



PSD3 & the PSR:

Payments Reform, Fraud Liability and What Firms Should Do Now





At a glance

- In November 2025, the EU's lawmakers reached a provisional political agreement on the Payment Services Directive (PSD3) and the Payment Services Regulation (PSR), followed by publication of final compromise texts in April 2026 and the European Parliament's ECON committee approval in May 2026, bringing the package close to formal adoption
- PSD3 updates and strengthens PSD2 framework¹, reflecting how fraud, payments and technology have evolved.
- Together, PSD3 and the PSR introduce stronger rules on Strong Customer Authentication (SCA), enhanced fraud prevention, data sharing, and open banking.
- The rules apply to a wide range of organisations from banks and payment service providers (PSPs) to technical service providers, online platforms, device manufacturers and open banking providers.
- While the final adoption is expected in the second half of 2026, firms should start preparing now.

¹ In our earlier article, "The 3rd Payment Services Directive is around the corner: Are you ready?", we outlined how PSD2 strengthened payment security through SCA while unintentionally enabling the rise of APP fraud, impersonation scams and ATO frauds. We also summarised the **initial PSD3 key changes** proposed at that time. For readers who would like to revisit that background and the original PSD3 change overview, the full article is available [here](#).

Introduction

In late November 2025, EU legislators reached a landmark political agreement on **PSD3** and the **PSR**. Since then, the legislative process has advanced significantly, with final compromise texts published in April 2026 and approved at committee level in May 2026, signalling that the reforms are now entering their final adoption phase.

This package represents one of the most significant reforms to the EU payments framework since PSD2, driven by accelerating digitalisation, persistent payment fraud risks, and the need for greater regulatory harmonisation across the EU.



Key milestones and implementation overview

While PSD3 and the PSR are not yet in force, the legislative process is now largely complete. The exact implementation timeline will depend on:

- the final publication date,
- the length of transposition periods for PSD3 (as a Directive),
- the application date set for the PSR (as a Regulation).

In practical terms, the next phase involves formal adoption of the final texts by the European Parliament and their publication in the Official Journal of the EU, before they enter into force. Based on the final compromised texts, it is anticipated that:

- PSD3 is expected to have a **21-month transposition period**, giving Member States time to reflect its provisions into national law

- The **PSR** will **apply directly** across the EU, likely **21 months after publication**

On this basis, most obligations introduced by PSD3 and the PSR are expected to take effect during 2028.

Who will be affected?

PSD3 and the PSR introduce obligations that extend beyond traditional payment service providers, affecting every actor involved in providing, supporting, or enabling payment services across the EU. The scope reflects the EU's ambition to create a harmonised, fraud-resistant payments environment.

Entities in scope include:

- **Financial institutions (banks and credit institutions):** harmonised conduct of business requirements and strengthened fraud controls apply across the EU.
- **Payment institutions and e-money institutions:** PSD3 consolidates and strengthens the authorisation/supervisory regime, including bringing e-money activity into the revised framework.
- **Open banking providers (AISPs/ PISPs²):** strengthened rights and rules aimed at reducing obstacles to data access and improving consistency of access.
- **Device manufacturers and electronic service providers:** requirements to provide fair access to device functions/data necessary for payment services on non-discriminatory terms.
- **Merchants and retailers (indirectly):** targeted transparency obligations (e.g., merchant name clarity on statements; fee transparency), plus special provisions for retailers offering limited cash-withdrawal services.

² Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs)

Key requirements of PSD3 and PSR with direct fraud and liability impact

While PSD3 and the PSR will introduce a broad set of new obligations for PSPs, several requirements will stand out because of their direct impact on **fraud prevention, liability exposure and customer protection**. These changes will be particularly relevant for fraud, compliance and operational teams, as they will fundamentally reshape how fraud risks are expected to be prevented, detected and managed.

Heightened liability for impersonation fraud

PSD3 will explicitly clarify PSPs' liability where customers are deceived by fraudsters impersonating their bank or payment service provider. In such cases, PSPs will be required to refund their customers unless they can demonstrate that the customer acted fraudulently or with gross negligence. This will place greater emphasis on:

- Clear definitions of gross negligence,
- Robust investigation procedures and evidence trails, and
- Transparent customer communications where refunds are declined.

Mandatory IBAN-name verification and accountability for failure

PSPs will be required to operate a verification service that matches the unique identifier (e.g., IBAN) with the payee's name and will be liable where failures in this control contribute

to fraud losses. If a discrepancy between the payee's name and the verification service is detected but not properly communicated to the payer, the payer will not bear the resulting financial loss.

In such cases, PSPs will have to, within 10 business days, either refund the full amount of the authorised credit transfer or provide a clear and reasoned justification for refusal, including information on escalation and dispute resolution.

This will make clear that technical implementation alone will be insufficient and that PSPs will need to ensure accuracy, seamless integration into payment flows, and reliable audit trails.

