Hogan Lovells

PSD3 Impacts

Contents

1. Introduction

Given the sea change of PSD2, one might expect the prospect of the proposed PSD3 and PSR to have PSPs groaning at the thought of yet more root and branch reg change projects. However, whilst the proposals are certainly wide-ranging and will require PSPs to make further changes, this latest chapter in the ongoing saga of payments regulation is slightly more "evolution" than the "revolution" of its predecessor.

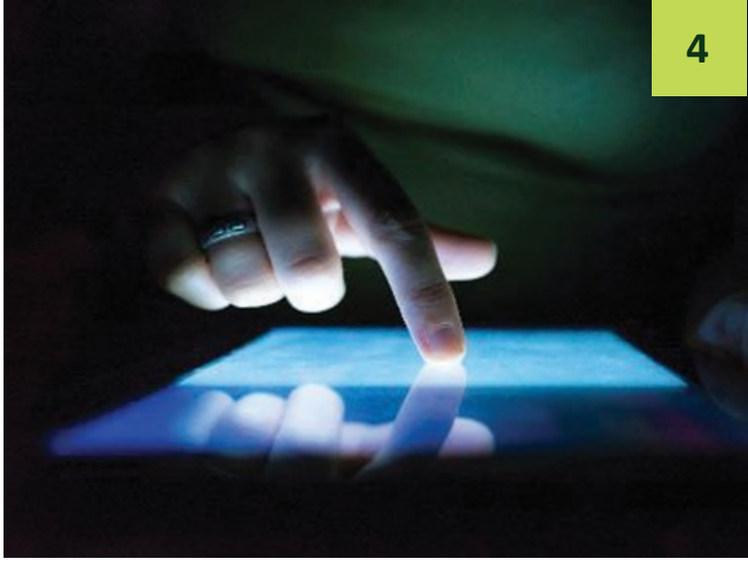
That is not to say the changes required will be insignificant or unchallenging (not least in terms of the tech and ops projects the proposed changes appear to require). However, the legislative package is less all encompassing in its vision, building on various aspects of the PSD2 regime.

Following the publication of the Council Text, this briefing has been updated and summarises the impact of the draft proposals in all three texts thematically, highlighting the areas where the trilogue process might shift the dial further, and flagging where changes might need to be reflected in PSPs' businesses. See our "at a glance" table mapping these changes.

Who is impacted?

The proposals affect different parties in different ways:

- EMIs will need to consider their approach to safeguarding due to the merging of the money and payments regimes and will have to register their distributors with regulatory authorities.
- Consumer facing PSPs will need to grapple with an increased liability regime that will encompass authorised push payment fraud (the extent of which is "TBD") alongside the existing regime for unauthorised and defective transactions, and remain liable to the consumer potentially for longer than the 13-month protection first introduced under PSD1.
- Corporate facing ASPSPs may have much less discretion when it comes to the requirement to provide banking services to other PSPs.
- ASPSPs will have to review their SCA solutions – with an increased focus on ensuring non-tech savvy PSUs are not left behind - as well as TPP access solutions, which are expected to be dedicated interface solutions rather than modified customer interfaces. Additionally, ASPSPs will be required to enable PSUs to manage the various consents they have given to TPPs centrally, within the ASPSP domain via a "dashboard".
- "Big Tech" will face the challenge of indirect regulation as legislators seek to expand the scope of payment regulations.
- ASPSPs will need to share details of accounts/ customers that are suspected of operating fraudulently.
- Online platforms that have made use of the commercial agent exemption will need to consider if they can still operate without needing to be authorised or at least partner with a PSP to continue their operations.
- PSPs will need to provide the additional information they are required to provide to the regulatory authorities within the two-year transitional period.
- CASPs may need to become dual authorised to provide payment services in EMTs.



What is the impact?

The changes this legislative package proposes will also affect particular areas of a PSP's business in different ways. This is likely to include a combination of changes to customer agreements, policies and procedures, technology and operations, as well as, in some cases, a need for regulatory engagement.

The table below maps out where we believe the incoming changes will affect a PSP's business.

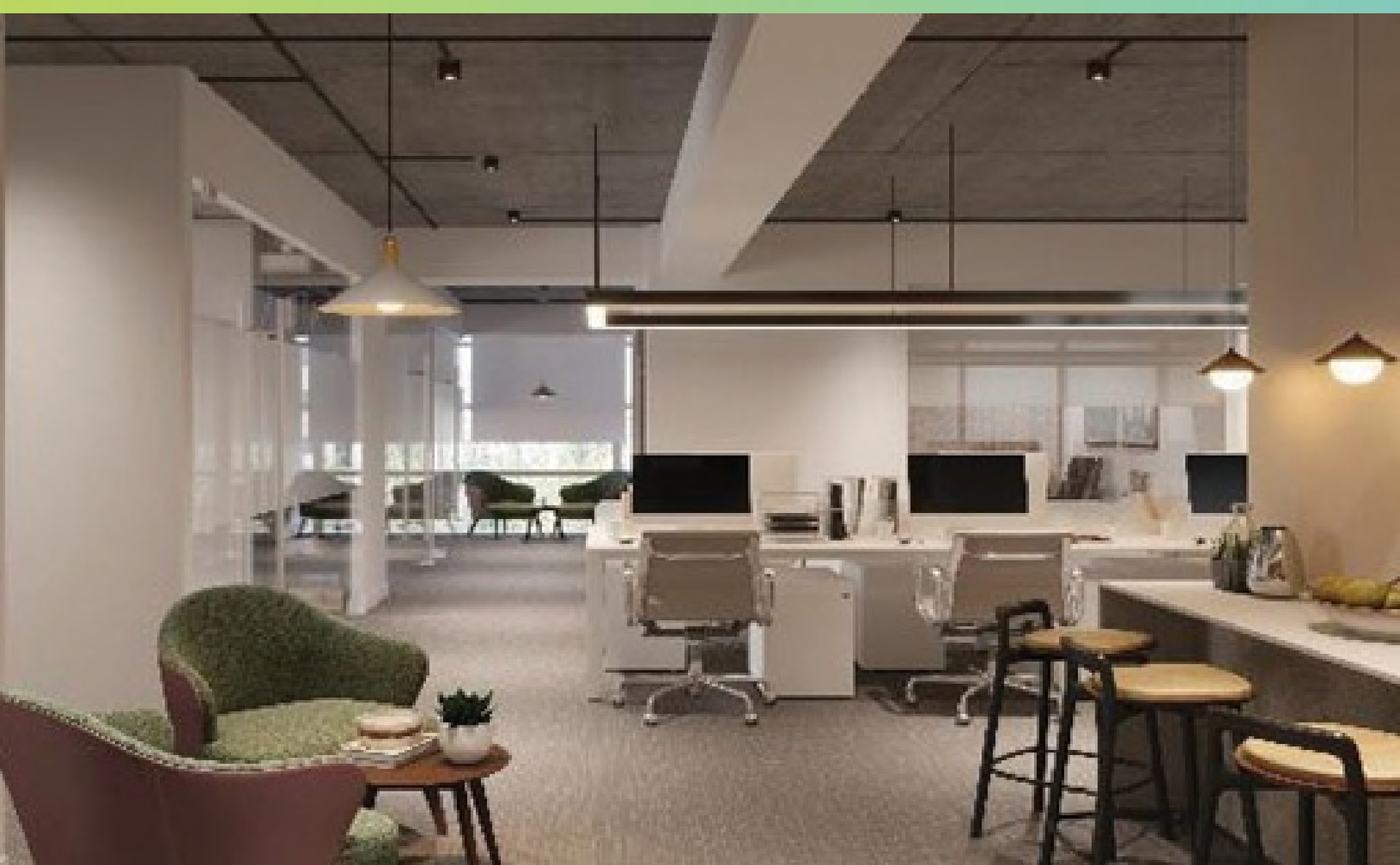
Area of Impact						
PSD3 area of focus	Regulatory Engagement	Technological Build	T's and C's	Policies and Procedures	Operational Change	Impact on PSP Liability
Distributors (E-Money only)						
Regulatory Information	✓			✓	✓	
Safeguarding	✓					
Transaction Monitoring	✓				✓	
Data Sharing	✓			✓	✓	
Technical Service Providers	✓	✓	✓		✓	✓
Electronic Communications Services Providers				✓	✓	✓
Access to payment systems/services				✓	✓	✓
TPP Interface				✓		
TPP Dashboard	✓	✓		✓	✓	
SCA	✓	✓	✓	✓	✓	
Confirmation of Payee		✓		✓	✓	✓
Impersonation Fraud (Consumer only)		✓	✓	✓	✓	✓
Surcharging		✓	✓	✓	✓	✓
EBA Intervention	(if it impacts financial projections)		✓		✓	
CASPs	✓	✓	✓	✓	✓	✓
Card Schemes			✓	✓	✓	

