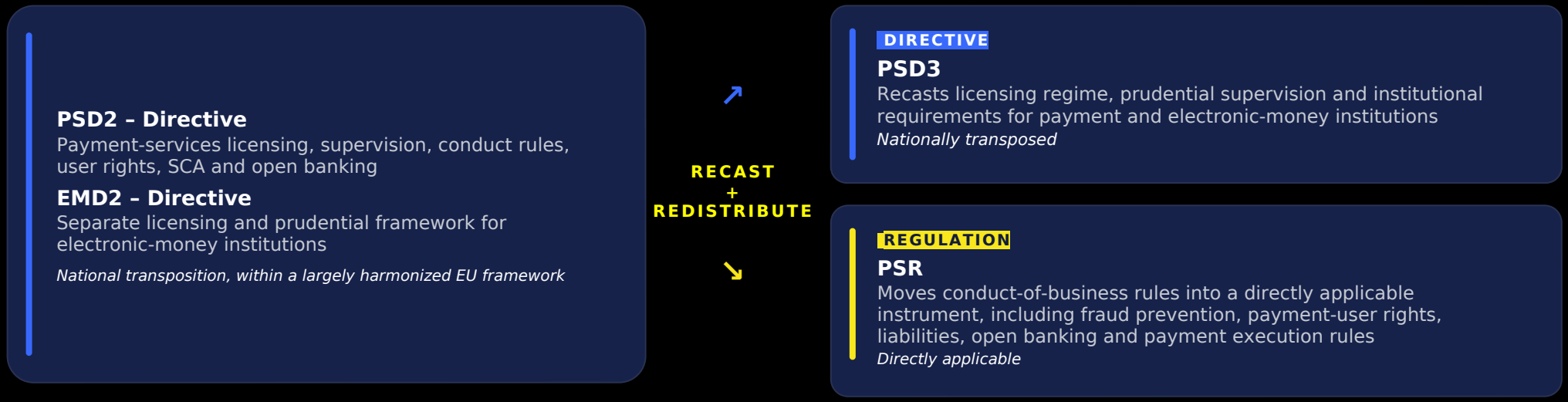


Figure 1. A move from nationally transposed operational rules to a more uniform, directly applicable EU rulebook.

PSD2 and the second E-Money Directive (EMD2) are both repealed. Their successor is deliberately split. PSD3, a directive, recasts licensing and prudential rules and folds e-money institutions into the payment-institution regime; because it is a directive, it is still transposed into national law and can vary at the edges. The Payment Services Regulation is the new instrument: a regulation, directly applicable EU-wide, carrying the conduct-of-business rules – SCA, open banking, fraud prevention measures and, for the first time in harmonized form, an authorized-fraud reimbursement framework.

What changed is not only the level of harmonization but also the route to it. Whether a text harmonizes minimally or fully is set by its own wording, not by whether it is a directive or a regulation: PSD2 was itself largely maximum-harmonization in its core conduct rules, and a regulation can still leave discretion where it expressly says so. The weakness of PSD2 was structural rather than definitional. As a directive it had to be transposed into national law in every member state, and the discretions it left – compounded by divergent implementation – fragmented the single market and opened room for regulatory arbitrage. The PSR removes the transposition layer: one directly applicable text, with member state discretion confined to the areas the regulation narrowly specifies. The revision was driven by the rise of new fraud types – a consumer-protection concern – and by that arbitrage. The decision that followed was structural: conduct rules for PSPs must apply uniformly and move into a

regulation, while licensing and supervision – the supposedly more flexible matters – remain in a directive.

The case for extending fraud prevention beyond authentication was measured rather than assumed. Successive years of harmonized fraud reporting after PSD2, reviewed by the EBA for the Commission and then quantified in its impact assessment, tracked where authentication was holding and where it had stopped being the relevant control at all. The implementation of PSD2 and SCA substantially reduced unauthorized payment fraud by making the misuse of stolen credentials significantly more difficult. Rather than overcoming authentication, however, fraudsters increasingly shifted towards social-engineering schemes – including invoice fraud, impersonation fraud and other authorized push payment (APP) scams – in which the payer is deceived into authenticating the payment personally. Because these transactions are both technically and legally authorized, SCA cannot distinguish a genuine payment from one made under deception: the authentication is successful, while the payer's intention has already been manipulated.

The statistical evidence illustrates this evolution. The joint EBA–ECB payment fraud report demonstrates (Figure 2) that although the overall fraud rate remained broadly stable, the total reported value of payment fraud increased from approximately €3.5 billion in 2023 to €4.2 billion in 2024. Credit transfers accounted for the largest share of fraud losses (approximately €2.2 billion), while payment service users bore around 85% of those losses, predominantly in fraud scenarios involving payer manipulation. The EBA and ECB conclude that SCA continues to be effective against the fraud types for which it was designed, but that fraudsters are increasingly exploiting the manipulation of payers, requiring mitigation measures beyond authentication alone.

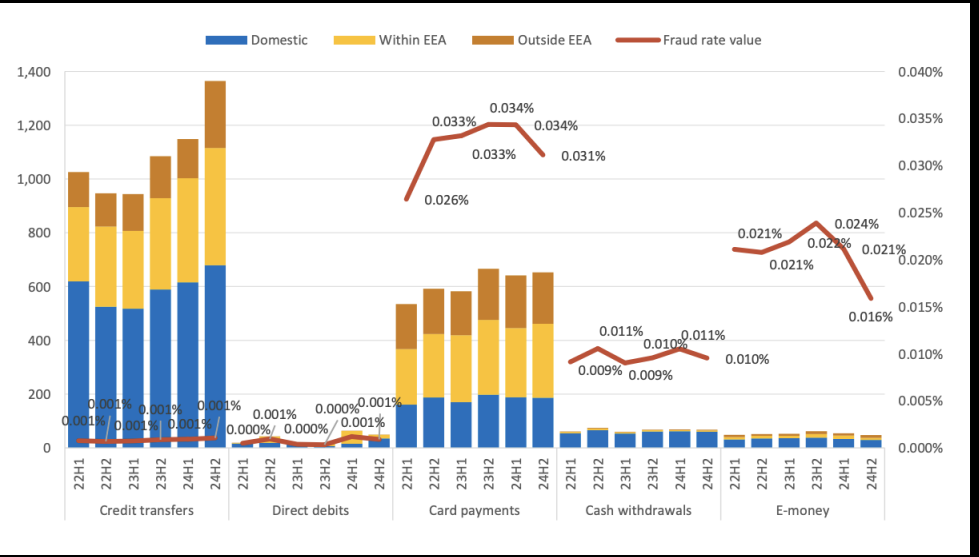


Figure 2. Absolute and relative levels of fraud by type of payment instrument (in values) *(left axis: total value of fraud (million EUR); right axis: fraud as a share of the total value of transactions of that type)*[3]

The data point to a conclusion that although PSD2 successfully strengthened verification of intention to execute payment, but fraud increasingly migrated from attacks on authentication towards attacks on the customer's decision-making. The PSR responds to this issue by complementing SCA requirements with preventive measures that operate before, during and after authentication, including Verification of Payee, transaction monitoring, fraud intervention powers, payment limits, fraud information sharing and a targeted reimbursement framework for certain authorized fraudulent transactions.

