EU RegCORE Client Alert

The PSR and PSD3 move forward: What the EU's new payments framework means for regulated firms

April 2026

Financial Services

The PSR and PSD3 move forward: What the EU's new payments framework means for regulated firms

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com

Dr. Jörg Schwerdtfeger
Tel.: +49 160 8839939
joerg.schwerdtfeger@pwc.com

Fabian Joshua Schmidt
Tel.: +49 151 414 904-37
fabian.joshua.schmidt@pwc.com

Contact the EU RegCORE Team
de_regcore@pwc.com

QuickTake

On 23 April 2026, the Council of the EU published an 'I' Item Note (dated 17 April 2026)[1] inviting the Committee of Permanent Representatives (**COREPER**) to approve the final compromise texts of the draft Payment Services Regulation (**PSR**)[2] and the Third Payment Services Directive (**PSD3**)[3], paving the way for a second-reading agreement with the European Parliament. The headline points for regulated firms are summarised below in brief.

- **What.** The PSR and PSD3 will repeal and replace the (second) Payment Services Directive (Directive (EU) 2015/2366) (**PSD2**) and the (second) Electronic Money Directive (Directive 2009/110/EC) (**EMD2**), merging the regulatory regimes for payment services and electronic money into a single, directly applicable conduct-of-business regulation alongside a recast directive on authorisation, prudential supervision and safeguarding.

- **When.** Subject to formal adoption, both instruments will apply 21 months after entry into force, with the mandatory verification of payee (**VoP**)[4] service applying from 27 months and existing EMIs benefitting from a 27-month transitional regime.

- **Who.** The framework will affect credit institutions, payment institutions (**PIs**), electronic money institutions (**EMIs**), account information service providers (**AISPs**), payment initiation service providers (**PISPs**), account servicing payment service providers (**ASPSPs**) and — for the first time — certain technical service providers, electronic communications providers, hosting service providers, mobile device manufacturers and operators of very large online platforms (**VLOPs**) and very large online search engines (**VLOSEs**).

[1] Available here.
[2] Available here.
[3] Available here.
[4] See coverage here.

- **Three biggest changes.** (i) a single, harmonised PI/EMI authorisation and safeguarding regime; (ii) a recalibrated fraud and liability framework, including a dedicated refund right for impersonation ("spoofing") fraud, mandatory transaction monitoring on both payer and payee sides and the new VoP service and strict PSP liability for monitoring/VoP failures; (ii) a single, harmonised PI/EMI authorisation and safeguarding regime, eliminating the separate EMI track; and (iii) a deeper open banking regime with mandatory dedicated interfaces, data parity, a consent dashboard and a non-exhaustive list of prohibited obstacles.

- **Immediate action.** Firms should begin a structured gap analysis covering authorisation conditions, safeguarding arrangements, fraud controls, open banking interfaces, framework contracts and customer disclosures and should track the European Banking Authority (**EBA**)'s forthcoming regulatory and implementing technical standards (**RTS** and **ITS**) - most of which are due within 12 to 18 months of entry into force.

The PSR will be directly applicable in all Member States and will govern the conduct-of-business rules - including transparency, information requirements, the rights and obligations of payment service users (**PSUs**) and payment service providers (**PSPs**), open banking, fraud prevention, strong customer authentication (**SCA**) and enforcement. PSD3 will retain in directive form the rules on authorisation, prudential supervision, safeguarding (i.e. the protection of customer funds from the insolvency of the payment institution holding them) and passporting (i.e. the ability of a firm authorised in its home Member State to provide services across the EEA on the basis of that single licence), which by their nature require transposition into national law. Both instruments will apply 21 months after entry into force, with certain provisions, notably the VoP service, applying from 27 months and existing EMIs benefitting from a transitional regime of up to 27 months as mentioned above.

Together, the PSR and PSD3 will deliver the most far-reaching reform of the EU's payment services framework since PSD2 and EMD2, repealing and replacing both instruments and merging the regulatory regimes for payment services and electronic money into a single, unified framework. This Client Alert, which should be read in conjunction with our earlier alert[5] as well as further coverage from PwC, analyses the Council's final compromise texts of the PSR and PSD3, which remain subject to formal adoption and is current as at the date set out above. Non-EU firms offering in-scope payment services into the European Economic Area (**EEA**) will need to comply with the new framework once it applies.

Legislative timeline to date and what lies ahead

The European Commission first published the Payment Services Package on 28 June 2023, comprising the proposals for the PSR and PSD3. The European Parliament adopted its initial reports on both the PSR and PSD3 proposals in April 2024; following the 2024 European elections, the ECON Committee confirmed its negotiating mandate in late 2024 and opened interinstitutional negotiations.

COREPER agreed on the Council's negotiating mandate in June 2025 and trilogues (i.e. the informal tripartite negotiations between the European Parliament, the Council and the European Commission used to agree the final text of EU legislation) with the European Parliament commenced on 9 July 2025, with the final political trilogue taking place in Strasbourg on 26 November 2025. Numerous technical meetings between the Council Presidency, the European Parliament's ECON Secretariat and the Commission's DG FISMA (i.e. the Directorate-General for Financial Stability, Financial Services and Capital Markets Union) took place in parallel to finalise the compromise texts.

The draft texts were submitted to the Council Working Party on Financial Services on 20 March 2026 for a silent consultation ending on 25 March 2026; no delegation objected to the proposed texts. The 'I' Item Note now suggests that COREPER approve the final compromise texts (doc. 8221/26 for the PSR and doc. 8222/26 for PSD3) with a view to reaching an agreement at second reading with the European Parliament.

Architecture upgrade – from Directive to Regulation

A structural change of fundamental importance is the decision to elevate the conduct-of-business rules governing payment services from an EU directive, which required national transposition and tolerated significant divergence across Member States, to a directly applicable EU regulation. The recitals to the PSR

[5] Available here.

make explicit the rationale: under PSD2, there was significant room for "forum shopping" - i.e. PSPs choosing, as their home country, Member States that applied more advantageous interpretations or less active enforcement of EU payment services rules and then providing cross-border services on a passporting basis into jurisdictions with stricter approaches. The PSR is designed to eliminate this margin for interpretation and to achieve maximum harmonisation of the rules governing the conduct of payment services business.