2. Latest developments in legislative process and expected timing

The Council of the EU's drafts of PSD3 and the accompanying PSR were approved by COREPER on 18 June 2025, meaning that the trilogue process can now begin.

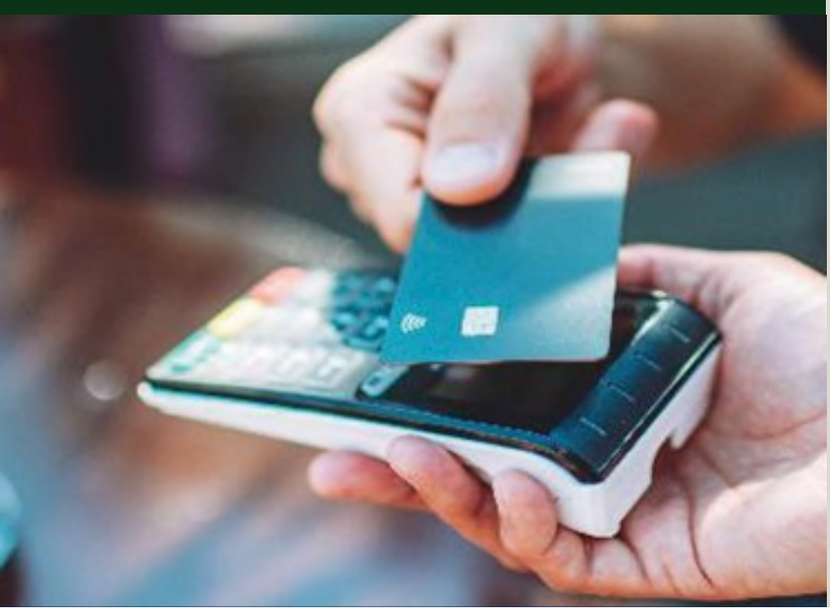
Whilst the Council does not appear to have deviated wildly from the original text, there are points of contention and differences. Trilogues can often be a long process; however, there is strong appetite to get both files concluded under the Danish presidency which concludes at the end of the year.

At present there is an 18-month implementation period (although the Council proposes to extend this to 24 months). As such, the earliest PSD3/PSR is likely to become applicable is H2 2027, although this could move into early 2028 if the Council is successful in extending the implementation period.



3. Authorisation/ re-authorisation and changes to the e-money regime

(PSD3 Arts 3, 9, 19-20 & 44 – 45)



Overview

- No significant changes concerning the procedures of application for authorisation, control of shareholding and prudential requirements under Title II of PSD3; however:
  - additional information is required to be submitted to address ICT, data sharing, passporting and wind down arrangements;
  - changes required to the way APIs and EMIs safeguard to mitigate concentration risk will need to be notified to the regulator; and
  - EMIs will need to register their distributors (like APIs do agents).
- Current APIs and EMIs will have two and a half years to demonstrate compliance with the incoming prudential requirements under the Council Text (up from 2 years in the other texts).

What is changing?

Authorisation Information (PSD3 Art 3)

More information is required as part of an application for authorisation under PSD3, consisting of:

- a description of arrangements for the use of ICT services, demonstrating governance arrangements, internal control mechanisms and arrangements for the use of ICT services are proportionate, appropriate, sound and adequate (for AISPs this will include digital operational resilience measures in details of security control and mitigation measures);
- for institutions wishing to enter into information-sharing arrangements for the exchange of payment fraud-related data under the proposed PSR, the conclusions of the relevant data protection impact assessment;
- an overview of passporting footprint (current or planned); and
- a winding-up plan tailored to the envisaged size and business model of the applicant.

Existing APIs/EMIs will need to provide additional information required as part of an application for “re-authorisation”.

The EP Text proposes to confirm that licensed APIs/EMIs should only be required to submit additional information introduced by PSD3, and clarifies that noncompliance should be met with suspension rather than loss of licence.

Safeguarding (PSD3 Art 9)

Changes to the safeguarding regime will also trigger NCA engagement since the draft PSD3:

- Aligns the safeguarding regimes of PSD2 and EMD2 – with the result that EMIs will now have to safeguard by the end of the following business day following receipt of funds (previously, EMIs were permitted to safeguard funds within 5 business days after issuing the e-money where such funds were paid by card).
- Introduces a new requirement to mitigate concentration risk of safeguarded funds.

Firms will therefore need to notify regulators of their new arrangements.

E-money distributors (PSD3 Art 19, 20)

Additionally, the PSR proposes to align the status of e-money distributor with that of payment services agent with the result that distributors would be subject to registration requirements (as agents are) with NCAs (and the EBA).

Transition (PSD3 Art 44, 45)

APIs and EMIs will have two and a half years under the Council Text (up from two in the Original Commission Draft and EP Text) to demonstrate compliance with the above Title II requirements of PSD3.

