ACI Worldwide®

Strengthening trust and accountability in European payments: ACI's response to PSD3 and PSR1

Table of contents

Executive summary

ACI Worldwide is a global leader in payments technology, with 50 years of experience shaping the world's most critical payment infrastructures. From card and instant payment rails to fraud management and payments intelligence solutions, we continue to support financial institutions, central banks, and payment providers across Europe and beyond in delivering safe, modern, and accessible digital payments.

We welcome the European Commission's PSD2 review, which includes the third Payment Services Directive (PSD3) and the first Payment Services Regulation (PSR1) frameworks, as a timely and necessary step toward building greater trust, resilience, and innovation across the EU payments ecosystem. As fraud becomes more sophisticated and digital adoption accelerates, the need for coordinated, forward-looking policy has never been more urgent.

This paper identifies three areas where these proposals can be further improved to achieve stronger outcomes. The aim is to reinforce the EU's global leadership in digital payments while protecting consumers, merchants, and financial institutions from the growing threat of financial crime. We hope this contribution will support a constructive dialogue with policymakers, industry stakeholders, and regulators across the region.

I. Encourage real-time fraud intelligence sharing across the ecosystem

The PSD3 and the PSR1 proposals mark an important shift by introducing a General Data Protection Regulation (GDPR)-compliant legal basis for the voluntary sharing of fraud-related data. For the first time, financial institutions across the EU will be able to exchange fraud intelligence legally, laying the groundwork for faster, more collaborative threat detection.

While a legal basis is a vital first step, it will not drive adoption on its own. Without shared infrastructure, regulatory incentives, or clear liability frameworks, the burden falls on individual institutions to act, often at a high cost to them and with interoperability issues.

In some markets, access to fraud intelligence may be shaped by commercial arrangements, which can limit participation and scalability. Yet the rise of "underground" value transfer systems, through which more than £2 billion is laundered annually in the UK, according to HMRC, underscores the urgent need for cross-sector intelligence sharing beyond regulated financial institutions. When commercial terms govern access to fraud signals rather than public-interest outcomes, this can undermine collective resilience, discourage participation, and lead to fragmented defences across the market.

The EU could go further in the current legislative term by turning legal permission into practical protection. Policymakers could mandate banks, telecoms, and other entities to share real-time fraud intelligence systematically. This could begin with central infrastructures and trusted third parties. This would allow institutions of all sizes to access actionable insights without duplicating efforts or compromising user privacy.

In this context, we would like to suggest the following areas of focus for the European Commission in this legislative term:

Promote the sharing of real-time fraud intelligence via central infrastructures

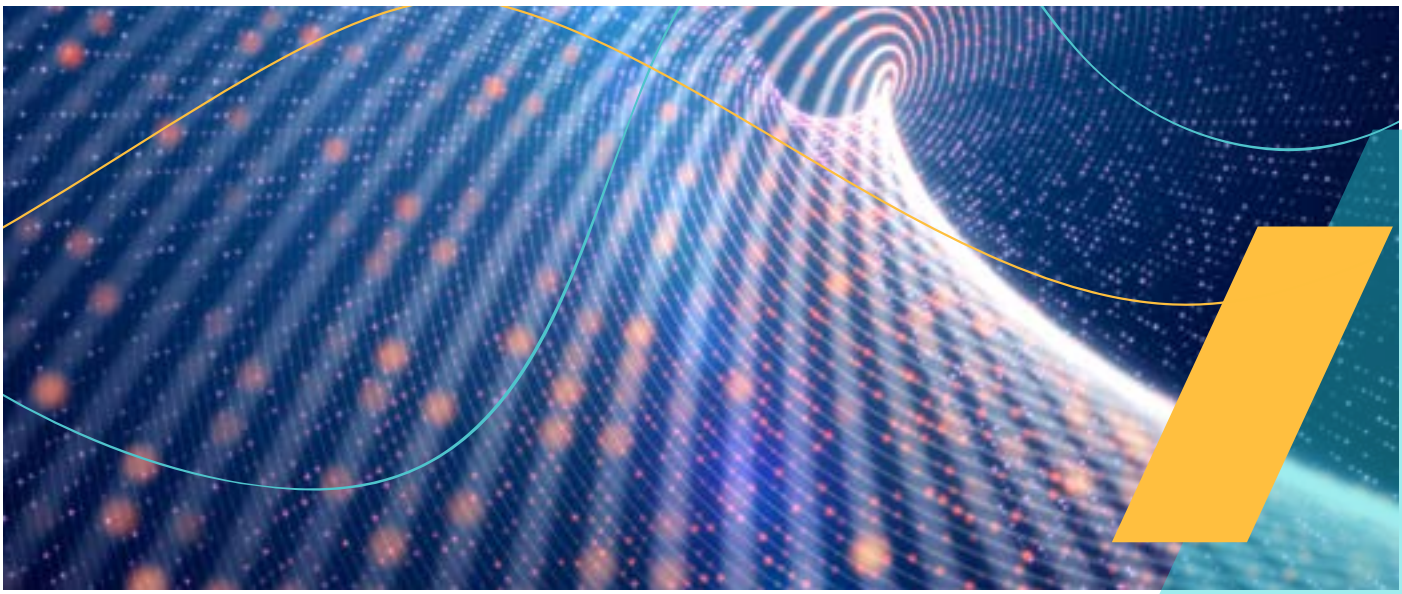
Require central infrastructures to offer fraud data-sharing services on fair, transparent terms, ensuring that institutions of all sizes can access protection. Broaden the range of shared intelligence to include emerging issues, such as spoofed websites, remote access software, and underground banking networks. This strategy helps cross-sector detection and ensures that the system adapts to changing criminal methods.