PSD3, meanwhile, preserves the directive format for the rules on authorisation, supervision and safeguarding of payment institutions. This reflects the fact that those requirements interact with national insolvency law, administrative law and supervisory structures, making full harmonisation through a regulation impracticable at this stage. Nevertheless, the EBA is mandated to develop extensive RTS and ITS to harmonise key aspects of the prudential framework, including the authorisation process, safeguarding risk management, own funds calculation and cross-border supervisory cooperation.

For regulated firms, the practical consequence is significant: conduct-of-business rules will be uniform across the EU from the date of application, with no scope for Member States to gold-plate (i.e. to impose stricter requirements than those required by the EU instrument when transposing it into national law) or diverge. Firms that have relied on favourable national transpositions of PSD2 will need to re-assess their compliance posture against the single PSR text.

PSD2 vs PSR/PSD3 - at a glance

The principal contrasts between the existing and incoming regimes can be summarised as follows:

- **Legal instrument.** PSD2: a directive requiring national transposition. PSR/PSD3: a directly applicable regulation for conduct-of-business rules, plus a recast directive for authorisation, prudential supervision and safeguarding.

- **Scope of regulated entities.** PSD2/EMD2: separate PI and EMI regimes. PSR/PSD3: a single PI regime, with electronic money issuance reclassified as a payment service.

- **Tightened scope and harmonised exclusions.** The PSR will harmonise the interpretation of two exclusions that have generated significant divergence under PSD2: the “commercial agent” exclusion and the “limited network”/”specific-purpose instrument” exclusion. The commercial agent exclusion will only apply where the agent acts on behalf of either the payer or the payee (not both) under a genuine mandate. The limited network exclusion will be narrowed and subject to enhanced notification thresholds and EBA guidelines, with consequential implications for marketplaces, platforms and closed-loop programmes that have relied on a broad reading of these carve-outs.

- **Surcharging.** The PSR will explicitly extend the prohibition on payee surcharging to all credit transfers and direct debits in the EU, resolving the divergence left by inconsistent national transposition of Article 62(4) PSD2.

- **Virtual IBANs.** The PSR will expressly recognise virtual IBANs (**vIBANs**) as valid payment account identifiers and the Commission is mandated to review the risks and benefits of their use within three years of entry into force. Their recognition might have a substantial impact on business models involving centralized payment such as “payment factories”.

- **Open banking.** PSD2: dedicated interface obligation with optional fallback. PSR: mandatory dedicated interface with prohibited obstacles, data parity, consent dashboard and a definitive ban on screen-scraping.

- **SCA.** PSD2: two-factor authentication based on three element categories. PSR: extended scope (mobile activation, accessibility, digital wallet outsourcing) and possible use of two inherence elements subject to demonstrated independence.

- **Fraud and liability.** PSD2: limited PSP liability framework. PSR: recalibrated framework with mandatory transaction monitoring, mandatory VoP, dedicated impersonation-fraud refund right and strict liability for monitoring/VoP failures.

- **Cross-sectoral obligations.** PSD2: confined to PSPs. PSR: extends fraud-prevention and access duties to electronic communications providers, hosting services, mobile device manufacturers and VLOPs/VLOSEs.

- **Enforcement.** PSD2: divergent national approaches. PSR: harmonised minimum sanctions and powers, EBA product intervention powers and a single internal market reference text.

Tightened scope: commercial agent and limited network exclusions

Two of the most heavily exploited PSD2 exclusions are materially narrowed under the PSR. The commercial agent exclusion will, as noted above, only be available where the agent acts on behalf of either the payer or the payee, but not both, under a genuine mandate. This is intended to put an end to the marketplace and platform structures that, on a broad reading of the PSD2 wording, treated themselves as agents for both sides. Marketplaces, ride-hailing platforms and similar intermediaries that have relied on this analysis will need to assess whether their flow of funds requires authorisation as a PI or restructuring through a regulated PSP partner.

The limited network exclusion (also referred to as the "specific-purpose instrument" exclusion – **LNE** or **SPI**) is similarly recalibrated. The PSR narrows the categories of instruments capable of falling within the exclusion, lowers the notification threshold above which providers must notify their competent authority and mandates the EBA to issue guidelines on its uniform application. Closed-loop programmes, including fuel cards/charge cards for electric vehicles, gift cards, employee benefit cards, transit cards and store-branded payment instruments, should review their issuance volumes, redemption networks and product design against the recalibrated tests, with particular attention to cross-Member-State use cases.

These changes, combined with the express recognition of vIBANs as payment account identifiers and the Commission's mandate to review their use within three years, are likely to prompt a wave of regulatory perimeter assessments in the marketplace, embedded finance and platform sectors.

Firms exiting the regulated perimeter as a result of these changes or which are unable to absorb the cost of authorisation typically have three structural alternatives to consider: (i) partnering with a regulated PSP under a sponsorship or BIN-sponsorship arrangement; (ii) operating as a distributor or agent of an authorised EMI or PI within the recalibrated boundaries of those exemptions; or (iii) restructuring the flow of funds so that no payment service is provided in the regulated sense (for example, by routing settlement directly between buyer and seller through a separate regulated channel). Each alternative carries its own contractual, prudential and operational implications and should be assessed against the respective commercial model and growth trajectory.

Merger of the payment institution and electronic money institution frameworks

One of the most structurally consequential changes is the integration of the EMI regime into the PI framework. PSD3 repeals the EMD2 and the issuance of electronic money is reclassified as a payment service listed in Annex I, point (8), of PSD3. Under the new framework, there will be a single category of PI, which may or may not be authorised to issue electronic money, depending on its licence.

