

12 August 2025

# A safe and future-proof digital payments ecosystem: Recommendations for PSR and PSD3 trilogues

## Executive summary

DIGITALEUROPE welcomes the efforts promoted by the co-legislators and the European Commission to promote a safe digital payment ecosystem through the proposed Payment Service Regulation (PSR) and Payment Service Directive 3 (PSD3).<sup>1</sup>

The PSR has the potential to future-proof the payment ecosystem against evolving fraud risks, ensuring robust consumer protection. At the same time, it can empower Payment Service Providers (PSPs) to deliver innovative payment solutions that enhance user experience and trust.

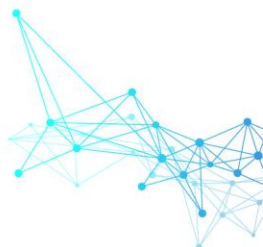
As trilogue negotiations progress, DIGITALEUROPE urges EU co-legislators to adopt the following recommendations:

- ▶ **Fraud:** the PSR should strengthen fraud prevention by establishing clear, objective rules on authorisation, liability, Strong Customer Authentication (SCA), and transaction monitoring, whilst avoiding disproportionate burdens on PSPs. A cross-sectoral, risk-based approach with defined responsibilities for all stakeholders, and a multi-stakeholder platform for fraud prevention, are essential to protect consumers and ensure a secure payments ecosystem.
- ▶ **Regulatory alignment:** the PSR must be consistent with the General Data Protection Regulation (GDPR), the Instant Payments Regulation (IPR), the proposed Framework for Financial Data Access (FIDA) regulation, the Digital Operational Resilience Act (DORA), the Anti-Money Laundering Regulation (AMLR) and the Digital Service Act (DSA).<sup>2</sup>

---

<sup>1</sup> COM/2023/367 final and COM/2023/366 final, respectively.

<sup>2</sup> Regulation (EU) 2016/679, Regulation (EU) 2024/886, COM/2023/360 final, Regulation (EU) 2022/2554, Regulation (EU) 2024/1624 and Regulation (EU) 2022/2065 respectively.



## Table of contents

<b>Executive summary .....</b>	<b>1</b>
<b>Table of contents .....</b>	<b>2</b>
<b>Fraud.....</b>	<b>2</b>
<b>Authorisation .....</b>	<b>2</b>
<b>Impersonation fraud .....</b>	<b>3</b>
<b>Spending limits and cooling off periods .....</b>	<b>3</b>
<b>Transaction monitoring mechanism.....</b>	<b>3</b>
<b>Verification of payee .....</b>	<b>3</b>
<b>Strong Customer Authentication .....</b>	<b>4</b>
Liability of technical service providers and of operators of payment schemes for failure to support the application of SCA.....	4
SCA in respect of payment initiation and account information services .....	4
SCA in respect of credit transfers .....	4
<b>Merchant-Initiated Transactions (MITs).....</b>	<b>5</b>
<b>Multi-stakeholder platform on combatting fraud .....</b>	<b>5</b>
<b>Simplification and regulatory alignment.....</b>	<b>5</b>
<b>PSD3 .....</b>	<b>6</b>
<b>Cash in shop .....</b>	<b>6</b>

## Fraud

### Authorisation

We are concerned with the subjective definition of authorisation proposed by the European Parliament in Art. 3(34a) and its subsequent implications reflected in Art. 55.<sup>3</sup> The PSR should establish a clear and objective definition of authorisation, coupled with a framework for managing customer losses. Introducing subjective elements into the concept of authorisation - such as the Payment Service User's (PSU) claimed lack of intent - risks making payment orders reversible and conditional. This could result in payers' PSPs being obligated to refund transactions based on unverifiable claims. Such an approach would not only create legal and operational uncertainty but could also expose PSPs operating in the EU to substantial financial losses. Moreover, it may incentivise fraudulent claims, enabling bad actors to exploit the regulation by falsely asserting that they did not intend to authorise payments, thereby reclaiming funds to which they are not entitled. In light of these risks, we welcome the incorporation of the objective approach, as reflected in Recital 69 c and Art.55 of the Council's text, and recommend that this version be maintained, provided that these provisions will align with the original objective of the Commission's proposal.<sup>4</sup>