What is the impact?

The uplift will be a less burdensome exercise than that required for PSD2 – although this will still require PSPs to perform a gap analysis and work out what (if anything) must be provided to regulators.

Credit institutions are less likely to be impacted since most of the new requirements would be covered by licensing requirements under the CRD in any event.

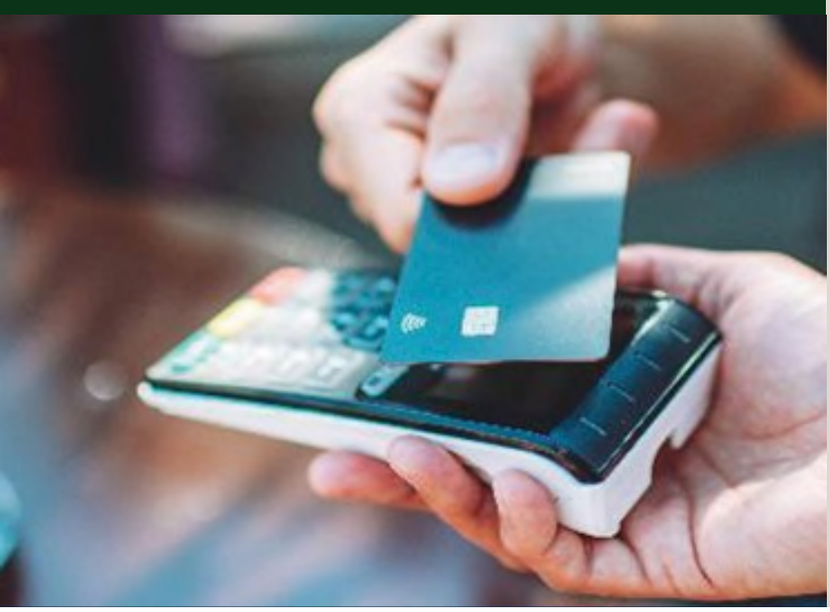
However, certain aspects of the PSD3 changes could prove costly and time-consuming for some – especially EMIs who will need to register all their distributors (like APIs are required currently to register their agents).

The proposed transitional periods provide a certain amount of respite in terms of time pressure – but for some EMIs, this could be a huge exercise (even with the additional 6 months the Council Text allows).

Both APIs and EMIs will need to review their safeguarding arrangements and notify regulators of changes they are making to comply.

4. Electronic money tokens

(PSD3 Art 3(a) Council Text; PSR Art 67(a) Council Text)



Overview

- The Council Text is the first that seeks to properly address electronic money tokens.
- Crytpoasset service providers may need dual authorisation under MICA and PSD3 if they want to provide payment services in relation to electronic money tokens.
- The vast majority of PSR information and conduct obligations will apply to such payment transactions.

What is changing?

The Council Texts are the first set of drafts to properly engage with the emergence of EMTs.

Subject to a couple of specific exemptions (see "Scope of application and exemptions"), the Council Texts ensure that transactions involving EMTs are within the scope of both the payments authorisation and conduct regimes, by widening the scope of 'funds' to include EMTs.

Authorisation (PSD3 Art 3a – Council Text)

Firms authorised under MiCAR seeking permission to carry out payment services using EMTs will also be required to apply for authorisation under PSD3.

The Council Text also provides that where the application is from a CASP licensed under MiCAR, and relates only to authorisation for the provision of payment services with EMTs, NCAs have 60 days to decide an application.

Conduct and Information requirements (PSR Art 67a – Council Text)

Inscope EMT activity will be subject to the full remit of the PSR requirements, save for the specific exclusions proposed in Article 67a of the Council Text that provides that PSPs providing EMT payment services are not required to:

- disclose maximum execution times and costs (although reasoned estimates are required);
- provide access to PISPs and AISPs (where they operate as ASPSPs); or
- comply with confirmation of payee requirements.

What is the impact?

The Council's drafting makes it clear that the existence of a MiCAR licence in itself is insufficient to enable a CASP to operate as a PSP and an additional application for authorisation is required.

In several cases, the elements of the application required for this are required to "build on" the information provided for MiCAR purposes.

That the payments and cryptoassets regimes overlap is made clear in Recitals 90 and 93 of MiCAR, which state that:

- certain CASP activities (e.g. providing custody and administration of cryptoassets on behalf of clients, placing cryptoassets, and transferring services for cryptoassets on behalf of clients) might overlap with payment services as defined in PSD2; and
- many cryptoasset service providers offer transfer services that may (depending on the precise features of the services) mean services could fall under the definition of payment services in PSD2, such that those transfers should be provided by an entity authorised to provide such payment services.

However, the precise nature of the overlap has been unclear.

The EBA has recently issued guidance to NCAs recommending "no action" be taken in relation to CASPs engaging in payment services without a payments licence, pending confirmation of the approach the legislators want to take.

With the publication of the Council Text, we have the first concrete position adopted by an EU legislative body that being licensed as a CASP is not sufficient to qualify as a PSP and that a further (albeit hopefully quickly determined) authorisation process is required.

However, even if the final text moves away from dual authorisation, the intention of the Council Text is that payments involving EMTs should merit the same treatment as payments in other forms.

It is to be welcomed that the Council proposes to exempt CASPs from having to comply with confirmation of payee requirements or provide access to TPPs; however, the application of the PSR regime more generally means CASPs will need to get to grips with:

- the liability regimes for impersonation fraud, unauthorised and defective transactions;
- SCA;
- notice requirements for variation and termination of framework agreements; and
- payments complaints handling timelines.

This will necessarily mean technological build and changes to processes and procedures, and potential divergence among CASPs seeking to provide payments services in EMTs between those that adopt a highest common denominator approach for all services and those that observe the conduct requirements under MiCAR and the PSR separately.

5. Transaction monitoring and data sharing

(PSR Arts 83 & 89)

Overview

- Unique identifiers that have been reported twice to the same PSP in connection to fraud must be shared with the other PSPs.
- Such data sharing between PSPs will be subject to arrangements that define the details for participation and the requirements for operational elements, including the use of dedicated IT platforms.
- Data sharing will require a joint DPIA between PSPs under the GDPR and regarding engagement with the authorities.

What is changing?

PSPs will be required to implement transaction monitoring mechanisms to prevent and detect potentially fraudulent transactions, including fraud involving payment initiation services (as well as to support the application/exemption of SCA).

The proposed PSR prescribes the data that may be used, its retention period (no longer than necessary and not after termination of the relationship), the minimum risk-based factors that must be considered under the monitoring system, and it requires RTS to be introduced.

For transaction monitoring purposes, PSPs will also be required to share unique identifiers to prevent and detect fraud when at least two different PSUs who are customers of the same PSP have notified their PSP that a unique identifier of a payee was used for fraud.

Information-sharing arrangements will define details for participation and will set out the details on operational elements, including the use of dedicated IT platforms.