Transitional provisions allow existing EMIs to continue their activities for up to 27 months after entry into force of PSD3 without seeking new authorisation. During this period, existing EMIs must submit to their competent authorities all information necessary to demonstrate compliance with the new PSD3 requirements. Competent authorities must assess compliance by the end of the transitional period; EMIs that do not comply will be suspended from providing payment services until they demonstrate compliance. Where competent authorities already have evidence of compliance, automatic authorisation is available.

The merger also extends to prudential requirements. PIs that issue electronic money are subject to a distinct own funds calculation, Method D, requiring own funds of at least 2% of average outstanding electronic money, in addition to the own funds requirements applicable to any other payment services they provide. The initial capital requirement for electronic money issuance is set at EUR 250,000. Electronic money tokens, as a specific category of crypto-asset under the Markets in Crypto-Assets Regulation (Regulation (EU) 2023/1114) (**MiCAR**), are addressed with bespoke provisions, including recognition that certain PSR transparency and execution-time requirements may not be technically feasible where distributed ledger technology (**DLT**) is used.

Territorial scope and third-country firms

Like PSD2, the PSR and PSD3 retain the principle that the provision of payment services within the EEA on a regulated basis requires authorisation as a credit institution, PI or comparable EU-established entity. Neither instrument introduces a third-country equivalence regime nor a recognition mechanism for non-EEA branches

comparable to that available under MiFID II for certain investment services. Non-EEA firms wishing to provide payment services into the Union on a sustained basis will accordingly need to establish, or continue to maintain, an EU-authorised PI (or credit institution) and rely on intra-EEA passporting.

The doctrine of reverse solicitation, while not codified in the PSR, remains narrow under settled EU principles: it permits a non-EEA firm to provide a service to a customer who has approached the firm on the customer's own exclusive initiative, but does not extend to ongoing service relationships, marketing activity or the offering of further or related services. The Commission has indicated that it will continue to monitor reverse-solicitation practices and may revisit the position should evidence of widespread reliance emerge.

For UK PSPs, the position is unchanged in substance: post-Brexit access to the EEA market continues to require an EU-established and authorised entity. Firms operating under temporary permissions or relying on transitional arrangements should ensure that their long-term operating model is consistent with the EU-establishment requirement under PSD3.

UK firms should also have regard to the UK's parallel reform agenda. HM Treasury's Future Regulatory Framework review, the FCA's ongoing safeguarding reforms and the Payment Systems Regulator's authorised push payment (**APP**) fraud reimbursement regime are converging on outcomes broadly comparable to the PSR in some areas (notably APP fraud reimbursement) ahead of it. UK groups serving both markets should map the two reform tracks against each other and consider whether a single, harmonised global operating model is achievable.

Authorisation and prudential framework

PSD3 maintains and harmonises the authorisation process for payment institutions. A three-month decision period applies from receipt of a complete application. The application requirements are comprehensive and include, among other things, a programme of operations, a three-year business plan, evidence of initial capital, a description of safeguarding measures, governance arrangements, ICT security controls aligned with the Digital Operational Resilience Act (Regulation (EU) 2022/2554) (**DORA**), a security policy document with a detailed risk assessment, a description of business continuity arrangements and a winding-up plan.

A streamlined 60-business-day authorisation process is available for crypto-asset service providers already authorised under MiCAR that wish to add payment services involving electronic money tokens.

Conversely, payment institutions authorised under PSD3 will be able to provide certain crypto-asset services in relation to electronic money tokens, such as custody, transfer and exchange, by notification to their competent authority, rather than by seeking a separate MiCAR authorisation. The PSR/PSD3 package specifies the equivalences between the PSD3 and MiCAR authorisation conditions to enable this streamlined route, which is relevant for tokenised payment use cases.

The strategic significance of these PSR/MiCAR equivalences should not be understated: PIs will, in effect, become the single regulated channel for retail-facing electronic money token (**EMT**) issuance, custody and transfer and the framework provides a coherent route for the integration of tokenised payment instruments into existing payment infrastructures. Firms developing tokenised deposit, EMT or wholesale settlement use cases should map their product features and counterparty arrangements against both the PSD3 and MiCAR perimeters at an early stage.

On own funds, Method B, based on payment volume, is the default calculation method. Competent authorities may require Methods A or C for specific business models involving a small number of high-value transactions. The EBA is mandated to develop RTS specifying the criteria for identifying such business models.

By way of brief reference, the four own funds calculation methods carried over (with refinements) from PSD2 measure capital adequacy against different proxies for the firm's payment activity: Method A is a fixed proportion of the firm's previous year's overheads; Method B applies a sliding-scale percentage to total payment volume processed in the previous year; Method C applies sliding-scale percentages to a relevant indicator representing the firm's net income from payment services; and Method D, which is specific to electronic money issuance, requires own funds of at least 2% of average outstanding electronic money. Method B is the default under PSD3, with competent authorities empowered to require Methods A or C where the business model, for example, a small number of high-value transactions, would otherwise produce a misleading capital figure.

By way of indicative illustration: a mid-sized PI processing EUR 2 billion of payment volume annually under Method B would face an own funds requirement of approximately EUR 800,000, calculated by applying the prescribed sliding-scale percentages to the relevant volume bands. The same firm, if also issuing electronic money with average outstanding balances of EUR 50 million, would carry an additional Method D requirement of EUR 1 million. The aggregate own funds requirement EUR 1.8 million would also need to be tested against the firm initial capital floor (EUR 350,000 for Annex I, points (1) to (5) services and EUR 250,000 for electronic money issuance), with the higher figure prevailing. The actual calculation will depend on the EBA RTS on business-model criteria and on competent-authority discretion to require Methods A or C.