[3] EBA and ECB, 2025 Report on Payment Fraud, EBA/REP/2025/40, 15 December 2025, chart on absolute and relative levels of fraud by type of payment instrument..

WHY IT MATTERS *The PSR is best read as four changes of philosophy of fraud prevention – each one moving fraud prevention earlier, wider and closer to the perpetrator and predicate crime itself with an objective to protect the fraud victim.*

2 Four paradigm shifts in fraud prevention



Figure 3. The four paradigm shifts – what moves, and the PSR articles that carry each one

The fraud-related provisions of the PSR are best understood not as a collection of isolated amendments but as a coherent transformation of the regulatory approach to payment fraud. Rather than introducing a single new control, the Regulation restructures the allocation of responsibilities throughout the payment lifecycle. This transformation may be viewed through four interconnected paradigm shifts, each addressing a different weakness of the PSD2 framework and together forming a comprehensive fraud-prevention model.

First, the PSR fundamentally redraws the reimbursement framework. Under PSD2, reimbursement obligations were primarily designed around unauthorized payment transactions. The PSR retains that protection but extends liability to selected categories of authorized fraud, strengthens reimbursement rights in specific fraud scenarios, expands evidential burden for payer PSP and introduces recourse mechanisms between payment service providers of payer and payee.

Second, the Regulation shifts the regulatory focus from authentication towards broader fraud prevention. SCA remains a central security measure, but it is complemented by additional preventive controls operating before, during and after payment execution, including VoP, transaction monitoring, intervention powers, customer-controlled transaction limits and fraud-information sharing. Rather than replacing authentication, the PSR embeds it within a wider framework designed to prevent fraud that authentication alone cannot address.

Third, fraud prevention expands beyond the boundaries of an individual payment service provider. The PSR recognizes that effective fraud prevention depends upon coordinated action across the payment chain, including cooperation between payer's and payee's payment service providers, telecommunications providers, online platforms and other actors capable of disrupting fraud before criminal proceeds disappear. Fraud monitoring therefore

evolves from an institution-centric function into an ecosystem of distributed responsibilities.

Finally, the PSR brings fraud prevention and anti-money laundering into closer operational alignment. While their legal objectives remain distinct, both regimes increasingly rely upon similar intervention mechanisms, information-sharing arrangements and operational decision points. The Regulation therefore creates an interface between fraud prevention and AML obligations without merging the two legal frameworks.

These four shifts are cumulative rather than independent. The redesign of reimbursement supports a stronger preventive model; prevention becomes more effective through coordinated action across the payment ecosystem; and that broader ecosystem naturally creates points of convergence with anti-money laundering processes. Together they illustrate the PSR's transition from a framework centered primarily on authenticating payment transactions towards one designed to prevent, interrupt and respond to fraud throughout the payment lifecycle.

WHY IT MATTERS *For the first time, a transaction the customer themselves authorized can be refundable in full – and the PSP, not the customer, must prove why it should not be.*

3 Reimbursement redrawn

> *Where a payment services user who is a consumer was manipulated by a third party pretending to be the consumer's payment service provider using communication channels attributed to the consumer's payment service provider and that manipulation gave rise to subsequent fraudulent authorized payment transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorized payment transaction under the condition that the consumer has, without undue delay after becoming aware of the fraud, notified its payment service provider and reported the fraud to the police.*
>
> **PSR Art. 59 (published text, doc 8221/26)**



Figure 4. Article 59 in four conditions – who is protected, which fraud, what transaction status, and what the consumer must do

The centerpiece of the new authorized-fraud liability framework is Article 59, which establishes a harmonized reimbursement mechanism for impersonation fraud. The provision combines two interdependent elements. **First**, it imposes a preventive obligation on payment service providers to maintain adequate prevention measures and robust technical safeguards capable of preventing fraudsters from replicating or misusing communication channels attributed to the PSP. **Secondly**, where a consumer is manipulated by a third party impersonating the PSP through such a communication channel, and that deception results in one or more fraudulent authorized payment transactions, the PSP must reimburse the full amount of the transaction, provided that the consumer notifies the PSP without undue delay and reports the fraud to the competent law-enforcement authorities.

The reimbursement right is deliberately framed through cumulative conditions. It is not sufficient that the fraudster merely claims to represent the PSP. Rather, the deception must be carried out through a communication channel attributed to the PSP itself, such as a spoofed caller identification, an existing bank SMS conversation or an email appearing to originate from the PSP's domain. The victim must also qualify as a consumer, namely a natural person acting outside their trade, business or profession. Only where these conditions are satisfied does Article 59 confer a harmonized right to reimbursement, subject to the additional procedural requirements discussed below.

> *Within 15 business days of being notified and provided with the police report by the consumer, the payment service provider shall … refund the consumer the amount of the fraudulent authorised payment transaction*

> *… [or] provide a justification for refusing the refund.*
>
> **PSR Art. 59(2) (published text, doc 8221/26)**

The reimbursement period commences only after both statutory preconditions have been fulfilled: notification to the PSP and submission of a police report. Within fifteen business days, the PSP must either reimburse the consumer in full or provide a reasoned refusal. Such refusal is permitted only where the PSP possesses objectively justified grounds to suspect that the consumer acted fraudulently or with gross negligence. Importantly, the burden of establishing those circumstances rests with the PSP.

The narrow scope of Article 59 reflects a deliberate legislative choice. During the preparation of the PSR, the European Commission examined the possibility of extending reimbursement to all authorized fraudulent transactions but ultimately concluded that such a solution would be disproportionate. A general reversal of liability would have transferred a substantial proportion of APP fraud losses to PSPs, potentially conflicted with the principle of payment irrevocability and created significant moral-hazard concerns by reducing incentives for payment service users to exercise appropriate caution. The legislative compromise therefore retained a targeted reimbursement mechanism for a particularly serious form of deception in which the PSP's own identity and communication channels become the instrument of the fraud.