---

<sup>3</sup> A9-0052/2024

<sup>4</sup> Doc. 10268/25



## Impersonation fraud

We support the Council's position in Art. 59, which confines the concept of impersonation fraud to cases involving the user's PSP, and does not extend it to the impersonation of unrelated authorities or third parties. This framework ensures that PSPs are not held liable for fraudulent activities involving entities with whom they have no affiliation or control, thereby preserving legal clarity.

The PSR should also establish clear minimum responsibilities for all stakeholders in the payment ecosystem. Fraud imposes a significant burden on society and demands a comprehensive, cross-sectoral approach that goes beyond the scope of fraud prevention efforts carried out by PSPs. Electronic communications service providers (ECSPs) should have clearly defined obligations to prevent fraud, including verifying calls and messages, preventing fraudulent use of email, and storing identity verification records (e.g. for SIM swaps).

## Spending limits and cooling off periods

We are concerned that imposing limits per payment method and instrument, as currently envisioned by Art. 51 of the Council's text, may result in a proliferation of overlapping thresholds, creating unnecessary complexity and confusion for users. Instead, we recommend that users receive the option to establish a global limit applied at the level of the payment instrument (e.g. card and instant payments). These limits should initially be set by the PSP, with the option for the PSU to lower them if desired. In the event a PSU wishes to increase a limit, a cooling off period should apply. PSPs may choose – but should not be obliged – to offer an opt-out of this cooling off period in their terms and conditions


## Transaction monitoring mechanism


We are concerned that the Council's proposed amendment to Art. 83(2) unduly limits transaction monitoring by the payer's PSP to certain data, excluding payee-related information. In practice, specific characteristics of the payee - such as account age (e.g. newly opened accounts), activity status (e.g. dormant accounts suddenly becoming active), or account type (e.g. business vs. private) - are crucial indicators used during the pre-execution transaction screening stage to assess fraud risk. This approach is already common, proven effective, and fully compliant with the GDPR. Excluding payee data from monitoring would constitute a step backward in the fight against fraud. Therefore, the PSR should explicitly permit the use of relevant payee data in transaction monitoring, supporting rather than restricting proven fraud prevention practices.

## Verification of payee

We support the Council's efforts in Art. 50 and Art. 57 to bring consistency and clarity to the implementation of the Verification of Payee (VoP), by formally incorporating it into the PSR framework. This is a necessary step to resolve the fragmented and inconsistent application of the VoP across Member States. Crucially, the VoP should rely solely on the legal name of legal entities, not on their commercial or trade names. Trade names are not formal identifiers, lack reliable public registries, and are often subject to insufficient validation. The regulation should prioritise verifiable, legally grounded data to ensure effective fraud prevention and legal certainty in payment transactions.

To ensure proportionality and preserve business continuity, the option to opt out of the VoP should be explicitly permitted for single payments, especially for low-value or one-off transactions. Allowing such flexibility would enable businesses to maintain streamlined payment processes in cases where fraud risk is minimal, without undermining the overarching objectives of the regulation.





A targeted exemption from the VoP obligation should be included in the PSR for instant payments initiated through corporate channels that do not support the VoP for technical reasons. Imposing the VoP in such contexts would create excessive complexity without improving fraud prevention. The regulation should take a risk-based, proportionate approach, applying the VoP only where technically and operationally feasible. These changes should also apply to the IPR from the date the PSR takes effect.

## Strong Customer Authentication

We welcome Art. 85 and Art. 89 of the European Parliament's mandate, which instructs the European Banking Authority (EBA) to differentiate between corporate and consumer payers in the revision of the Regulatory Technical Standards (RTS) on SCA. Corporate users often rely on advanced security tools like single sign-on and face different risk profiles than consumers. Tailored rules would reduce unnecessary friction and better support business efficiency and EU competitiveness.