Enhanced safeguarding regime

The safeguarding framework is substantially strengthened under PSD3. Payment institutions providing payment services listed in Annex I, points (1) to (5), or point (8), must safeguard all funds received from payment service users (other than electronic money tokens) in one of two ways: (a) by ensuring non-

commingling with their own funds, followed by deposit in a separate account at a credit institution or central bank, or investment in secure, liquid, low-risk assets; or (b) by covering those funds with an insurance policy or comparable guarantee from an insurance company or credit institution not in the same group.

Concentration risk must be avoided - payment institutions shall endeavour not to safeguard all payment service users' funds with a single credit institution. Funds held in settlement accounts with designated payment systems are deemed compliant, provided they are held ultimately at credit institutions or central banks.

Critically, payment institutions must now inform their payment service users, in a clear and transparent manner, how their individual funds are safeguarded, the insolvency law of which Member State is applicable and in which Member State a claim should be raised in the event of insolvency. This transparency obligation must be fulfilled prior to the user entering into an agreement and upon any material change in safeguarding measures.

The EBA is mandated to develop RTS on safeguarding risk management frameworks, including segregation, designation, reconciliation and calculation of safeguarded funds.

Open banking: dedicated interfaces, data parity and content management

The PSR will enhance the open banking framework (i.e. the regulatory regime requiring ASPSPs to share customer payment account data and to enable payment initiation, with authorised third-party providers where the customer has given consent) established under PSD2. ASPSPs will need to maintain at least one dedicated interface, such as an application programming interface (**API**), for data exchange with AISPs and PISPs within three months of obtaining their authorisation. Screen-scraping - i.e. automated access to payment account data through the customer-facing interface using the customer's own credentials, without proper identification of the requesting third party - will be definitively prohibited in all circumstances.

The dedicated interface must use standards issued by European or international standardisation bodies (CEN, ISO, or equivalent). ASPSPs must ensure that response times of the dedicated interface are no longer than those of the customer-facing interface. Quarterly statistics on the availability and performance of dedicated interfaces must be published on the ASPSP's website, with comparison data for the customer interface. A testing facility must be made available to authorised AISPs and PISPs.

The PSR will introduce a principle of data parity: AISPs will receive at least the same information from designated payment accounts and associated transactions as is available to the PSU when directly accessing their account, including pending card transactions visible to the user. PISPs will be able, at a minimum, to initiate single payments, place and revoke standing orders and initiate future-dated and multi-beneficiary payments, as well as verify the name of the account holder before payment initiation.

A non-exhaustive list of prohibited obstacles to open banking is set out in Article 44 PSR. Prohibited conduct includes requiring two SCA authentications in a PIS-only journey, imposing additional steps in the authentication user journey beyond what is offered to the ASPSP's own users and failing to support all authentication procedures available to the PSU.

ASPSPs will provide a consent dashboard, integrated into their user interface, enabling PSUs to monitor, withdraw and re-establish (within 48 hours) data access consents given to AISPs and PISPs. The dashboard must surface granular details of each consent, including its purpose, the categories of data accessed and the dates of access, and must be neutral and free of deterring or discouraging language. AISPs may access account data on a user-consent basis even where the PSU is not actively online, subject to the consent terms surfaced in the dashboard. ASPSPs are expressly prohibited from prompting the user to withdraw consents or designing the dashboard in a way that deceives, manipulates, or directs the user.

Competent authorities may exempt certain ASPSPs from the dedicated interface obligation, allowing them to offer data access via their customer interface (provided it is already an API endpoint), or in certain cases, to offer no open banking interface at all. The EBA will develop RTS on the criteria for such exemptions.

The PSR will introduce a new obligation on mobile device manufacturers, i.e. original equipment manufacturers (**OEMs**), and electronic communications services providers to grant PSPs and electronic money issuers effective, secure and fair, reasonable and non-discriminatory (**FRAND**) access to the device and software features (such as near-field communication (**NFC**) chips, secure elements and biometric authentication interfaces) necessary to process payments. This is intended to support competition in the digital wallet space (i.e. software applications that store payment credentials on a device and enable contactless or in-app payments) and is strategically significant for issuer wallet roadmaps.

Transparency, pricing and access to cash

Changes introduced by the PSR will impact also much more than just online payments:

Access to cash. The PSR will enable merchants to provide cash to consumers without a corresponding purchase, supporting financial inclusion in areas with reduced ATM coverage. ATM operators will also be subject to enhanced charge disclosure requirements and equality-of-treatment rules between cardholders of different PSPs.

Currency conversion and pricing transparency. The PSR will require pre-transaction disclosure of currency conversion mark-ups, expressed both as a monetary amount and as a percentage over an aggregated mid-market reference rate. PSPs and currency conversion service providers will also be prohibited from non-transparent pricing practices, including value dating that operates to the detriment of the PSU.

Security, fraud prevention and enforcement

Strong customer authentication

The PSR preserves and builds upon the SCA framework. SCA continues to be required for online account access, electronic payment initiation and any remote action implying a risk of payment fraud - including the creation or replacement of tokenised payment instruments, changes to spending limits and changes to contact information. SCA remains based on two or more elements drawn from the categories of knowledge (i.e. something the user knows, such as a password or PIN), possession (i.e. something the user holds, such as a card or registered device) and inherence (i.e. something the user is, such as a fingerprint or facial biometric). However, two inherence elements may now be used if the PSP demonstrates to the competent authority that independence of the elements is fully preserved.

Dynamic linking, requiring SCA elements that link the transaction to a specific amount and specific payee, continues to apply for remote payment transactions. SCA exemptions are based on the level of fraud risk, the amount or recurrence of the transaction, the payment channel and whether the payer is a consumer, but are not mandatory, PSPs retain discretion to apply SCA regardless.

The PSR introduces specific provisions on mobile application activation: SCA and the use of different communication channels are required, with a default delay period of four hours before the activation takes effect. The payment service user has the right to adjust or opt out of this delay.

The accessibility of SCA is a significant new compliance dimension. Payment service providers must ensure that SCA does not depend on the exclusive use of a single means of authentication and must not depend, explicitly or implicitly, on possession of a smartphone, unless the user has agreed to exclusively mobile services. Multiple means must be developed to cater for persons with disabilities, older persons and those with low digital skills.