PSPs must jointly conduct a DPIA under Article 35 of the GDPR and, where applicable, consult with the supervisory authority as referred to in Article 36 of the GDPR.

PSPs must notify authorities of their participation/cessation in the information-sharing arrangements.

The sharing of such data must not lead to the termination of the customer's contractual relationship or affect their future onboarding by another PSP.

The EP Text seeks to expand the data that firms will be required to share to include the name, personal identification number, organisation number, modus operandi and other transaction information.

It also proposes that the EBA sets up a dedicated IT platform to facilitate information exchange and will permit PSPs to terminate future relationships of customers with unique identifiers that have been shared between PSPs where a thorough fraud investigation by the relevant authorities concludes that the customer has participated in fraud.

The Council Text proposes to mandate transaction monitoring prior to a payment being made and following receipt of a payment, with the PSP bearing liability for any loss suffered by the payer where they fail to do so.

It also broadens the categories of data that should be monitored by the payer's PSP to include device data (e.g. identifiers of the device used to initiate or authenticate a payment) and sets out the data that a payee's PSP is required to monitor.

The Council Text limits the data that is required to be shared between PSPs to unique identifiers (as per the Original Commission Draft). However, it mandates that these be shared to the extent necessary to prevent and detect potentially fraudulent payment transactions where there are reasonable and objective grounds to suspect fraud. This is a departure from the proposal that such identifiers would need to be shared where they had been associated with fraudulent activity twice by different PSUs using the same PSP.

The Council Text also imposes an obligation on PSPs not to draw conclusions or take decisions that have an impact on the business relationship with the PSU, or on the execution of a payment transaction based on information received from other PSPs. This is broader (and somewhat vaguer) than the previous obligation preventing them from terminating the relationship per the EP Text.

What is the impact?

PSPs will have been monitoring transactions in any event; however, the requirement to share the results of such monitoring will require participation and use of data sharing arrangements with other PSPs, which will need to comply with GDPR assessment requirements and trigger regulatory engagement.

6. Scope of application and exemptions

(PSD3 Arts 2(38), 38; PSR Arts 2 – 3, 55a, 58, 59(5a) – (5c), 87 & 89)

Overview

- ATM deployers that do not service payment accounts will be required to register with NCAs and potentially be subject to information requirements around fees and charges.
- Both the Original Commission Draft and EP Text seek to capture technical service providers and electronic communications services providers within the scope of the regulatory regime, albeit indirectly.
- The scope of the commercial agent exemption is being reduced further.

What is changing?

ATM deployers (PSD3 Art 2(38), 38)

PSD3 introduces a light touch registration regime for ATM deployers (ATM operators that do not service payment accounts).

The EP Text proposes a new provision requiring ATM deployers to comply with the requirements on transparency of fees and charges in Article 7 of the proposed PSR, with a particular obligation to ensure the display of those fees and charges at the very beginning of the transaction.

Indirect extension of the regime (PSR 58, 87, 89 and PSR 55a, 59(5a) – (5c))

All three texts reveal moves to extend the scope of the payments regime to technical service providers and electronic communications services providers via indirect application.

- The Original Commission Draft and Council Text seek to make technical service providers that provide and verify the elements of SCA outsourced service providers (and subject to audit and access rights).
- The Council Text also removes the exemption for services provided by technical services providers generally.
- The EP Text seeks to impose obligations on electronic communications services providers in connection with impersonation fraud.

In each case, none of the third parties will be directly regulated by PSD3 or the proposed PSR, so presumably the intention is that obligations will be imposed by contractual arrangements with the PSP.

Exemptions (PSR Arts 2-3)

In terms of the regulatory perimeter, the PSR is further clarifying the scope of the commercial agent exemption, providing that the appointment to represent only one of the payer or payee exempts activity regardless of whether the agent is in the flow of funds or not, but only does so where the appointment gives the payer or payee a 'real margin' to negotiate with the agent or conclude a sale/purchase.

The EP Text proposes the addition of a new optional exemption where, for payment transactions used for the execution of trading and settlement services using EMTs as defined in Article 3(1), point (7) of MiCAR, the PSP has already been authorised as a CASP in a member state for those services under Title V of MiCAR.

The Council Text goes one step further, proposing to exempt:

- payments transactions carried out by a CASP intermediating between a buyer and a seller where EMTs are exchanged for EMTs or cryptoassets, as well as the exchange of EMTs for funds, including EMTs, or cryptoassets carried out by a CASP acting in its own name as buyer or seller of such tokens;
- payment transactions with EMTs, without any intermediary involved, including transfers of EMTs between two self-hosted addresses; and
- payment transactions between CASPs for their own account.

What is the impact?

Parties more tangentially connected to the payments world (ATM networks, commercial agents, technical service providers and tech platforms) will need to consider the extent to which the new regime applies to them.

This will be particularly relevant to tech platforms — which are clearly within certain regulators' sights.

Businesses that have relied on the commercial agent exemption to date will need to consider the extent to which their appointment continues to allow them to remain exempt.

7. Access for PSPs to payment systems and services

(PSR Arts 31–32)

Overview

- The detailed access requirements are now addressed in the proposed PSR, and so will have direct effect, which should limit the scope for divergence between member states.
- Grounds for refusing access to payment services are significantly limited.
- The proposed PSR requires increased transparency around the requirements/ assessment process for access to payment systems.

What is changing?

The proposed PSR clarifies the requirements around access to payment systems and seeks to level the playing field even further:

- In addition to being objective, non-discriminatory, and proportionate, rules must be transparent and can be imposed to guard against credit and liquidity as well as other risks (such as settlement or business risk).
- The rules and procedures for admission to the payment system, as well as the criteria and the methodology used for the risk assessment of applicants, must be publicly available.
- A system operator can only refuse access where an applicant poses risks to the system.

The proposals go somewhat further in the changes it makes to the rules requiring ASPSPs to provide access to payment accounts.

Access requirements will be extended to agents and distributors (to conduct payment services on behalf of APIs) and to entities applying for authorisation under PSD3.

The proposed PSR also seeks to limit the grounds on which an ASPSP can refuse or withdraw services, restricting such reasons to:

- where there are serious grounds to suspect defective AML controls or illegality by the applicant or its customers;
- breach of contract;
- failure to provide insufficient information when applying to open an account; and
- where the applicant presents an excessive risk profile or a disproportionately high compliance cost for the credit institution.

The proposals changes the process of refusal too, with notice being required to go to the applicant, who can then appeal to the NCA as a court of appeal.

The EP Text softens this slightly, reverting to 'reasons justified on objective, nondiscriminatory and proportionate grounds' and providing the grounds listed above as examples (although requiring a breach of contract to be a material breach and removing disproportionately high compliance costs for the credit institution as a reason). However, this would still involve a raising of the bar.