Authentication no longer equals legitimacy

Under PSD3, successful authentication or use of a payment instrument alone will no longer be sufficient proof that a transaction was legitimately authorised or that the customer acted fraudulently or with gross negligence. Where fraud or negligence is alleged, the burden of proof will lie with the PSP. This will increase the importance of behavioural monitoring, transaction logs, authentication data and structured investigation processes, both for customer disputes and supervisory assessments.

Refund timelines and investigation efficiency

Unauthorised transactions will generally require immediate refunding no later than the end of the following business day, unless there are reasonable grounds to suspect customer fraud.

Where such suspicion exists, PSPs will have 10 business days to conclude the investigation and either issue the refund or provide a substantiated refusal. These expectations will place pressure on operational efficiency, decision-making speed and case tracking accuracy.

Transaction monitoring, SCA and information sharing

PSD3 and the PSR will require PSPs to have effective transaction monitoring and fraud-detection systems capable of identifying suspicious activity at an early stage. Transaction monitoring systems will be expected to assess key risk factors such as common fraud scenarios, unusual transaction amounts, compromised or stolen authentication elements, signs of malware, or abnormal use of the device. In addition, PSPs will be required to apply SCA for high-risk actions like adding new payees or changing account limits, helping prevent account takeover and other remote fraud.

To strengthen fraud and scam prevention, PSPs will also be able to participate in information-sharing, for example by exchanging payee identifiers where there is sufficient evidence of fraud. In practice, this means:

- If at least two different customers of the same PSP report that the same payee identifier (e.g., IBAN) was used in fraudulent transactions, the PSP will be permitted to share that payee identifier with other PSPs participating in approved fraud-information-sharing networks.

Such information sharing will help other PSPs identify and block emerging fraud patterns earlier, reducing exposure across the ecosystem.

Fraud governance, awareness and accountability

Finally, PSD3 and PSR will significantly strengthen expectations around fraud governance and organisational accountability. PSPs will be required to maintain incident-management frameworks, conduct regular operational and security risk assessments, report fraud statistics for different payment methods annually to competent authorities and provide mandatory, recurring fraud training to employees.

At the same time, PSPs will be required to actively educate customers on fraud risks and ensure that fraud reporting is simple, accessible and available at all times, including through 24/7 channels tailored to vulnerable and multilingual customer groups. Crucially, PSPs will remain responsible for ensuring compliance across employees, agents and outsourced providers, reinforcing that outsourcing does not reduce regulatory accountability.





What firms should do now?

Although the final text and timelines are still being confirmed, there are several practical actions that firms should already begin preparing for:

- Review and, if needed, uplift their investigations and refund processes to meet the strict next day and 10-day deadlines.
- Verify the reliability of IBAN–name checks, including detection, customer notifications and audit trails.
- Strengthen treatment of impersonation cases through updated scripts, workflows and evidence standards.
- Review and, if needed, upgrade their fraud transaction monitoring systems to identify unusual behaviour, known fraud patterns and malware indicators.
- Ensure consistent application of SCA across all relevant customer journeys.
- Review and, if needed, uplift their current fraud awareness campaigns and the ways customers get alerted to suspected fraud to help users recognise new fraud types and report them quickly.
- Provide regular employee training to improve awareness of fraud risks and operational responsibilities.
- Reinforce incident management and reporting processes, including obligations related to Account Information Service/Payment Initiation Service access issues.
- Review and tighten oversight of outsourced providers, as firms remain fully liable for their actions.
- Align record-keeping and reporting frameworks to meet expanded fraud and operational risk reporting requirements.

How PwC can support you



As firms prepare for PSD3 and the PSR, strengthening fraud capabilities becomes not only a regulatory requirement but a critical enabler of trust, customer protection and operational resilience. The new standards elevate expectations across real-time monitoring, SCA controls, behavioural analytics, investigation quality, and customer communications.

At PwC we have developed a **PSD3/PSR** maturity assessment tool **to diagnose** your current state against the evolving regulatory requirements around payment fraud. The assessment identifies areas of heightened exposure and enables you to proactively strengthen fraud prevention and transaction monitoring capabilities, clarify

liability and refund decision-making, improve investigation speed, and enhance customer communications. It delivers a practical, prioritized roadmap covering customer protection, fraud investigation & dispute handling, refunds & PSP's liability, transaction monitoring, fraud detection, prevention, and reporting & management information. The maturity assessment helps PSPs assess whether their operating model, controls, data and management information are sufficient to support increased requirements and tighter refund timelines under PSD3. If you are interested in discussing the topic of PSD3/PSR and what the requirements of the new legislation will mean for your organisation, feel free to get in touch.

Contacts



Ivana Gerhardová
Fraud Consultant
PwC CEE Financial Crime
ivana.gerhardova@pwc.com



Jeny Rasheva
Fraud Services Lead
PwC CEE Financial Crime
jeny.r.rasheva@pwc.com

Disclaimer: The information contained in this article is for general information purposes only and is provided as of the date of publication. It should not be relied upon as legal advice, nor as a basis for determining how applicable laws or regulations may apply to your organisation. Readers should seek appropriate guidance from their legal or regulatory advisors regarding obligations specific to their business and how to ensure compliance. The authors do not accept any liability for actions taken or not taken based on the contents of this publication.