Digital pass-through wallet operators that verify SCA elements must enter into outsourcing agreements with payers' payment service providers, which retain full liability for any SCA failure.

Fraud prevention and the expanded liability framework

The PSR will recalibrate the anti-fraud framework to reflect the evolution of fraud typologies since PSD2, particularly social engineering (i.e. the manipulation of a customer into authorising a transaction or disclosing security credentials, often by impersonating a trusted institution) and impersonation ("spoofing") fraud. Some key aspects include:

- **Transaction monitoring.** Both payer-side and payee-side payment service providers are now required to have transaction monitoring mechanisms in place. The payer's PSP must carry out monitoring prior to execution (in real-time for instant credit transfers) and the payee's PSP must monitor before making funds available to the payee. Where a PSP fails to carry out such monitoring and the transaction was fraudulent, the non-compliant PSP bears full liability; the burden of proof rests with the PSP.

- **Verification of Payee.** A mandatory VoP service will apply for credit transfers. The payer's PSP will verify whether the payee's name matches the unique identifier (IBAN or equivalent) provided and will notify the payer of any mismatch before authorisation. The service must be provided free of charge and within seconds. For instant credit transfers, payer-contact obligations are adapted to fit the 10-second execution window and PSPs must notify counterpart PSPs of any refusal within 10 seconds. Non-consumer PSUs (and micro-enterprises that have opted not to be treated as consumers) may opt out of VoP for automated payment channels. PSP liability for failure to provide or correctly provide VoP is strict: the payer's PSP must refund the full amount of any defective credit transfer resulting from such failure.

- **Liability for unauthorised transactions.** In the case of an unauthorised payment transaction, the payer's PSP must refund the payer immediately and in any event no later than by the end of the following business day, unless the PSP has objectively justified reasons for suspecting fraud or gross negligence by the payer. The payer's maximum liability for losses from loss, theft, or misappropriation of a payment instrument is capped at EUR 50, unless the payer acted fraudulently or with gross negligence. Where the PSP fails to require SCA, the payer bears no financial loss (unless the payer acted fraudulently).

- **Impersonation fraud.** The PSR will create a dedicated refund right for impersonation (“spoofing”) fraud. Where a consumer is manipulated by a fraudster pretending to be the consumer's PSP, using communication channels attributed to that PSP, the PSP must refund the full amount of the resulting fraudulent authorised transaction. Two conditions apply: the consumer must, without undue delay after becoming aware of the fraud, notify the PSP and report the matter to the police. The PSP must then either refund the consumer or provide justified reasons for refusing the refund within 15 business days. The burden of proving that the consumer acted fraudulently or with gross negligence lies with the PSP,

which must invite the consumer to provide information and duly consider it before reaching any conclusion. The use of a payment instrument or the completion of SCA will not, of itself, be sufficient evidence that a transaction was authorised or that the payer acted fraudulently or with gross negligence.

- **Anti-spoofing obligations.** Payment service providers must have adequate prevention and robust technical safeguards in place to prevent the fraudulent replication and misuse of their communication channels, including their domain name, email address and calling line identification.

- **Fraud data reporting and information-sharing guardrails.** PSPs will be required to report periodic fraud data to their competent authorities (anticipated to be on at least a semi-annual basis, in a harmonised format to be specified by EBA ITS), feeding a joint EBA/ECB publication on fraud trends. Voluntary information-sharing arrangements between PSPs are permitted, subject to robust safeguards including a joint data protection impact assessment under Article 35 of the General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**). Importantly, a PSP may not take "de-risking" decisions (i.e. decisions to terminate, restrict or refuse a customer relationship in order to avoid perceived compliance, regulatory or financial-crime risk) such as termination or onboarding refusal solely on the basis of shared fraud signals, without conducting an independent assessment (see further the contractual and policy section below).

Cross-sectoral cooperation and advertising of financial services

The PSR establishes new obligations for cross-sectoral cooperation in fraud prevention. Payment service providers may exchange data with providers of hosting services and electronic communications services where there are objectively justified grounds to suspect fraud. Electronic communications services providers must take appropriate measures to detect and prevent the use of their services for impersonation fraud, including manipulation of calling line identification.

Providers of VLOPs and VLOSEs within the meaning of the Digital Services Act (Regulation (EU) 2022/2065) (**DSA**) must request authorisation or registration details from advertisers of regulated financial services and make best efforts to verify these details before permitting advertisements. The Commission has exclusive supervisory and enforcement powers over these VLOP/VLOSE obligations.

Enforcement, penalties and dispute resolution

The PSR requires Member States to set up complaint procedures and grants competent authorities a comprehensive minimum set of investigatory and sanctioning powers, including the power to require submission of documents, carry out on-site inspections, obtain written or oral explanations, seize items and data, request freezing of assets and refer matters for criminal investigation. In the absence of other available means, competent authorities may order the removal of online content, block access to websites of unauthorised PSPs and request domain registries to delete domain names.

The PSR establishes a harmonised minimum set of maximum administrative pecuniary sanctions, applicable both to firms and to natural persons holding management responsibility. For legal persons, the maximum administrative fine must be at least the higher of a fixed monetary amount and a percentage of the firm's total annual turnover, in line with the calibration adopted in other recent EU financial-services instruments such as MiCAR and DORA, with proportionate ranges for natural persons. Competent authorities are also empowered to publish their decisions, including the identity of the sanctioned firm or individual, subject to proportionality safeguards. The framework expressly contemplates personal liability of members of the management body and other senior persons where a breach can be attributed to their conduct.

PSPs must maintain internal complaint resolution procedures, replying to complaints within 15 business days (or 35 in exceptional cases). Participation in alternative dispute resolution (**ADR**) procedures for consumer disputes is mandatory for PSPs.