Additionally, we see value in the European Parliament's Art.89(2)(ea), which mandates that the EBA consider the balance between fraud risk and consumer experience in low-value transactions when developing RTS. This approach enables an outcome-based model for SCA and fraud prevention, shifting the focus from strict compliance to achieving defined targets balancing security and user experience, enabling innovation in authentication processes while maintaining strong customer protection.

## Liability of technical service providers and of operators of payment schemes for failure to support the application of SCA


Art. 58 on the liability of Third-Party Service Providers (TSPs) and operators of payment schemes should ensure a fair and proportionate balance. The provision should take into account existing liability frameworks in commercial law, under which TSPs and payment scheme operators already operate through contractual arrangements that define responsibilities and liabilities, including in relation to SCA. Furthermore, the PSR should recognise the complexity of the payment chain, which involves multiple actors beyond TSPs and scheme operators, many of whom contribute to the SCA process but fall outside the control of these entities. In this context, Art. 58 of the PSR should ensure that failure to apply SCA by TSPs and operators of payment schemes results in proportionate compensation.

## SCA in respect of payment initiation and account information services


We express our concerns with the Council's Art. 86(4), mandating the application of SCA by the Account Servicing Payment Service Providers (ASPSPs) only for the first data access when the customer accesses their payment account via an Account Information Service Provider (AISP). This would entail that SCA is conducted between customers and the AISP every 180 days. The additional SCA prevents end-to-end business processes, hampering business continuity and compatibility with existing solutions. We would rather support the European Parliament's mandate, which proposes the deletion of Art. 86(4).

## SCA in respect of credit transfers

With regard to Art. 85 a of the Council's text, we consider the inclusion of Transaction Risk Analysis (TRA) exemptions for credit transfers a welcome step toward ensuring technological neutrality and fostering competition across payment instruments. However, the liability framework must not automatically shift the burden to PSPs - particularly when they do not control the initiation or fraud risk of the transaction. At the same time, PSPs must retain the discretion to apply SCA based on their own risk assessments.







This balanced approach will reinforce legal clarity, promote fairness, and ensure that all actors maintain strong incentives to prevent fraud. The EBA should reflect these principles in the RTS, ensuring sufficient flexibility and annual review to accommodate evolving technologies and market practices, including an assessment and a report that describes the actors in the fraud value chain that are outside of the EBA's supervisory remit.

## Merchant-Initiated Transactions (MITs)

We support the European Parliament's approach in Art. 62(1), which restricts the application of unconditional refund rights solely for direct debit transactions, thereby excluding merchant-initiated transactions (MITs). We believe that unconditional refund rights should not apply where there is clear evidence that the intended good or services have been duly delivered, where delivery of goods or services occurred prior to the consumer's cancellation of a subscription, or where SCA was performed at the time of mandate set up with the mandate terms clearly presented to the user. MITs already provide a high level of consumer protection under existing EU legislation.<sup>5</sup> Extending unconditional refund rights to MITs would significantly increase the risk of first-party fraud, placing disproportionate financial and operation pressure on merchants.

## Multi-stakeholder platform on combatting fraud

We welcome the proposal to establish a multi-stakeholder platform on combatting fraud, as outlined in Art. 83 b of the Council's text. To ensure its effectiveness, we recommend that a set of minimum responsibilities for this platform be enshrined in the regulation. The platform should facilitate real-time cooperation and cross-sectoral data sharing, which are critical for effective monitoring, risk mitigation, and enforcement in the evolving payments ecosystem.

## Simplification and regulatory alignment

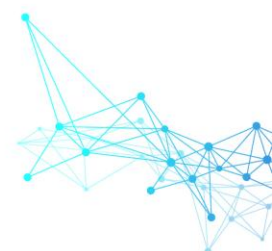
We support the European Parliament's adoption of the term "permission" in place of "explicit consent," as well as the Council's recognition of the applicability of all legal bases under the GDPR. However, to ensure full legal clarity, we recommend that the final text of PSR explicitly state that all legal grounds under Art.6 of the GDPR are valid for the processing of personal data in the context of payment services. Such clarification is essential to ensure legal certainty for payment service providers and to support the lawful, proportionate, and effective use of personal data across diverse operational contexts.