The Impact Assessment supporting the Commission's proposal demonstrates that this policy choice was grounded in practical experience rather than theoretical considerations. Four major Dutch banks had already introduced voluntary reimbursement schemes for victims of impersonation fraud, reimbursing approximately €51 million during 2022, representing around 89% of reported losses. Extrapolating those figures to the Union level suggested that similar reimbursement mechanisms could involve costs approaching €1 billion annually. Consultations with Member States similarly demonstrated broad support for strengthening preventive measures – including Verification of Payee, transaction monitoring and fraud-information sharing – while expressing considerably greater caution regarding a comprehensive reversal of liability for all authorized payment fraud. Viewed in that legislative context, Article 59 represents a negotiated balance between competing policy objectives: strengthening consumer protection without transforming PSPs into universal insurers against every authorized payment scam[4]

This legislative compromise should not, however, be understood as exhausting the PSR's approach to authorized fraud. Article 59 establishes the express harmonized reimbursement mechanism for impersonation fraud, but the Regulation simultaneously links liability to compliance with a wider range of mandatory fraud-prevention obligations.

> *Where payment service providers fail to comply with Article 50 [Verification of Payee], and where that failure results in a defectively executed payment transaction, the payer's payment service provider shall without delay refund the payer the amount transferred and, where applicable, restore the debited payment account …*
>
> **PSR Art. 57 (published text, doc 8221/26)**

> *Where the payer's payment service provider does not provide evidence to the payer that such monitoring … has been carried out by both providers, it shall refund the payer the amount of the transaction.*
>
> **PSR Art. 83 (published text, doc 8221/26)**

Verification of Payee, transaction monitoring, fraud intervention, information-sharing duties and the allocation of recourse between payment service providers all contribute to the overall liability architecture. Consequently, while Article 59 currently constitutes the principal harmonized reimbursement regime for authorized fraud, other authorized push payment scenarios may also engage liability where the statutory conditions governing those preventive obligations are satisfied or where failures to comply with them contribute to the resulting loss.

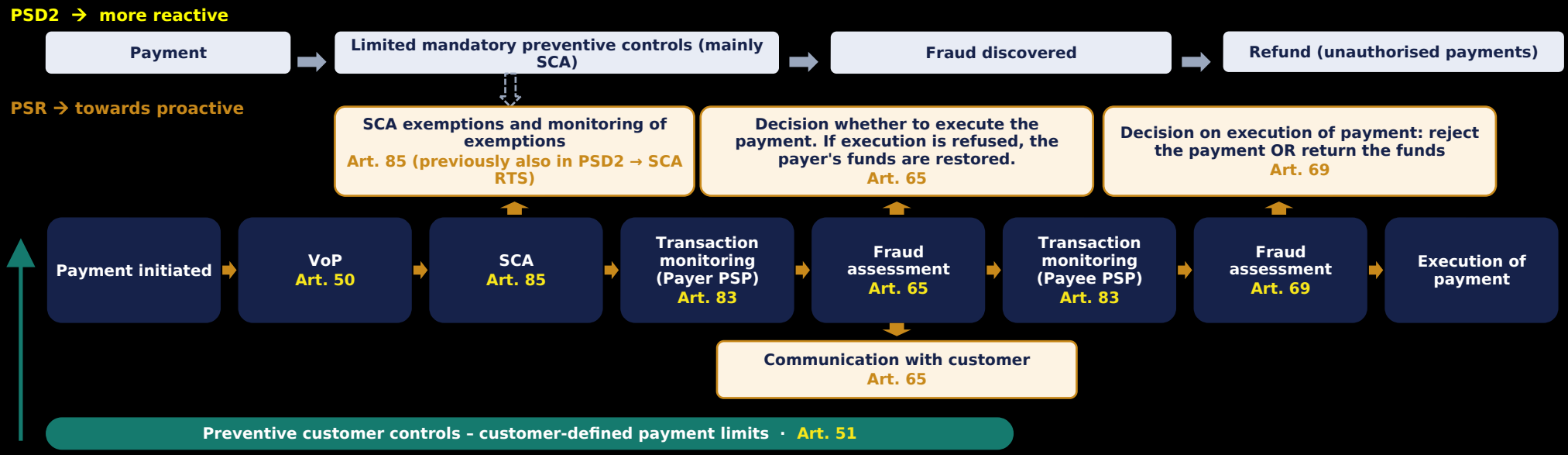
Liability under the PSR is therefore no longer determined solely by the traditional distinction between authorized and unauthorized payment transactions. The Regulation increasingly allocates responsibility according to whether payment service providers complied with their statutory fraud-prevention duties

[4] European Commission, Impact Assessment accompanying the proposals for a Payment Services Regulation and a recast Payment Services Directive (PSD3), SWD(2023) 231 final, 28 June 2023, p. 39 (Netherlands reimbursement of €51 million in 2022 scaled to EU level) and p. 82 (Commission Expert Group on Banking, Payments and Insurance, sessions of 16 and 21 March 2023).

throughout the payment lifecycle. That approach is reinforced by the right of recourse established in Article 78, under which a PSP that has reimbursed a payer may recover its losses from another PSP or intermediary whose failure contributed to the liability. Article 78 further extends that mechanism to certain hosting service providers whose failure to comply with their obligations under the Digital Services Act facilitates fraudulent payment transactions. The allocation of responsibility between institutions becomes largely invisible to the customer, who receives reimbursement from their PSP while responsibility is subsequently redistributed within the payment ecosystem.

4 Fraud prevention – from siloed towards ecosystem

WHY IT MATTERS *Fraud prevention now spans the whole payment lifecycle, and fraud and AML controls draw on the same operational levers – so the two functions can no longer be run as strangers.*



The PSR embeds fraud prevention across every stage of the payment lifecycle, right up to the decision to execute.

Each control point – VoP, SCA, monitoring, fraud assessment, decision to suspend transaction, communication with customer and decision to execute transaction, payee-PSP monitoring, fraud assessment and decision to execute transaction – carries its own statutory obligations, liability and evidential burden in the case of reimbursement.
*Customer-defined payment limits (**Art. 51**) are the **earliest statutory fraud-prevention measure** – active from the start of the customer relationship.*

Figure 5. The fraud journey – PSD2 reactive vs PSR proactive lifecycle, with control points

The second major shift concerns the architecture of fraud prevention itself. Under PSD2, the regulatory framework was centered primarily on the security of payment initiation, with Strong Customer Authentication (SCA) serving as the principal preventive safeguard. The PSR retains both SCA and the protection afforded in cases of unauthorized transactions, but places authentication within a considerably broader sequence of preventive measures operating before, during and, in certain circumstances, immediately after payment execution. Importantly, failures within this broader fraud-prevention framework may carry their own liability and reimbursement consequences. Fraud prevention thereby becomes less dependent on a single control or a single PSP and increasingly operates as a continuous process across the payment lifecycle.