The EBA is granted product intervention powers, enabling it to temporarily prohibit or restrict certain types of payment or electronic money services that may cause harm to consumers or threaten the orderly functioning and integrity of financial markets. Any such EBA action prevails over prior national competent authority measures and must be reviewed at least every three months.

Key implications for regulated firms

The new framework carries several important implications for payment service providers and other regulated firms operating under the EU payments regime:

1. **Re-authorisation and transitional planning.** Existing payment institutions authorised under PSD2 and electronic money institutions authorised under the E-Money Directive must demonstrate compliance with the new PSD3 requirements within 27 months of entry into force or face suspension. Firms should begin gap analyses against the new authorisation conditions and prudential requirements without delay.

2. **Access to payment accounts for PIs.** The PSR will require credit institutions to provide payment accounts to PIs and licence applicants on an objective, non-discriminatory and proportionate basis. Refusal or closure of an account must be substantiated in writing and PIs will have a right of appeal. The EBA is mandated to develop RTS specifying the format and content of refusal/closure notifications. This addresses the long-standing "de-risking" exposure for PIs and EMIs and is a material structural mitigant for new market entrants.

3. **Safeguarding overhaul.** The enhanced safeguarding requirements, including concentration risk avoidance, user transparency obligations and the forthcoming EBA RTS on safeguarding risk management frameworks, will require many PIs to review and potentially restructure their treasury and safeguarding arrangements, including maintaining relationships with multiple credit institutions.

4. **Open banking infrastructure investment.** ASPSPs must invest significantly in API infrastructure, data parity and performance monitoring to comply with the enhanced dedicated interface requirements. The prohibition on obstacles and the consent dashboard obligation will require redesigns of both backend systems and customer-facing interfaces.

5. **Fraud prevention systems.** The expanded liability framework, particularly for impersonation fraud and transaction monitoring failures, significantly increases the financial exposure of PSPs. Firms must invest in robust real-time transaction monitoring on both the payer and payee sides, implement anti-spoofing technical safeguards and establish clear internal procedures for handling disputed transactions and refund requests within the prescribed timeframes.

6. **Verification of Payee.** The mandatory VoP service (see Fraud prevention and the expanded liability framework above), applying from 27 months after entry into force, will require systems development, coordination with payee PSPs and integration with existing payment initiation channels.

7. **SCA and accessibility.** PSPs must review and update their SCA implementations, particularly around mobile application activation protocols, digital wallet outsourcing arrangements and accessibility requirements for persons with disabilities, older persons and those with low digital skills.

8. **Governance and operational resilience.** PSD3 explicitly integrates DORA requirements into the authorisation conditions and PIs must demonstrate a high level of digital operational resilience as a condition of authorisation.

9. **Cross-sectoral obligations.** Firms operating VLOPs, VLOSEs, or electronic communications services should note the new cross-sectoral obligations concerning fraud prevention and the advertising of regulated financial services.

10. **Board and senior management governance.** The PSR's expanded liability provisions and the integration of DORA into the authorisation conditions elevate the role of the management body in the oversight of fraud prevention, ICT and operational resilience and customer outcomes. Firms should review reporting lines, management information packs (in particular for fraud KPIs and dedicated-interface availability), the role of the compliance and risk functions and the documentation supporting the suitability of senior managers under PSD3 fit-and-proper assessments.

Key priorities for contractual and policy documentation

The PSR and PSD3 will necessitate a comprehensive review of regulated firms' contractual documentation and internal policy frameworks. The following priorities emerge from the new requirements:

- **Framework contracts and customer-facing terms.** The PSR's enhanced information and transparency requirements under Titles II and III will require firms to update their framework contracts with PSUs. Framework contracts will need to include, among other things: information on the PSP's liability for impersonation fraud under Article 59 PSR; the conditions for refund of authorised transactions; the procedure for notifying the PSP and the police in cases of spoofing fraud; and details of the VoP service and the consequences of proceeding despite a notified mismatch. Terms governing the keeping of personalised security credentials must not be drafted in a way that prevents users from taking advantage of open banking services offered by third-party providers. Any changes to framework contracts must be proposed to users no later than two months before their proposed date of application, with clear information on the user's right to terminate free of charge.

- **Safeguarding disclosures.** PSD3's new transparency obligation requires payment institutions to provide each payment service user, prior to entering into an agreement and upon any material change, with clear information on how that individual user's funds are safeguarded, the applicable insolvency law and the Member State in which a claim should be raised in the event of insolvency. This will require new standardised disclosures to be integrated into onboarding documentation and existing customer communications, as well as internal procedures to ensure disclosures are updated promptly when safeguarding arrangements change.

- **Open banking agreements and API documentation.** ASPSPs must prepare and maintain technical documentation for their dedicated interfaces, make a summary publicly available on their website and provide full documentation free of charge to authorised AISPs and PISPs. Changes to API technical specifications must be notified at least two months in advance. Where ASPSPs and third-party providers enter into voluntary multilateral contractual arrangements (such as premium API schemes), these must not restrict the right of AISPs and PISPs to access regulated payment account data without charge and without being party to such arrangements. Consent dashboard design and functionality must comply

with the prohibition on deterring language and manipulative design, requiring legal review of dashboard terms and user-interface wording.

- **SCA outsourcing agreements.** Operators of digital pass-through wallets that verify SCA elements must enter into outsourcing agreements with payers' payment service providers. These agreements must allocate full liability to the PSP for any SCA failure by the wallet operator and must include the PSP's right to audit and control the wallet operator's security provisions. PSPs should review existing wallet operator arrangements against these requirements and negotiate new or amended agreements as necessary.

- **Fraud prevention policies and procedures.** Firms must develop or update internal policies to reflect the new transaction monitoring obligations on both the payer and payee sides, including real-time monitoring for instant credit transfers. Internal procedures for handling impersonation fraud claims must be documented, including the 15-business-day response window, the process for inviting consumers to provide evidence and the escalation procedure where a refund is refused on grounds of fraud or gross negligence. Anti-spoofing technical safeguard policies, covering domain name protection, email address security and calling line identification, must be formalised and maintained.