Clarify ecosystem-wide responsibilities to support collaboration

Define clear obligations and liabilities across banks, payment service providers, vendors, telecoms, and other providers that hold relevant intelligence. Aligning incentives and responsibilities will drive adoption, foster trust, and unlock broader participation in real-time fraud prevention.

Promote privacy-preserving, real-time intelligence models

Establish solutions such as signal sharing, where anonymised data points trigger fraud alerts without exposing personal information. This allows cross-institutional detection while upholding GDPR standards.



II. Position Verification of Payee as a foundational trust layer across the EU

The PSD3 and the PSR1 mark a decisive shift in fraud prevention by mandating Verification of Payee (VoP) for all credit transfers. This requires payment institutions to verify both the IBAN and payee name, free of charge. An expansion of the EU's Instant Payments Regulation, which originally limited such checks to euro-denominated instant transfers, now effectively introduces a pan-European approach to payee verification.

The intent is clear: build trust and reduce fraud in electronic payments. However, implementation across Member States remains uneven, and real-time use of VoP, particularly in cross-border contexts, is far from standardised. Without broader and more consistent implementation, gaps will remain. Fraudsters are increasingly exploiting these inconsistencies, bypassing static checks using spoofing and social engineering. Implementation efforts are further impacted by limited collaboration between sectors, such as telecoms and digital platforms, which often hold critical signals but lack the frameworks or incentives to share them.

Therefore, VoP should not be positioned as a standalone fix but as a gateway to a broader, smarter fraud prevention model—one that builds on cross-industry signal sharing and establishes trusted, interoperable frameworks across all relevant payment types. This aligns with the PSD3's and the PSR1's wider ambition to revitalise open banking, reduce friction, and reinforce trust in digital payments.
This approach also complements the strategic goals of European industry initiatives, such as the European Payments Initiative and its digital wallet, Wero. As new instant payment services are rolled out, consistent, EU-wide identity and verification standards will be critical to their security, adoption, and success.

Consequently, we would like to suggest the following areas of focus for the European Commission in the current legislative term:

Mandate interoperable, real-time VoP across all relevant payment types
Extend VoP obligations beyond SEPA credit transfers to cover digital wallet and app-based payments. Establish a framework of consistent, cross-border coverage, underpinned by standardised technical specifications and shared EU-level directories.

Promote cross-sector collaboration on identity and fraud prevention
Facilitate structured cooperation between payment institutions, telecoms, and digital platforms to enable secure identity verification and early fraud detection. This should include the development of shared standards and protocols for signal sharing.