The Commission's Impact Assessment helps explain the rationale for this change. Its starting point was not that SCA had failed, but rather that the fraud problem had evolved beyond what authentication alone could address. The

Commission therefore rejected both regulatory inaction and a blanket transfer of all social-engineering fraud losses to PSPs. Instead, its preferred package combined several complementary interventions: greater use of SCA, IBAN/name verification, a legal basis for PSP-to-PSP fraud-information sharing and targeted changes to liability. The significance of that choice is structural. Fraud prevention was no longer conceived as a problem capable of being addressed by strengthening a single authentication control; different vulnerabilities required different controls at different stages of the payment process[5].

Prevention may begin even before an individual payment is initiated. Article 51 enables payment service users to set payment transaction limits, agreed in the framework contract, and to modify those limits subsequently. A remote increase of the limits is itself subject to SCA, and the final text adds a cool-off dimension on top of authentication: an increase requested by the payment service user does not take effect immediately, but only after a waiting period during which the previous, lower limit continues to apply. The design borrows from Dutch market practice, where limit increases become effective only after four hours, and its purpose is behavioral rather than technical – a customer being coached in real time by a fraudster cannot raise their own ceiling and pay within the same session. Payment limits perform a different function from transaction monitoring: they do not identify fraud but constrain the amount that can be transferred before fraud detection or intervention becomes relevant. They may therefore operate as an ex ante limitation of potential loss. At the same time, changes to established limits may themselves become relevant to fraud monitoring where, together with other information, they depart from the customer's normal behavioral characteristics.

Once a credit transfer is initiated, Verification of Payee (VoP) provides another preventive layer by testing whether the payment account identifier and the information identifying the intended payee correspond. This safeguard is not introduced into Union law for the first time by the PSR. It was already established by Article 5c of Regulation (EU) No 260/2012 (the SEPA Regulation), as inserted by Regulation (EU) 2024/886 on credit transfers in euro, which requires the payer's PSP to provide a service ensuring verification of the payee before the payer is offered the possibility of authorizing the credit transfer. The PSR incorporates VoP into the broader payment-services and fraud-prevention architecture. Its function is particularly relevant where a payer is induced to direct an otherwise authorised payment to an account other than that of the intended recipient. VoP therefore addresses a vulnerability that authentication cannot resolve: SCA can establish that it is the payer who authenticates the transaction, but cannot by itself establish that the payment is being directed to the person whom the payer intends to pay.

The Commission's Impact Assessment provides useful empirical support for the policy rationale, although the evidence available to the Commission at the time largely concerned national implementations rather than experience with a Union-wide VoP regime. The Commission regarded the extension of IBAN/name verification as one of the most effective fraud-prevention measures considered and relied particularly on experience from the Netherlands and the United Kingdom. According to the Dutch provider cited in the Impact Assessment, introduction of the IBAN/name check in 2017 was followed by an 81% reduction in invoice fraud/scams and a 67% reduction in payments misdirected as a result of payer error. The Commission considered that these results demonstrated significant potential for reducing APP fraud losses and supported extending payee verification more broadly across credit transfers[6].

SCA under Article 85 nevertheless remains the authentication layer within this wider architecture. Importantly, the PSR expressly connects SCA with transaction monitoring. Article 83 requires transaction-monitoring mechanisms to support the application of SCA and, under specified risk-based conditions, its exemptions. Monitoring might be therefore not merely an ex post fraud-detection function. It supplies the risk assessment on which decisions concerning authentication and the treatment of a transaction may depend. This connection is not new: Commission Delegated Regulation (EU) 2018/389 on regulatory technical standards for strong customer authentication and common and secure open standards of communication (SCA RTS) under PSD2 already requires transaction-monitoring mechanisms capable of detecting unauthorized or fraudulent payment transactions and expressly relies on transaction monitoring and real-time risk analysis for the transaction risk analysis exemption from SCA.

[5] European Commission, Impact Assessment accompanying the proposals for a Payment Services Regulation and a recast Payment Services Directive (PSD3), SWD(2023) 231 final, 28 June 2023, section 6.1(a)–(e) (considering complementary measures concerning the application of SCA, PSP-to-PSP fraud-information sharing, IBAN/name verification and liability for fraudulent authorised transactions), and section 7.4 (selecting options 1a, 1b, 1c and 1e as the preferred anti-fraud package).

[4] European Commission, *Impact Assessment accompanying the proposals for a Payment Services Regulation and a recast Payment Services Directive (PSD3)*, SWD(2023) 231 final, 28 June 2023, **section 6.1(c)**

The monitoring obligation is itself considerably broader than it was under the SCA RTS under PSD2. Article 83 requires PSPs to maintain transaction-monitoring mechanisms capable of supporting SCA and of preventing and detecting potentially fraudulent payment transactions. Importantly, monitoring is required on both sides of the transaction: the payer's PSP must carry it out prior to execution, while the payee's PSP must do so before making the funds available to the payee. Failure to perform the required monitoring may itself give rise to liability and reimbursement consequences.

The Regulation specifies both the categories of data that may be processed and the minimum risk-based factors that those mechanisms must take into account. A more detailed mapping of Article 83 requirements to transaction-monitoring capabilities, including a practical vendor-assessment checklist, is provided in the Box below, however one aspect should be brought forward – monitoring framework is not limited to information generated internally by the PSP… Information received through fraud-information-sharing arrangements is expressly included among the data that may be processed, insofar as necessary, by both payer and payee PSPs. Fraud intelligence therefore becomes an input into the monitoring process, alongside customer, account, transaction, session and device data. The purpose of monitoring is consequently not simply to generate fraud alerts, but to combine relevant internal and external information into a risk-based assessment upon which the PSP can determine whether further intervention is required.

The Level 1 requirements are, however, not the end of the regulatory specification. Article 89 requires the EBA to develop draft regulatory technical standards specifying the technical requirements for the transaction-monitoring mechanisms and submit those draft RTS to the Commission within one year after the PSR enters into force (as of the final PSR text known to the date of this paper). Thus important elements of its technical implementation remain to be revealed later.

BOX No. 1: CHECKLIST FOR ASSESSING THE FRAUD PREVENTION VENDOR, ITEM BY ITEM

Fraud monitoring is not new to payment-services regulation. Under PSD2, the SCA RTS already required PSPs to maintain transaction-monitoring mechanisms capable of detecting unauthorised or fraudulent payment transactions and linked real-time transaction risk analysis to certain SCA exemptions. The PSR builds on that framework rather than replacing it. Article 83 brings transaction monitoring into the Regulation itself and gives it a broader role within fraud prevention: supporting SCA, preventing and detecting potentially fraudulent transactions, and informing further intervention where necessary.