- **Information sharing arrangements.** The PSR provides for voluntary fraud data sharing between PSPs, subject to robust safeguards. Firms intending to participate in multilateral information sharing arrangements must carry out a joint data protection impact assessment under Article 35 of the GDPR before concluding such arrangements and must ensure that the arrangements contain appropriate technical and organisational measures, including pseudonymisation, encryption and access controls. Critically, firms must not draw conclusions or take decisions affecting a business relationship with a payment service user, such as terminating the contractual relationship or affecting onboarding, solely on the basis of information received from other PSPs through an information sharing arrangement without having independently assessed that information.

- **Complaint handling and ADR documentation.** PSPs must update their complaint handling procedures to reflect the 15-business-day response deadline (35 business days in exceptional cases) and the mandatory participation in ADR procedures for consumer disputes. Information about the competent ADR entity must be prominently displayed on the firm's website, mobile application, at branches and in general terms and conditions.

- **Winding-up plans and business continuity.** PSD3 introduces a new requirement for payment institutions (other than those providing only payment initiation or account information services) to prepare a winding-up plan adapted to the firm's size and business model, including arrangements for the return of safeguarded funds in the event of a disorderly wind-up. This plan forms part of the authorisation application and will need to be maintained on an ongoing basis.

- **Agent and outsourcing agreements.** PSD3 requires payment institutions to remain fully liable for the acts of their agents and outsourced service providers. Outsourcing arrangements must be reviewed to ensure that they do not violate PSD3 requirements and firms must take reasonable steps to ensure continuing compliance. Where operational functions are outsourced, the payment institution must inform its competent authority without undue delay and notify any changes regarding outsourced entities.

- **Customer communications and conduct risk.** Beyond framework contracts, firms should review marketing and pre-contractual materials (including app-based and in-journey disclosures), vulnerable customer policies (informed by the new SCA accessibility requirements) and treatment of complainants under the recalibrated impersonation-fraud refund regime. Particular attention should be paid to consistency between disclosures, customer journeys and internal procedures, given the strict liability standards now applicable to monitoring and VoP failures.

Key dates and implementation timeline

The principal milestones for programme planning, calculated by reference to the date of entry into force of each instrument, are summarised below. Firms should track these dates closely as the EBA's RTS and guidelines mandates fall into the same window.

- **Entry into force**. Twenty days after publication in the Official Journal of the European Union, currently anticipated for the second half of 2026 subject to formal adoption.

- **T+12 to T+18 months**. Most EBA RTS and ITS deliverables fall due, including standards on dedicated interfaces, safeguarding risk management, refusal/closure of PI payment accounts and the independence of two inherence elements for SCA.

- **T+21 months**. Substantive provisions of the PSR and PSD3 generally apply.

- **T+27 months**. The mandatory VoP service applies for credit transfers; the transitional regime for existing EMIs expires; non-compliant EMIs are suspended from providing payment services.

- **T+3 years**. Commission review of vIBANs, EMT rules, the scope of the PSR and the obligations on electronic communications and hosting service providers.

- **T+7 years**. Comprehensive Commission review of open banking, fraud prevention and consumer refund rights.

Interaction with adjacent EU frameworks

The PSR and PSD3 do not sit in isolation. Several adjacent EU instruments, both already in force and in the legislative pipeline, interact with the new payments framework and should be considered together when planning implementation.

- **Instant Payments Regulation.** The Instant Payments Regulation (Regulation (EU) 2024/886) (**IPR**) introduced standalone VoP and reachability obligations for euro-denominated instant credit transfers. The PSR generalises VoP across credit transfers and aligns the underlying liability framework; firms that have already implemented IPR-driven systems should reassess them for PSR fit, including the harmonised liability standard and the treatment of non-consumer opt-outs.

- **AML/CFT package.** The new AML package, comprising the Anti-Money Laundering Regulation (**AMLR**), the sixth Anti-Money Laundering Directive (AMLD6) and the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (**AMLA**), interacts directly with the PSR's de-risking guardrails, the safeguarding regime and the cross-sectoral information-sharing provisions. Firms should ensure that AML, fraud and sanctions controls are designed to operate coherently with the PSR's prohibition on de-risking decisions taken solely on the basis of shared fraud signals.

- **Financial Data Access framework.** The proposed Financial Data Access Regulation (FiDAR) is the natural successor to open banking, extending data access obligations beyond payment accounts to a wider set of financial services data. ASPSPs investing in PSR open-banking infrastructure should design their interfaces, consent dashboards and operating models with FiDAR's broader scope in mind.

- **Digital Euro.** The Commission's proposal for a digital euro contemplates that PIs and credit institutions will be the primary distribution channel. The PI authorisation perimeter under PSD3 will, accordingly, define which firms can offer digital euro services, with consequent implications for product design and infrastructure investment.

- **Consumer Credit Directive II.** The Consumer Credit Directive II (Directive (EU) 2023/2225) (CCD II) extends consumer protection obligations to a wider range of credit products, including certain card-based credit. PSPs offering credit cards or buy-now-pay-later services should align CCD II disclosures with the PSR's transparency and framework-contract requirements.[6]

- **DORA and MiCAR.** As discussed above, DORA is now embedded in the PSD3 authorisation conditions and MiCAR is bridged with PSD3 through streamlined authorisation routes. Firms should treat the three instruments as a single regulatory perimeter for tokenised payment, ICT-resilience and crypto-asset operations.

Transitional and grandfathering planning

Although the headline transitional regime concerns existing EMIs, regulated firms should map a wider set of legacy authorisations, registrations and exemption notifications against the new framework.

- **Existing PI authorisations**. PIs authorised under PSD2 will be expected to demonstrate compliance with the PSD3 conditions by the application date and competent authorities will assess updated documentation (including governance, ICT and safeguarding documentation) on a case-by-case basis.