The EP Text also proposes to require closure to be subject to 4 months' notice, reintroduces the need to notify an NCA of refusal/closure, and proposes EBA guidelines to specify permitted grounds for refusal.

The Council Text proposes yet another formula:

- Providing that APIs or their agents or applicants for a licence as an API shall have access on an objective, nondiscriminatory and proportionate basis and that refusal is only permitted where opening or maintaining an account would breach the AMLR, there has been a substantive breach of contract, or insufficient information or documents have been received by the ASPSP;
- Removing excessive risk and compliance costs as grounds for refusal;
- Imposing a 1-month response time for the ASPSP to revert to the applicant PSP;
- Imposing a 3-month notice period for closure.

What is the impact?

System operators and banks will need to review their policies and procedures for granting access to PSPs, and in particular the grounds on which they can refuse access to bank account services.

The only grounds for refusal that appear to go to a bank's risk appetite to undertake this business are those of' excessive risk or cost'. Banks (PSR Arts 31–32) should start thinking about what excessive risk or cost might look like should these grounds make it back into the text.

8. TPP access

(PSR Arts 35–39, 44–45)

Overview

- Much of the RTS on SCA and secure communications has been absorbed into the proposed PSR.
- ASPSPs will be required to implement dedicated interface solutions for TPP access.
- In the event that the dedicated interface is unavailable, ASPSPs may have to offer an alternative interface without delay, with TPPs able to lobby regulators that they should have use of the customer interface if this takes too long. The Council Text, however, has removed these last two elements.

What is changing?

The proposed PSR now requires all ASPSPs to rely on a dedicated customer interface for TPP access.

The obligation to maintain a contingency mechanism, or apply for an exemption from doing so, has been “replaced” in the Original Commission Draft with the requirement to offer an alternative interface without delay in the event that a dedicated interface becomes unavailable. TPPs can ask their NCA to require the ASPSP to allow them to use the customer interface if this takes too long. The Council Text has removed both of these elements.

PSPs can apply to their NCA to use the customer interface in place of a dedicated customer interface.

The EP Text proposes to require ASPSPs to always allow access to interfaces that allow business continuity for TPPs and, where an ASPSP permits multiple SCA options, to allow the TPP the option to choose what can be offered to the payer.

Interestingly all three texts permit ASPSPs to apply for a derogation from having to have a dedicated interface (relying instead on a customer interface) or from having to 'offer any interface at all for secure data exchange', with the EBA to provide RTS on the granting of such an exemption.

The Council Text limits these standards to the exemption from having to have an interface at all, committing the EBA to consider 'inter alia... the size, annual turnover and payments volume of the account servicing payment service provider'.

What is the impact?

ASPSPs with a modified customer interface will either have to apply to their NCA to be allowed to use their customer interface for TPP access, or will need to move to a dedicated customer interface.

ASPSPs that currently have the benefit of the contingency mechanism exemption will now need to ensure that they are able to make an alternative interface available to TPPs “without delay” (and potentially the customer interface if requested).

Both could involve significant regulatory projects requiring considerable tech build.

As before, this will not be subject to the corporate optout so ASPSPs operating in the corporate banking space will be required to undertake regulatory projects requiring operational build for TPPs that have shown limited interest (if any) in accessing accounts in this space unless they can be exempted from the requirement to provide an interface at all.

9. TPP dashboard

(PSR Art 43)

Overview

- ASPSPs will need to provide a customerfacing dashboard that enables PSUs to see and manage the consents they have granted to TPPs (and to cancel them).
- ASPSPs and TPPs will need to communicate to ensure the data on the dashboard is accurate and live.
- This is not subject to the corporate optout.

What is changing?

The proposed PSR imposes a new obligation on ASPSPs to provide a "dashboard" as part of their online service to enable PSUs to:

- see and manage the consents they have granted to TPPs to access their accounts (i.e., who, what, why, when); and
- allow cancellation and re-establishment of those consents in the ASPSP domain.

ASPSPs and TPPs will be required to co-operate to ensure the information on the dashboard is live and to communicate changes in permission/new permissions to each other.

Specifically, TPPs will need to disclose the purpose of permissions and the duration of the consent.

The EP Text proposes:

- minor changes to reflect the scope of the ASPSP's ability to control the TPP/PSU relationship (for example, a dashboard can't enable a PSU to re-establish consent once cancelled);
- to allow PSUs to opt out of data sharing with third parties generally (for both present and future access requests);
- that the EBA introduces guidelines on the data that the dashboard will cover; and
- to impose obligations on TPPs to stop using, and to withdraw and erase all data following cancellation by the customer.

Interestingly, the Council Text also plans ahead for the eventual enactment of the draft FIDA, requiring TPP dashboards to be consistent with FIDA equivalents, and to allow PSUs to manage data permissions pursuant to both the PSR and FIDA through a single dashboard.

What is the impact?

Unless a market solution emerges, ASPSPs could be put to significant cost to provide a solution that enables the necessary communications between themselves and TPPs to ensure that PSUs can cancel the permissions they have given to TPPs and that details of ongoing consents remain accurate and current.

Further clarity is needed around scope – for example, it would be logical for the dashboard to be limited to permissions granting ongoing access rather than onetime, limited access to initiate a payment.

ASPSPs in the corporate space will need to consider the effect on their current TPP solutions. Such providers were not spared the expense of having to permit TPP access to corporate bank accounts under PSD2, and a new requirement to provide a dashboard (and potentially move to a dedicated customer interface) adds further cost and operational complexity in a sector of the industry in which TPPs have shown very little (if any) interest to date. Such providers might consider themselves better off applying to be exempted from the requirement to provide access (depending on the extent to which they might be required to permit similar access under FIDA).

10. Strong Customer Authentication (SCA)

(PSR Arts 85–89)

Overview

- The proposed PSR confirms the extent to which SCA might apply to instruction channels that may also expose the PSU to a risk of fraud (e.g. MOTO, contactless, paper-based).
- AISP access will be permitted for 180 days following the initial SCA without requiring further SCA to be performed (unless there are fraud concerns).
- SCA elements no longer need to be from different categories (i.e. it could rely on two knowledge elements).
- PSPs' SCA solutions must also cater for persons with disabilities, older persons, with low digital skills and those who do not have access to digital channels or payment instruments, by ensuring that these (and all other) customers have at their disposal at least a means, adapted to their specific situation, which enables them to perform SCA. In this regard, the performance of SCA cannot be made dependent on the possession of a smartphone. PSPs should develop a diversity of means for the application of SCA to cater for the specific situations of all their customers.
- Use of third parties to provide and verify elements will be considered outsourcing.

What is changing?

SCA elements do not necessarily need to belong to different categories (e.g. knowledge, possession, inherence), provided independence is fully preserved.

Paper-based and MOTO transactions are not inscope of SCA requirements, provided the relevant security checks and requirements that are performed by the PSP allow another form of authentication of the payment transaction to occur.