The PSR also provides more detail on what monitoring should consider. Article 83 specifies categories of data that may be processed, including information received through fraud-information-sharing arrangements, as well as minimum risk factors to be taken into account. This makes the Level 1 requirements relatively easy to translate into practical monitoring capabilities. The tables below use these requirements as a regulatory baseline and illustrate how they can be mapped against the functionality of a transaction-monitoring solution, including as a practical checklist when assessing a potential vendor.

A · WHAT MUST BE PROCESSED

Fraud-data the PSR requires to be processed by payer PSP	PSR basis	YOUR VENDOR
PAYER DATA LINKED TO USE OF SECURITY CREDENTIALS		
Environmental characteristics	✓ Art. 83(2)(a)	
Behavioral characteristics	✓ Art. 83(2)(a)	
INFORMATION ON PAYER LINKED TO ACCOUNT AND TRANSACTION DATA		
Account information (not further specified)	✓ Art. 83(2)(b)	
Transaction data: history, amount, payment instrument, currency, date and time of execution, payee identifier	✓ Art. 83(2)(b), (c)	
Session data: device IP address-range (access to payment account and initiation of transaction)	✓ Art. 83(2)(d)	
Device data: identifiers of the initiating transaction	✓ Art. 83(2)(e)	
Payee data: unique identifier of the payee	✓ Art. 83(2)(ea)	
Information received through the fraud-information-sharing arrangements	✓ Art. 83(2)(eb)	

Fraud-data the PSR requires to be processed by payee PSP	PSR basis	YOUR VENDOR
INFORMATION ON PAYEE LINKED TO TRANSACTION AND ACCOUNT DATA		
Account information (not further specified)	✓ Art. 83(2a)(b)	
Transaction data: history, amount, payment instrument, currency, date and time of execution, name of the payer	✓ Art. 83(2a)(b), (c)	
Information on the payee (not further specified)	✓ Art. 83(2a)(a)	
Information received through the fraud-information-sharing arrangements	✓ Art. 83(2a)(aa)	

B · WHAT MUST BE ASSESSED

Risk-based factor the PSR requires to be assessed	PSR basis	YOUR VENDOR
AUTHENTICATION COMPROMISE		
Lists of compromised or stolen authentication elements	✓ Art. 83(2b)(a)	
TRANSACTION CHARACTERISTICS		
Transaction amount	✓ Art. 83(2b)(b)	
BEHAVIOURAL INDICATORS		
Abnormal spending or behavioral pattern of the payer	(✓) Art. 83(2)(a)	
Abnormal location of the payer	(✓) Art. 83(2)(a)	
TECHNICAL COMPROMISE & THREAT INTELLIGENCE		
Known fraud scenarios in the provision of payment services	✓ Art. 83(2b)(c)	
Signs of malware infection in the authentication procedure	✓ Art. 83(2b)(d)	
Log of use, and abnormal use, of a PSP-provided access device or software	✓ Art. 83(2b)(e)	

Legend: ✓ explicit requirement · (✓) concept preserved through broader wording · VENDOR coverage: ✓ covered · (✓) partial · - not covered

Read together, those lists describe a control that is data-hungry in a very particular way. Most of the categories in Article 83(2) already sit inside a PSP's own transaction, session and device records. One does not: information received through the fraud-information-sharing arrangements has to be ingested from outside the institution, reconciled with internal customer data and made available to the same scoring engine. he effectiveness of monitoring therefore depends not only on the availability of data, but also on the PSP's ability to connect transaction-level information with relevant fraud intelligence.

The significance of that connection is particularly apparent in relation to "known fraud scenarios", which Article 83 identifies as a minimum risk factor. Such scenarios need not be limited to static rules derived from the PSP's own historical fraud cases. Information received from other PSPs about emerging fraud patterns, relevant identifiers or modus operandi may contribute to the PSP's understanding of a fraud scenario and subsequently inform its monitoring. The Regulation does not prescribe how individual pieces of shared intelligence must be translated into monitoring rules, indicators or risk scores; this remains part of the PSP's operational implementation and may be further informed by the forthcoming technical standards.

The other risk factors similarly require different levels of contextual analysis. Some – such as compromised authentication elements, transaction amount or use of a PSP-provided device – may be assessed relatively directly against the transaction concerned. Others require comparison with information accumulated over time or obtained from elsewhere in the payment ecosystem. Identifying abnormal behaviour, for example, requires an understanding of the customer's established patterns, while information concerning emerging fraud scenarios may depend on intelligence extending beyond the PSP's own experience. This is where the connection between transaction monitoring and fraud-information sharing might become operationally significant: information sharing expands the pool of fraud intelligence available to PSPs.

Monitoring itself, however, does not determine the ultimate treatment of the payment. It produces the risk assessment on which further action may be based. Whether a transaction proceeds, is refused, or – where the relevant conditions are met – funds are returned is governed by the separate intervention provisions considered next.

Distinction between monitoring and intervention remains important operationally. A transaction-monitoring mechanism need not itself be the system that ultimately executes, rejects or returns a payment. Its regulatory function can instead be understood as detecting and assessing relevant fraud indicators and communicating the outcome to the systems or functions responsible for the payment decision. The subsequent legal action may then differ according to the stage of the payment and the PSP involved.

For the payer's PSP, Article 65 introduces the possibility of intervention before execution where fraud is suspected on the basis of transaction monitoring and other relevant information. The PSP may therefore interrupt the ordinary payment flow while the circumstances are assessed and, where the statutory conditions are met, refuse execution. The provision also regulates communication with the payment service user and the outcomes of that communication.

Crucially, the preventive chain does not end when the payment leaves the payer's PSP. Article 83 extends transaction-monitoring responsibilities to the payee's PSP, while Article 69 creates a separate intervention point on the receiving side. Depending on the circumstances and the stage reached by the transaction, the relevant outcome may involve refusal to make funds available or the return of funds to the payer's PSP. This becomes particularly significant in an instant-payment environment. Once funds can move within seconds, prevention cannot depend exclusively upon the sending institution identifying fraud before execution; the receiving PSP may represent the next point at which the movement of suspected fraudulent funds can still be interrupted.

The resulting structure is therefore a chain of preventive controls rather than a single fraud-monitoring obligation. Payment limits constrain exposure; VoP tests the intended recipient; SCA authenticates the payer; transaction monitoring evaluates fraud risk; the payer's PSP may intervene before execution; and monitoring and intervention continue on the

payee side as the transaction progresses. These controls perform different functions and should not be conflated. Their regulatory significance lies precisely in their interaction.