Additionally, permission dashboards under PSR should be aligned with those mandated by FIDA, allowing clients to view and manage their permissions for both frameworks through a single interface.

Existing EU cybersecurity, anti-money laundering and online platforms legislation - such as DORA, AMLR and the DSA – should be fully applicable and leveraged to safeguard against cyber threats and money laundering risks.

---

<sup>5</sup> Art. 76(1) of Directive (EU) 2015/2366 - Payment Service Directive 2 (PSD2) - grants consumers an effective and proportionate right to a refund where a charge exceeds the payer's reasonable expectations. Similarly, Arts 9 - 13(1) of Directive 2011/83/EU - Consumer Rights Directive – entitles consumers the right to withdraw from online contracts within 14 days and receive a full refund.





## PSD3

The clarifications introduced by the European Parliament in Recital 45b of the PSD3 regarding platforms and marketplaces should be maintained. It is important to clarify that marketplaces and platforms which, by design, are supported by PSPs in a way that excludes them from control or possession of user funds, should not be considered agents of the PSP by default. Misclassifying these entities as PSP agents - and thereby subjecting them to extensive compliance obligations - despite their not providing payment services or handling funds, would run counter to the EU's objective of simplifying regulatory requirements. Such an approach risks placing disproportionate burdens on European businesses and would hinder the growth of digital platforms that are not actively involved in payment flows.

The option introduced by the Council in Art. 9(1)(a) of the PSD3, which considers funds held in settlement accounts as safeguarded funds, should also be retained. This clarification is essential to enable PSPs to settle payments efficiently and competitively as direct participants in TARGET, aligning with the policy objective of amending the Settlement Finality Directive (SFD) through the IPR.<sup>6</sup> Treating the funds of electronic money and payment institution clients held in settlement accounts as safeguarded under Art. 9(1) ensures that these institutions can maintain adequate liquidity, thereby supporting the smooth and secure facilitation of payment settlements.

The Council's approach in Art. 43, which mandates a review within one year of the entry into force to assess whether the regulatory framework should be extended to pass-through digital wallets, does not provide sufficient time for the European Commission to conduct a thorough evaluation. A longer review period - such as that originally proposed by the Commission - would allow for a more comprehensive assessment of the evolving payments ecosystem and its interaction with the broader regulatory landscape. This would ensure that any future legislative proposals concerning pass-through digital wallets are evidence-based, proportionate, and aligned with long-term market developments.

## Cash in shop

A "cash-in-shop" model comes with concerns from both a security and competitive standpoint that must be addressed. Unlike payment institutions, retail shops typically lack the robust security infrastructure, operational controls, and risk management procedures necessary for handling cash withdrawals. This disparity could create a new vector for fraud, exposing both consumers and businesses to heightened security risks. Furthermore, enabling such services in shops should not undermine fair competition. Financial institutions have made substantial investments in building and maintaining secure ATM networks as a core component of their service offerings. Cash-in-shop should serve as a complementary channel to ATMs, not a replacement. Setting appropriately low thresholds for cash withdrawals can help mitigate fraud concerns.

---

<sup>6</sup> Directive 98/26/EC



FOR MORE INFORMATION, PLEASE CONTACT:

Federico Di Benedetto

**Manager for Digital Transformation of Financial Services**

[federico.dibenedetto@digitaleurope.org](mailto:federico.dibenedetto@digitaleurope.org) / +32 493 12 34 88

---

Vincenzo Renda

**Director for Digital Transformation Policy**

[vincenzo.renda@digitaleurope.org](mailto:vincenzo.renda@digitaleurope.org) / +32 490 11 42 15

---

Alberto Di Felice

**Policy and Legal Counsel**

[alberto.difelice@digitaleurope.org](mailto:alberto.difelice@digitaleurope.org) / +32 471 99 34 25

## About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations which are global leaders in their field of activity, as well as national trade associations from across Europe.