An AISP will be able to access an account for 180 days following the initial SCA without the customer needing to repeat it (unless there are fraud concerns).

Contactless payments that rely on payer proximity will be subject to SCA or 'harmonised security measures of identical effect that ensure the confidentiality, authenticity and integrity of the transaction amount and payee'.

Where technical service providers provide and verify the elements of SCA, PSPs must enter into an outsourcing agreement under which the PSP retains regulatory liability and has the right to audit and control security provisions.

Accessibility requirements require PSPs to develop 'a diversity of means' for the application of SCA to cater for the specific situations of all their customers. Non-digitally savvy/non-digital customers must have at least a means, adapted to their specific situation, which enables them to perform SCA. SCA cannot depend on access to a smartphone.

The EP Text deletes the requirement for an outsourcing agreement, referring instead to new RTS on this subject which it expects to reflect EBA guidelines.

However, the Council Text has reverted to the original Commission wording.

Separately, the EBA has recently issued a consultation on Draft Guidelines on the sound management of third-party risk (EBA/CP/2025/12).

The Council Text also proposes:

- to make orders for the creation or replacement of a token of a payment instrument via a remote channel a scenario that requires SCA (although one would imagine this is something PSPs would require in any event); and

- activation of a mobile application on a new device that can be used for payment transactions to be subject to SCA, and to the use of different communication channels to activate the mobile application on a new device, if done remotely. In such circumstances, the PSP will be required to impose a delay of 4-12 hours for the activation of the mobile application to take effect (although the PSU can opt out of this delay subject, again, to SCA).

What is the impact?

Technical service providers are unlikely to want to be considered outsourced service providers, a status which brings with it regulators' rights of access and audit (and increased regulatory scrutiny) despite requiring regulatory responsibility to stay with the PSP.

Firms that currently rely on non-electronic payment instructions to remain outside the scope of SCA requirements will have to consider/review their approach to customer authorisation of those instructions to ensure they are sufficiently secure.

Firms will also need to consider the extent to which they comply with "accessibility" requirements in terms of their SCA solution.

Firms may also need to consider their processes for activation of new devices.

11. Confirmation of Payee

(PSR Arts 50 & 57)

Overview

- PSPs must implement a confirmation of payee service and notify PSUs of any discrepancy between the payee's unique identifier and the payee's name as provided by the PSU, and the degree of such discrepancy.
- Transactions can still be authorised in the event of a discrepancy and the customer can opt out of the service altogether, although the PSP is required to warn the PSU about the consequences of doing either.
- The payer's PSP will be liable to the PSU for the transaction if they do not notify their customer of any discrepancy or fail to provide the service when required to do so (and vice versa, with the payee's PSP liable to the payer's PSP if they are the reason for this failure).
- This requirement is not subject to the corporate optout; however, the 13-month period the PSU has to make a claim is.
- The requirement applies to non-electronic payment orders too where there is a realtime communication.

What is changing?

Under the Original Commission Draft, PSPs will be required to provide a confirmation of payee service free of charge to their customers that notifies the customer of any discrepancy, and the degree of such discrepancy, between a unique identifier and the payee name provided by the PSU.

PSUs can opt out of the service and opt in again at any time.

Payees' PSPs will be required to undertake verification at the request of the payer's PSP.

PSPs will be required to highlight the risks of opting out, or continuing with a transaction where there is a discrepancy, to the PSU.

The requirement applies to payment orders placed through electronic payment initiation channels and nonelectronic payment orders involving a realtime interaction between the payer and the payer's PSP.

It will not apply to transactions where the payer did not input the unique identifier and the name of the payee themselves or to instant credit transfers under the SEPA Regulation (as amended by the Instant Payments Regulation).

The existence of a discrepancy will not prevent a PSU from continuing to make a payment or undermine a PSP's ability to rely on the unique identifier provided by the payer. However, a PSP will be liable to refund the PSU for payments it authorises where the PSP has failed to notify the PSU of the discrepancy.

In such instances, the payer's PSP must refund (or explain) within 10 business days of the claim unless the PSU has opted out of using the confirmation of payee service or has behaved fraudulently.

If the payee's PSP is at fault, they will be liable to the payer's PSP.

The Council Text has opted to leverage the verification of payee requirements under the Instant Payments Regulation, which amended the SEPA Regulation and which are due to come into effect in Q3 2025, applying them to payment transactions that fall outside the scope of SEPA (e.g. e-money transactions). Under the SEPA regime, there is no ability for consumers to opt out; however, the principles of liability to the PSU (and between the PSPs) are similar.

What is the impact?

This will require ASPSPs to implement a confirmation of payee service. In the UK, the service was created by Pay.UK. If a market solution doesn't present itself, banks will be required to implement their own solutions.

The requirement is not subject to the corporate optout (although the SEPA Regulation, which the Council Text looks to, does permit a certain amount of flexibility in relation to corporate customers); however, the notification period for a claim is.

If banks operating in the corporate space want to limit their exposure to this new liability in the way they currently do for unauthorised or defective transactions, they will need to have their corporate customer agree to the change in the scope of the optout.

12. Impersonation fraud

(PSR Art 59)

Overview

- The proposed PSR seeks to make PSPs liable for authorised payments made by consumers that have been tricked into making those payments by someone impersonating the PSP.
- The EP Text proposes to extend this to payments that result from impersonation of any other relevant entity of a public or private nature. However, this has not been accepted in the Council's Text.

What is changing?

The proposed PSR is introducing a new obligation on PSPs to refund a consumer within 10 business days where the consumer is tricked into authorising a payment by a fraudster impersonating the PSP.

The consumer will not be entitled to a refund if they have been party to the fraud, or grossly negligent.

The text also requires the claimant to make a police report.

The burden of proof is on the PSP of the consumer to prove that the consumer acted fraudulently or with gross negligence.

The EP Text seeks to broaden this requirement significantly by:

- extending PSP liability to cover a wider range of impersonations (i.e. impersonation of the PSP or 'any other relevant entity of public or private nature'); and
- requiring the PSP's justification for refusing a refund to be "substantiated" and provided to the NCA.

The EP Text also seeks to expand the scope of regulation to electronic communications services providers, who will be liable to the PSP if they fail to remove the fraudulent or illegal content once notified of its existence where the consumer has, without any delay, reported the fraud to the police and notified its PSP.

The Council Text has remained closer to the Commission's original wording.

What is the impact?

The Original Commission Draft is relatively tame in comparison to the EP Text, which would increase the impact of this new PSP liability significantly. That said, it is unclear if Parliament's proposal is intended to be more limited than the scheme that has been introduced in the UK. The EP Text refers to the impersonation of entities of public or private nature. While not defined, this suggests frauds involving impersonation of individuals (e.g. romance frauds) would not be covered; however, this is an area to watch.