This is also where the Commission's Impact Assessment helps explain the broader shift from siloed prevention towards an ecosystem model. The preferred policy response deliberately combined controls that operate at different points and depend upon different information: authentication, payee verification, fraud-information exchange and targeted liability consequences. Significantly, the Commission rejected a blanket rule making PSPs liable for all fraudulent payments caused by social engineering, considering such an approach excessively costly or disruptive relative to its expected benefits. The regulatory response was therefore not simply to move fraud losses from customers to banks, but to strengthen the preventive architecture and alter incentives selectively where prevention could realistically be improved.

5 AML and Fraud convergence within payment service regulation

WHY IT MATTERS *The PSR and the AMLR now reach for the same lever – hold the payment – but point it at opposite outcomes: one restores the payer, the other preserves the assets for the authorities. Reading the two regimes as one control, or confusing which has been triggered, is where liability now sits.*

The PSR brings fraud prevention and AML closer together within payment-services regulation. This is not because fraud has suddenly become relevant to AML: fraud has long been capable of generating criminal proceeds and therefore forming the predicate criminal activity from which money laundering follows. What is changing is the perspective of payment-services regulation. Historically, fraud prevention and AML often approached different stages and different sides of the same financial-crime event through separate regulatory mandates, systems and governance structures. Fraud controls were primarily concerned with preventing fraudulent payments and protecting the victim from loss; AML controls focused on identifying suspicious activity, the movement of criminal proceeds and the customer or counterparty presenting money-laundering risk.

The two functions have also developed different operating models, although the distinction is more historical than inherent in their regulatory objectives. Fraud operations – particularly in card payments – were pushed relatively early towards continuous monitoring and rapid intervention by real-time authorisation processes, payment-scheme fraud controls and the immediate financial consequences of fraudulent transactions (pushing fraud prevention teams to work on a nearly 24/7 operational basis). AML transaction monitoring, by contrast, historically developed with a stronger emphasis on identifying patterns across transactions, investigating customer context and determining whether suspicious activity should be reported. This does not make AML inherently retrospective: AML obligations can also require immediate intervention before a transaction is executed. Rather, the two disciplines evolved with different operational rhythms and system architectures, even though both may ultimately need to act on the same transaction in real time.

The difficulty arises where those historically separate processes attach different significance to the same activity. A fraud assessment may resolve the immediate question that triggered intervention without exhausting the relevance of the underlying transaction data for AML purposes. Conversely, information available through AML controls may materially change the fraud assessment while there is still an opportunity to intervene. The same payment may therefore need to move between – or be assessed simultaneously through – both control frameworks rather than disappear from one simply because that function has closed its alert.

ILLUSTRATION · ONE SET OF FACTS, TWO QUESTIONS

Consider a customer who normally makes modest domestic payments but suddenly begins moving most of the account balance through a series of new beneficiaries on a Saturday evening. Fraud controls intervene because the activity may indicate either an account takeover or a customer being manipulated into making the payments. The customer responds promptly, successfully authenticates, confirms that the payment instructions are their own and, through further interaction with the PSP, provides information sufficient to dispel the immediate indicators of a scam. From the fraud perspective, the two immediate questions – “is this really our customer?” and “is the customer being deceived into making the payment?” – have therefore been addressed, and the fraud restriction may be lifted.

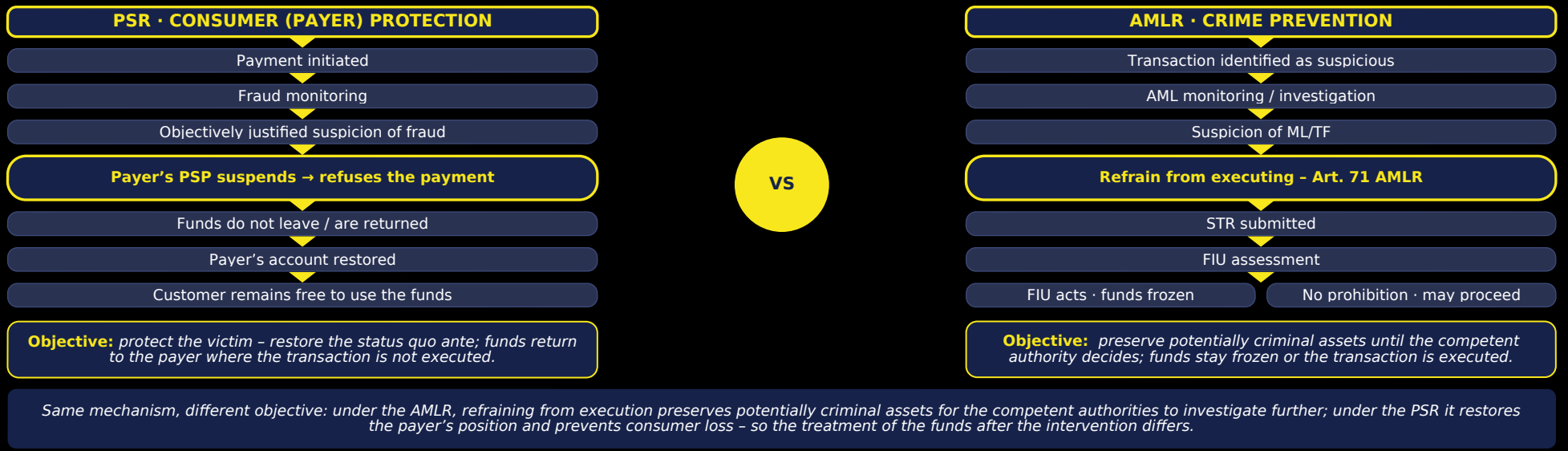
Yet the same activity may raise a different question when viewed through an AML lens. Suppose that the transfers continue over the weekend, involving several newly added beneficiaries and a pattern that departs substantially from the customer's historical activity. Assessed cumulatively rather than as a series of individually authenticated payments, the relevant question is no longer whether the customer is genuinely making the payments or has been deceived into doing so. It becomes “why is the customer moving funds in this manner, what is their source and destination, and could the account be being used in connection with criminal activity?” The information obtained through the fraud intervention remains relevant, but satisfactory answers to the fraud questions do not necessarily answer the AML question.