Establish EU-wide standards for fraud detection and reporting
Mandate certified fraud prevention tools for all payment institutions, with standardised public fraud reporting across Member States to benchmark impact and guide policy.

III. Introduce a more effective liability framework for the digital fraud era

The financial and social impacts of fraud are increasing across Europe, especially with Authorised Push Payment (APP) scams that exploit vulnerabilities in various sectors. ACI's latest Scamscope report forecasts global APP scam losses will hit $7.6 billion by 2028, a sharp rise from current figures. These losses weaken confidence as well as the adoption rates of real-time systems among consumers and merchants alike.

Current solutions risk placing disproportionate responsibility for fraud reimbursements on payment institutions, particularly banks. High-profile cases across the bloc show that this model does little to stop fraud at its source. Instead, it burdens one part of the ecosystem for a problem that starts elsewhere.

APP scams typically start outside the payments infrastructure through social media, spoofed telecoms, or fraudulent online platforms. Banks bear the financial loss, but the platforms enabling the fraud often avoid regulation and consequences. Shared liability is needed to incentivise these actors to improve their fraud defences.

Some EU countries are moving in the right direction. Nordic banks are already investing heavily in advanced tools to detect and prevent scams. In Sweden, where fraud has risen sharply, the Swedish Financial Supervisory Authority has proposed stronger monitoring and a reallocation of liability to drive safer design. Germany, too, is making progress through digital policy and fraud tech, though liability still falls mainly on financial providers.

This imbalance remains a critical gap in the PSD3 and PSR1 proposals, as the focus is still too narrow and centred on reimbursement, rather than addressing the fragmented accountability that allows the likes of APP fraud to flourish.

Europe can pioneer an advanced and equitable liability framework that addresses the origins of fraud. This includes assigning responsibilities and financial accountability to other service providers, platforms, and entities involved in such activities. Additionally, it requires differentiating between various types of fraud, such as first-party refund abuse, to prevent indiscriminate liability for legitimate providers. It is therefore essential that the European Commission continues its important work to protect consumers, merchants, corporations, and banks by building a liability framework that matches today's fraud realities even further.

In this context, we would like to suggest the following areas of focus for the European Commission in the current legislative term:

Introduce a shared liability framework for fraud
Distribute liability more fairly across the payments chain—including banks, telecoms, and digital platforms—to align incentives and drive collective action on fraud prevention.

Mandate EU-wide fraud reporting and intelligence sharing
Encourage Member States to publish fraud loss data annually and share real-time intelligence to help coordinate prevention efforts. Transparency allows for better benchmarking, accountability, and informed policymaking.

Establish fraud education and awareness campaigns
Require coordinated public awareness initiatives led by both public authorities and private sector providers, recognizing that consumer education is a critical and cost-effective defence against social engineering and authorised fraud.

Building a resilient payments ecosystem

At ACI Worldwide, we strongly support the European Commission's ambition to modernise payments regulation through the PSD3 and PSR1. These proposals are a step forward towards a more competitive, innovative, and secure digital finance ecosystem. As instant payments and open banking become the norm, Europe must ensure its regulatory framework is built not only for speed and access but also for trust and resilience.

We believe that now is the time to embed smarter, shared, and scalable approaches to fraud prevention across the payments ecosystem. Europe can lead with a framework that protects consumers, empowers innovation, and sets a global standard for digital trust. ACI Worldwide is prepared to collaborate with policymakers, regulators, and industry experts to help implement this vision.

[i] *AML Intelligence,* £2B per year laundered through 'underground' UK money transfer networks
[ii] *ACI Worldwide,* ACI Worldwide Scamscope Projects APP Scam Losses to Hit $7.6 Billion by 2028
[iii] *Sveriges Riksbank,* Are payments in Sweden safe?
[iv] *Market Data Forecast,* Europe Real-Time Payments Market

As an original innovator in global payments technology, ACI delivers transformative software solutions that power intelligent payments orchestration in real time so banks, billers, and merchants can drive growth while continuously modernizing their payment infrastructures simply and securely. We combine 50 years of trusted payments expertise with our global footprint and a local presence to offer enhanced payment experiences to stay ahead of constantly changing payment challenges and opportunities.

LEARN MORE
www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ATL2120 07-25