UK banks have been extremely vocal about the impact the UK regime will have, with challenger banks suggesting it could hit profits by as much as 10% and raising significant concerns about the moral hazard involved in this approach, effectively making banks responsible for any lapse in judgement or mistake by the PSU.

There is also considerable ambiguity about what "gross negligence" looks like in this context, and precisely where the obligation to refund falls where a fraud involves a string of payment transactions between PSPs.

The EP Text also seeks to capture "Big Tech", imposing liability on these companies where they do not act to remove scams from their platform. It's not clear how this could work in practice since the proposed PSR will not have direct application to these entities – but represents a growing desire to bring these companies within the scope of regulation.

13. Liability

(PSR Arts 54, 56, 57 & 60)

Overview

- Customers will have 13 months to claim for impersonation fraud or confirmation of payee refunds.
- All refunds payable by PSPs will be required to be repaid within 10 business days.
- Payer and payee PSPs will be liable for unauthorised transactions that have been executed in reliance on an SCA exemption.

What is changing?

The proposed PSR extends the ASPSP liability regime to cover:

- authorised payments where an ASPSP has failed to notify a discrepancy under confirmation of payee; or
- consumer claims for impersonation of PSP fraud (including where a PISP is involved).

In each case, PSPs will be required to refund or explain within 10 business days.

This timeline will also be extended to claims for unauthorised transactions where the ASPSP has reasonable grounds for suspecting fraud and therefore doesn't refund immediately. The ASPSP must refund or explain within 10 business days of a claim (previously there was no timeline).

The proposed PSR will also impose liability for unauthorised transactions where the payer's PSP/ payee's PSP applies an exemption from SCA, with the payee's PSP liable to the payer's PSP where it is the payee's PSP's exemption.

The payee/payee's PSP will be liable to a payer's PSP for loss from failure to develop or amend the systems, hardware and software that are necessary to apply SCA.

The EP Text proposes to extend:

- the scope of impersonation fraud protection to cover any loss resulting from any impersonation (not just impersonation of the PSP); and
- the 13-month long stop period currently in place for a PSU reporting unauthorised, defective transactions, and that would now also apply to authorised transactions where the ASPSP has failed to comply with confirmation of payee requirements or that result from impersonation fraud, to 18 months.

The Council Text follows the same approach as the Original Commission Draft; however, it requires a reimbursement for loss caused by failure to comply with confirmation of payee requirements to occur without undue delay.

What is the impact?

The EP Text on impersonation fraud and the deadline for making a claim to an ASPSP will increase considerably the liability which ASPSPs are exposed to.

Corporate banks will not be unaffected by these changes and will need to implement confirmation of payee services.

The corporate opt-out at least enables such banks to reduce the time period in which a customer can make a claim. However, this will need to be agreed with existing customers.

Other liability changes (PSR Arts 58 – 69)

The proposed PSR introduces liability for technical service providers and payment system operators for failure to provide the services they are under contract for regarding support of SCA that results in loss to a payee, a payee's PSP or a payer.

It also introduces obligations on electronic communication service providers to co-operate closely with PSPs and act swiftly to ensure that appropriate organisational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with the ePrivacy Directive, including with regard to calling line identification and electronic mail address.

The EP Text goes further in trying to bring tech companies within reach by:

- requiring electronic communications services providers to be subject to similar customer education/customer/alert/notice requirements as PSPs in relation to online scams;
- imposing fraud prevention obligations across the entire fraud chain in relation to having appropriate organisational and technical measures in place to safeguard the security of payments users when carrying out transactions; and
- providing that PSPs, electronic communications services providers and digital platform service providers will have in place fraud prevention and mitigation techniques to fight all fraud types (unauthorised and authorised push payment fraud). In either case, it isn't clear how such liability could be imposed on parties not authorised under PSD3. The Council Text acknowledges this difficulty, proposing that the Commission and European Board of Digital Services encourage and facilitate the creation of a voluntary code of conduct to foster cross sectoral co-operation. Despite this, it also requires electronic communication service providers to:
  - have in place measures to ensure effective co-operation with PSPs, having regard to the technical characteristics of each of their services;
  - establish dedicated communication channels with PSPs, or participate in a system for effective communication, or in an information sharing mechanism, to allow for faster and more effective sharing of any information that could be useful in the prevention and detection of fraud; and
  - take all reasonable organisational and technical measures to detect and prevent fraud within their sphere of competence, in accordance with applicable Union and national law.

We expect that both ASPSPs and tech platforms will want to engage to come up with an industry approach to addressing this issue – the former to ensure they are not solely on the hook for frauds that emerge and are disseminated through social media, the latter to ensure the resulting regime is both constructive and workable for them.

Should the Council Text's proposal for a new "fraud prevention platform" be accepted, this will be a helpful point of reference for them to do so (see "Platform for fraud prevention")

14. Surcharging

(PSR Art 28)

Overview

Under PSD2, payees were permitted to charge for instruments not covered by the IFR / state specific prohibitions provided such charges did not exceed the direct costs of the payee; however, member states had discretion to extend the prohibition on surcharging to cover such instruments.

The EP Text is seeking to change this so that a payee may not impose surcharges for any instrument, but may offer a reduction or other means for steering the customer towards a particular payment instrument.

The Council Text has not followed the EP's lead in this regard and has reverted to the Original Commission Draft.

What is the impact?

Should the Council Text be rejected in favour of the EP Text, surcharging permitted on non-consumer cards (for example) will be prohibited. Currently the position varies from member state to member state so uniformity in this regard should be welcomed in certain quarters. However, this would impact fees that are currently permitted to be charged for corporate cards.

15. Card scheme fees

(PSR Art 31a Council Text)

Overview

The Council Text seeks to deliver greater transparency over card scheme fees, requiring:

- Card scheme operators and processors to ensure their rules and fees are disclosed to acquirers in a transparent and consistent manner to allow acquirers to compare billing categories between the schemes; and
- Acquirers to provide transparency on merchant services charges applied to their business payment services users of the payment card scheme, consistent with their obligations under the IFR.

What is the impact?

Card scheme fees have been a point of focus for regulators (both EU and UK) in recent years, so it is unsurprising that this issue features in one of the drafts for the PSR.

The focus on the way fees are disclosed and their visibility is clearly intended to drive greater competition in a market with limited choice.

16. Platform for fraud prevention

(PSR Arts 59a & 83b Council Text)

Overview

The Council Text proposes a fraud prevention platform comprised of a broad and balanced mix of representatives and experts from both the public and private sectors, who have proven knowledge and experience in the field of payment services fraud.

What is the impact?

The new platform is tasked with:

- advising the Commission on developing and monitoring the implementation of legislation aimed at combatting fraud in payment services;
- making recommendations to the Commission and the European Board of Digital Services in connection with the voluntary code of conduct for electronic communications services providers; and
- sharing and analysing trends in fraud, measures to combat fraud, and ways to improve cross-border and cross-sectoral co-operation on the means of combatting fraud in the area of payment services.