This illustrates a practical weakness in treating fraud and AML as sequential or isolated controls. A fraud alert may contain information relevant to AML even where the immediate fraud suspicion is resolved; conversely, AML intelligence concerning a beneficiary, account or transaction pattern may be highly relevant

to a fraud decision that has to be made within seconds. The issue is therefore not that one team has failed while another subsequently identifies the “correct” risk. The same transaction can legitimately produce different assessments because fraud and AML controls address different risks, operate on different evidential horizons and may require action at different speeds. The operational challenge is ensuring that resolution of one risk hypothesis does not cause information relevant to the other to disappear with the closed alert.

The PSR makes that relationship considerably more explicit. Fraud risk assessment is built around transaction monitoring under Article 83, while the payer's PSP is given mechanisms for intervention where fraud is suspected under Article 65. Fraud intelligence can also move beyond the institution that originally identified it through the information-sharing arrangements under Article 83a, allowing information generated elsewhere in the payment ecosystem to contribute to fraud monitoring. The connection becomes particularly important on the receiving side of the payment. Article 69 and Recital 90a address circumstances in which the payee's PSP has objectively justified reasons to suspect that a payment transaction, or series of transactions, credited or to be credited to its account may be the result of fraud. Crucially, the PSR expressly connects the resulting intervention with the PSP's obligation to refrain from executing a suspicious transaction under Article 71 of Regulation (EU) 2024/1624 (the AMLR). Where the relevant conditions are satisfied, the PSR then provides the payment-law mechanism through which funds may be returned to the payer's PSP or an incoming transaction rejected. In cases meeting the higher evidentiary threshold specified by the PSR, that possibility becomes an obligation.

▌ Figure 6. Similar intervention, different objective – PSR (Art. 69) vs AMLR (Art. 71), incl. reject-vs-return

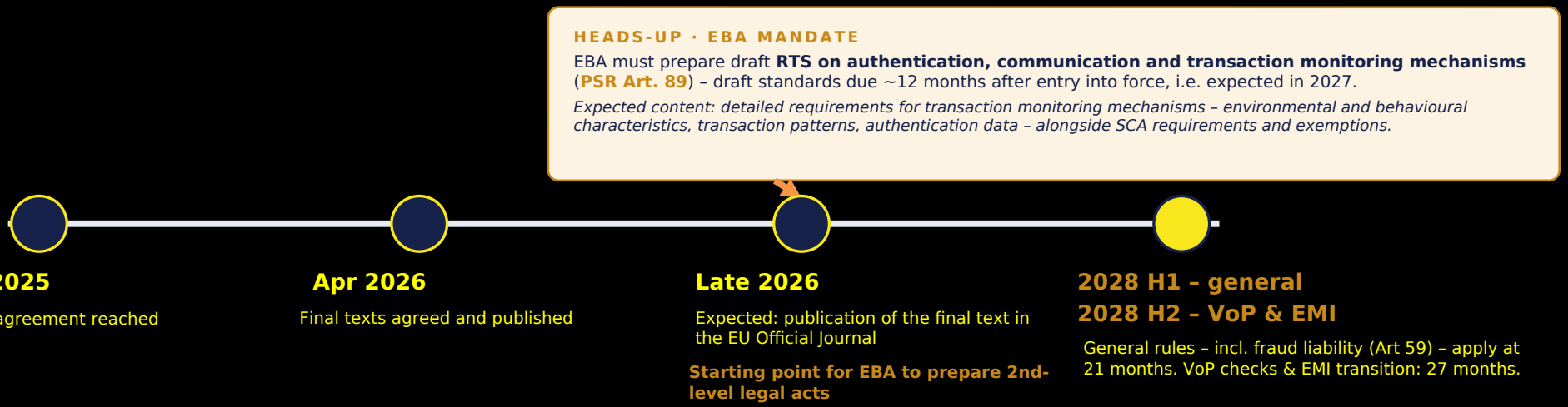


This is an important conceptual bridge. On the payer's side, the immediate regulatory concern may be to prevent the victim from sending a fraudulent payment. Once the funds reach the receiving side, however, the same fraud event also presents the AML problem of criminal proceeds entering and moving through the financial system. The PSR begins to connect those perspectives within the payment lifecycle rather than treating the fraud event as effectively finished once the payment has been executed. The customer-facing dimension adds another point of intersection. Article 84 requires fraud-related communication and awareness measures, while AML rules continue to restrict disclosures that could amount to prohibited tipping-off. PSPs therefore have to reconcile two legitimate regulatory objectives: providing customers with sufficient information to prevent fraud and respond appropriately to fraud risks, while avoiding communications that could prejudice an AML investigation or disclose that suspicious-transaction reporting or analysis is taking place.

The resulting change should therefore not be described as the PSR making fraud a predicate offence for the first time. Fraud and money laundering were already connected under AML law. The more significant development is that payment-services regulation itself increasingly recognizes the operational consequences of that connection. Articles 65, 69, 83 and 83a create a chain running from fraud detection and intelligence to intervention on both sides of the payment, while Article 69 expressly interfaces with the AMLR where suspected fraudulent funds reach the payee side. The two regimes retain different purposes, legal tests and consequences, but they increasingly operate on the same payment and the same underlying financial-crime event.

6 Conclusion: from regulation to implementation

WHY IT MATTERS *The clock is locked even where the detail is not. Waiting for every technical standard before starting means starting late.*



21 months to general applicability – including fraud-liability rules (Art 59 reimbursement). For VoP checks the transition run 6 months longer, to 27 months.

Figure 9. Implementation timeline – from political agreement to 2028 applicability

Source: Amlyze reading of the PSR published text (doc 8221/26) and the source deck; the EBA RTS mandate is Art. 89. Exact applicability dates to be confirmed against the final OJ text

As of the date of this paper, the PSR has not yet been published in the Official Journal. Political agreement was reached in late 2025 and the final compromise text was settled in April 2026. Under that text, the Regulation would generally apply 21 months after its entry into force, while the Verification of Payee requirements in Article 50 and the corresponding liability regime in Article 57 would apply six months later, after 27 months. One of the most consequential pieces of the framework is still to come: under Article 89, the EBA must, within one year of the Regulation's entry into force, submit draft regulatory technical standards covering authentication, communication and the technical requirements for transaction-monitoring mechanisms. In developing them, the EBA must balance security and fraud risk against, among other considerations, user experience, technological neutrality and innovation.

Those dates, however, mark the outer regulatory timetable rather than the starting point for change. National legislators are already moving ahead of the PSR in selected areas. Lithuania, for example, has proposed introducing a range of fraud-prevention requirements, including measures requiring intervention where fraudulently obtained funds reach the payee’s account. The relevant legislation has yet to be drafted, the proposal already signals a clear regulatory direction and intention to act ahead of the PSR timetable. While these measures

do not replicate the PSR architecture in full, they illustrate a broader point: fraud-prevention expectations are already evolving ahead of the PSR application date.