- **AISP and PISP registrations**. Existing AISPs and PISPs will need to align their operating models with the consolidated PSR perimeter and the enhanced open-banking conduct rules; existing registrations remain subject to verification of continuing compliance.

- **Limited network and SPI notifications**. Providers operating under previously notified limited network or specific-purpose instrument arrangements should re-test their products against the recalibrated PSR exclusions and EBA guidelines and may need to refresh notifications under the lower thresholds.

- **Safeguarding arrangements**. Existing safeguarding documentation and counterparty arrangements should be reviewed for compliance with the new concentration risk, transparency and risk-management requirements, with restructuring lead times factored into programme planning.

- **Implementation detail still to be finalised.** The EBA's mandate to develop extensive RTS, ITS and guidelines means that important operational detail, including the criteria for own-funds Methods A and

[6] See coverage also here.

C, the dedicated-interface key performance indicators, the parameters for SCA-element independence and the format and content of refusal/closure notifications will not be known until well into the application window. Firms should expect the EBA to consult on most of these instruments in the first half of 2027, with final standards published 12 to 18 months after entry into force.

- **Open lobbying battles.** Industry attention will focus on the scope and modalities of the FRAND access regime for OEMs and electronic communications providers (where the digital-wallet competitive dynamic remains contested), the calibration of the limited-network thresholds and the interaction between the PSR's information-sharing guardrails and the AMLR/AMLA framework. The vIBAN review (3 years) and the broader scope review (7 years) will be the two most consequential post-implementation policy battlegrounds

- **Likely supervisory focus.** Drawing on enforcement patterns under PSD2 and the EBA's recent supervisory priorities, regulated firms should expect early supervisory attention on (i) safeguarding integrity and concentration risk; (ii) the operationalisation of the impersonation-fraud refund right; (iii) the implementation of VoP within the prescribed execution windows; and (iv) the application of SCA exemptions, particularly for low-value and contactless transactions. Firms operating cross-border can expect intensified supervisory cooperation under the new EBA-coordinated framework.

- **Action posture.** The 21-month application deadline, while not imminent, is ambitious given the breadth of the changes. Firms should aim to complete their gap analyses by Q4 2026, agree their target operating models by Q2 2027 and begin their build phase no later than Q3 2027 to leave adequate runway for testing, supervisory dialogue and customer migration. Firms that treat the PSR/PSD3 reforms as a single regulatory perimeter alongside DORA, MiCAR, the AML package, the IPR, FiDAR and the digital euro will be better positioned to extract competitive advantage from the implementation cycle than those that treat each instrument as a separate workstream.

Outlook

The PSR and PSD3 represent a generational reform of the EU's payment services framework. The shift from a directive to a regulation for conduct-of-business rules will eliminate national divergence and create a single compliance standard for the internal market. The merger of the PI and EMI regimes will simplify the licensing landscape but will impose a mandatory re-authorisation exercise on existing EMIs. The recalibrated fraud prevention and liability provisions, particularly the dedicated refund right for impersonation fraud and the mandatory transaction monitoring obligations on both payer and payee PSPs, will require material investment in systems, processes and governance.

The EBA's mandate to develop extensive RTS and ITS across the framework means that important implementation detail remains to be finalised. In particular, the RTS on SCA, transaction monitoring, safeguarding risk management, dedicated interfaces and cross-border supervisory cooperation will be critical in determining the operational impact of the new framework. Most of these RTS are due within 12 to 18 months of entry into force of the respective instruments.

Among the standard-setting deadlines most relevant for programme planning are: (i) EBA RTS on dedicated interface key performance indicators and recovery times; (ii) EBA RTS on the format and content of refusal/closure notifications for PI payment accounts; (iii) EBA RTS on safeguarding risk management frameworks; and (iv) EBA guidelines on the independence of two inherence elements for SCA. Most of these deliverables are due within 12 to 18 months of entry into force, ahead of the 21-month application date for the substantive obligations.

The Commission is required to conduct a comprehensive review within seven years of entry into force, covering open banking, fraud prevention and consumer refund rights. An earlier review, within three years, is mandated for virtual IBANs, electronic money token rules, the scope of the PSR and the obligations on electronic communications and hosting service providers.

Regulated firms should monitor the development of the EBA's technical standards closely and engage in the consultation processes as they emerge. The 21-month transposition and application deadline, while not imminent, is ambitious given the breadth of the changes involved and early engagement with the implementation workstreams will be essential to ensure readiness.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from relevant related developments. We have assembled a multi-disciplinary and multijurisdictional team of sector experts to support clients navigate challenges and seize opportunities as well as to proactively engage with their market stakeholders and regulators.

Moreover, we have developed a number of RegTech and SupTech tools for supervised firms, including PwC Legal's Rule Scanner tool, backed by a trusted set of managed solutions from PwC Legal Business Solutions, allowing for horizon scanning and risk mapping of all legislative and regulatory developments as well as sanctions and fines from more than 2,500 legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

Equally, in leveraging our Rule Scanner technology, we offer a further solution for clients to digitise financial services firms' relevant internal policies and procedures, create a comprehensive documentation inventory with an established documentation hierarchy and embedded glossary that has version control over a defined backward plus forward looking timeline to be able to ensure changes in one policy are carried through over to other policy and procedure documents, critical path dependencies are mapped and legislative and regulatory developments are flagged where these may require actions to be taken in such policies and procedures.

The PwC Legal Team behind Rule Scanner are proud recipients of ALM Law.com's coveted "2024 Disruptive Technology of the Year Award" and the "2025 Regulatory, Governance and Compliance Technology Award in 2025".

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas	**Dr. Jörg Schwerdtfeger**	**Fabian Joshua Schmidt**
Tel.: +49 160 973 757-60	Tel.: +49 160 8839939	Tel.: +49 151 414 904 37
michael.huertas@pwc.com	joerg.schwerdtfeger@pwc.com	fabian.joshua.schmidt@pwc.com