The same is true of supervision. The legal consequences created by the PSR – particularly its new liability and reimbursement rules – cannot simply be applied before they become applicable. But supervisory concern about fraud does not begin with those rules. Competent authorities already possess tools under payment security, governance, operational-risk and AML/CFT frameworks through which they can examine whether an institution understands its fraud exposure and maintains controls appropriate to that risk. This becomes particularly relevant where fraud generates criminal proceeds: the absence of a future PSR liability rule does not remove the existing AML obligation to identify and manage risks associated with criminal activity.

Nor is fraud-information sharing starting from scratch. National arrangements already demonstrate how fraud intelligence can move beyond individual institutions. In the Netherlands, for example, PI-ISAC brings payment institutions together to exchange information and expertise on fraud and related financial-crime threats. Similar national initiatives illustrate the infrastructure on which the PSR's broader information-sharing framework can build: the shift is increasingly from institution-specific detection towards collective fraud intelligence. These developments address a basic limitation of institution-level fraud prevention: each PSP sees only part of the picture, while fraud networks operate across multiple customers, accounts and institutions. Information sharing can fill that gap by bringing external fraud intelligence into the PSP's own monitoring. The practical challenge is therefore to turn shared intelligence quickly into effective detection and intervention.

The same logic applies inside the institution. Fraud and AML need not – and legally should not – be collapsed into a single control. They have different purposes, legal thresholds, escalation routes and restrictions. But maintaining them as disconnected information environments becomes increasingly difficult to justify. A fraud intervention may establish that the genuine customer is making the payment and is not being manipulated, while the same transaction pattern remains relevant to an AML assessment. Conversely, AML intelligence concerning an account, beneficiary or transaction pattern may materially alter a fraud assessment while intervention is still possible. The opportunity is therefore not organisational consolidation for its own sake, but better orchestration: common or interoperable data, appropriate cross-functional escalation, reusable intelligence and governance that ensures information relevant to one financial-crime risk is not lost when another team's alert is closed.

That should also influence technology decisions being made before 2028. Institutions reviewing fraud or AML monitoring platforms have an opportunity to ask a different procurement question. Instead of acquiring another isolated engine designed around a single regulatory workflow, they can assess whether the architecture can support payer- and payee-side monitoring, behavioural and transactional analysis, external fraud intelligence, case management, evidence and decision logging, information sharing and appropriate interaction with AML controls. This does not necessarily mean one vendor or one system for everything. It means avoiding technical architecture that recreates the regulatory silos the PSR is beginning to dismantle.

BOX No. 2: PRACTICAL READINESS CHECK – FRAUD-MONITORING FUNCTIONALITIES AND THEIR REGULATORY BASIS

Illustrative vendor-assessment checklist

The regulatory requirements can also be translated into a practical vendor-assessment exercise. The checklist below provides an illustrative mapping between fraud-monitoring functionalities and their regulatory basis under the PSR. It distinguishes between capabilities expressly required by the regulatory text and those that follow operationally from broader obligations. It should therefore be read as a readiness and procurement tool rather than as an exhaustive statement of minimum legal requirements. Its level of detail is deliberately simple, and deliberately not a functional specification – but it gives a reasonably clear impression of what a PSR-ready monitoring capability is expected to cover.

Fraud-monitoring capability	PSR basis	Vendor capability
Transaction monitoring mechanisms should prevent and detect potentially fraudulent payment transactions		
Real-time (online) monitoring	✓ Art. 83(1b)	
Action logging and evidence storing	(✓) Art. 55, 57, 65, 69, 78	
Transaction risk evaluation and action prioritisation	(✓) Art. 65, 69, 83	
Transaction risk analysis (case management and resolution)	(✓) Art. 65, 69	
Support customer interaction	(✓) Art. 65	

The purpose of such a mapping is not to reduce PSR compliance to a technical box-ticking exercise. A platform may technically contain each individual functionality while still failing to provide an effective fraud-prevention framework if the data, risk assessment, case management and intervention processes do not operate together. The more important question is whether the solution can turn internal and externally received fraud intelligence into timely, explainable and evidenced decisions.

Legend: ✓ explicit requirement · (✓) concept preserved / implied by broader wording . **Vendor capability**: ✓ covered · (✓) partial · - not covered.
Source: PSR published text (Council doc 8221/26).

Effective fraud prevention increasingly depends on fast decisions and access to intelligence beyond a single institution. These capabilities require connected data, calibrated monitoring, information sharing and tested intervention processes; they cannot be created simply by updating policies shortly before the application date.

The PSR should therefore not be seen simply as a compliance project with a 2028 deadline. It changes the architecture of fraud prevention: monitoring extends across both sides of the payment, fraud intelligence moves between institutions, and intervention becomes increasingly connected with evidence and liability. Most importantly from a financial-crime perspective, payment regulation increasingly reflects what AML has long recognised: fraud does not end with the fraudulent payment – once the proceeds reach the receiving side, they may also become a money-laundering concern.

For PSPs, the practical direction is already visible: connect fraud and AML intelligence without confusing their legal purposes; build monitoring capable of using information from outside the institution; preserve evidence from detection through intervention; and participate in the emerging information-sharing ecosystem rather than waiting for it to become a compliance deadline. The runway to the PSR may still appear long. In operational terms, it has already started.

Abbreviations

AML	Anti-money laundering	**AMLR**	Anti-Money Laundering Regulation, Reg. (EU) 2024/1624
APP	Authorised push payment (fraud)	**CFT**	Countering the financing of terrorism
EBA	European Banking Authority	**ECB**	European Central Bank
EMD2	Second E-Money Directive, Dir. 2009/110/EC	**EMI**	Electronic money institution
IBAN	International Bank Account Number	**OJ**	Official Journal of the European Union
PI-ISAC	Payment Institutions Information Sharing and Analysis Centre (Netherlands)	**PSD2 / PSD3**	Second / Third Payment Services Directive
PSP	Payment service provider	**PSR**	Payment Services Regulation
RTS	Regulatory technical standards	**SCA**	Strong customer authentication
VoP	Verification of Payee		

About the author



Eglė Kontautaitė

Head of Client Solutions, AMLYZE

Eglė is an Anti-Money Laundering expert with hands-on experience in customer supervision and money laundering risk management in the context of financial institutions inspections. She has more than 13 years of experience in supervising financial market participants at the Bank of Lithuania, where her last position was Head of the Money Laundering Prevention Division. She represented the Lithuanian delegation during the Moneyval assessment of the country’s AML/CFT framework.