17. EBA powers of intervention

(PSR Art 104)

Overview

- The EBA will have temporary intervention powers to prohibit or restrict a certain type or a specific feature of a payment service or instrument or an electronic money service or instrument where certain conditions apply.
- Any such action taken by the EBA must be reviewed at least every 3 months to see if it is still necessary.

What's the impact?

The EBA will be able to restrict or prohibit a certain product or product feature where:

- doing so addresses a significant number of PSUs or electronic money services users or a threat to the orderly functioning of the payment or electronic money markets, and the integrity of those markets or to the stability of the whole or part of these markets in the Union;
- current regulatory requirements that apply do not address the threat; and
- the relevant NCA(s) have not taken action to address the threat or, where they have, the actions do not adequately address the threat.

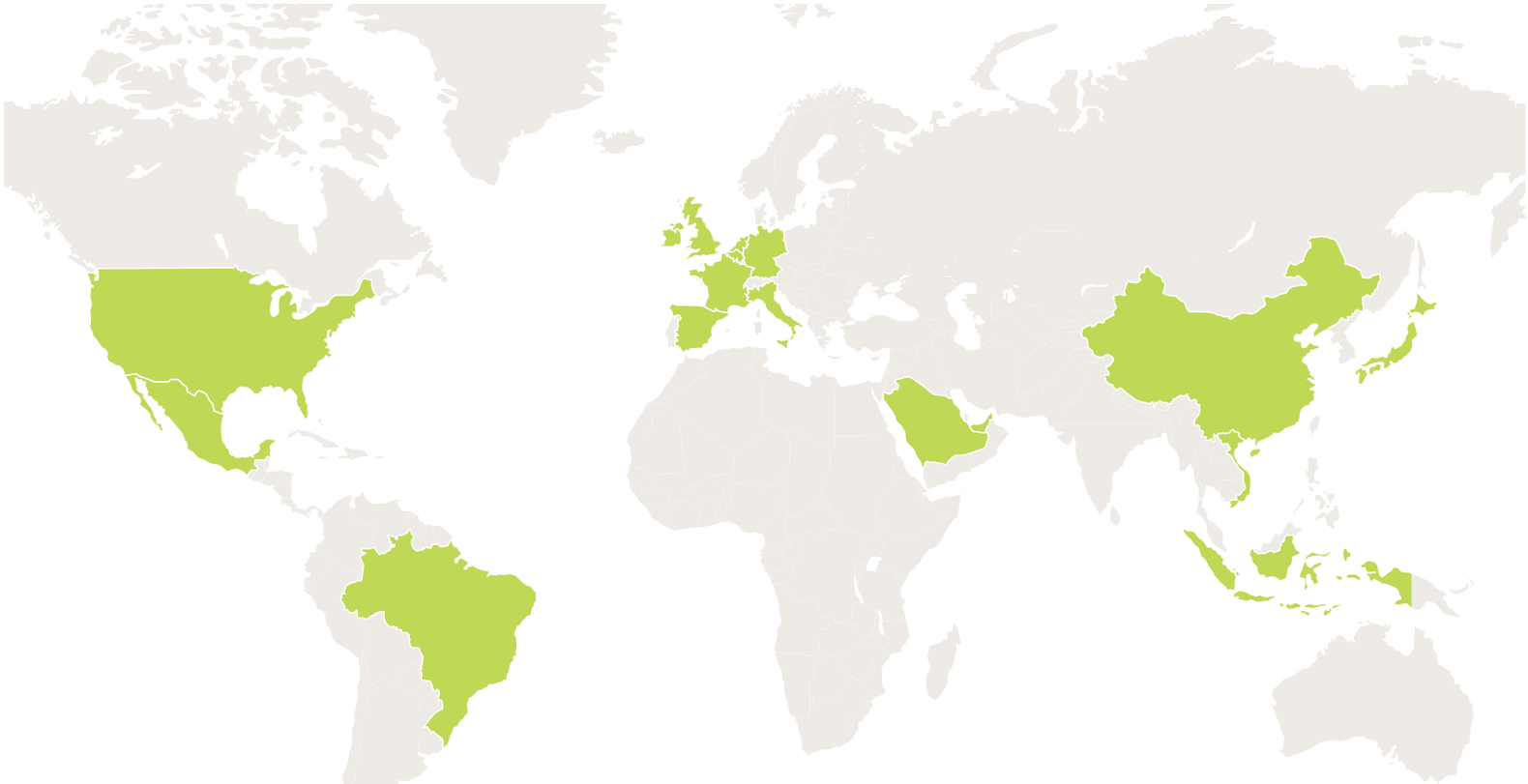
The EBA must ensure that any action:

- does not have a detrimental effect on the efficiency of the payments market or electronic money services market or on payment services or electronic money service providers that is disproportionate to the benefits of the action;
- does not create a risk of regulatory arbitrage; and
- has been taken after consulting the relevant NCA. Any prohibition or restriction must be published by the EBA on its website. In doing so, the EBA must specify when the measures will take effect. The EBA is required to review a prohibition or restriction at appropriate intervals and at least every 3 months, with the prohibition or restriction expiring if it is not renewed. The Commission will specify criteria and factors to be considered by the EBA in determining when it is right to intervene, which shall include:
  - the degree of complexity of a service or instrument and the relation to the type of users, including consumers, to whom they are offered;
  - the level of risk for consumers;
  - the possible use by fraudsters;
  - the size or the level of uptake of the service or instrument; and
  - its degree of innovation.

It will be interesting to see if this power to intervene marks the start of a more interventionist approach by the EBA (and national authorities as a result) given the speed with which digitalised payment services or products can reach scale on a cross-border basis – and the extent to which this reflects concerns that certain regulators are perceived as "light touch" in comparison to others.

18 Glossary of terms

Term	Meaning
AISP	Account information service provider
AMLR	Anti-Money Laundering Regulation (EU) 2024/1624
API	Authorised payment institution
ASPSP	Account servicing payment service provider
CASP	Crypto-asset service provider
COREPER	Committee of the Permanent Representatives of the Governments of the Member States to the European Union
Council Texts	Council of the EU's drafts of PSD3 and the accompanying PSR (June 2025)
CRD	Capital Requirements Directive 2013/36/EU
DPIA	Data Protection Impact Assessment
EBA	European Banking Authority
EMD2	Second Electronic Money Directive 2009/110/EC
EMI	Electronic money institution
EMT	Electronic money token
ePrivacy Directive	ePrivacy Directive 2002/58/EC
EP Text	European Parliament's drafts of PSD3 and the accompanying PSR (April 2024)
FIDA	European Commission's legislative proposal for a Regulation on a framework for Financial Data Access (June 2023)
GDPR	General Data Protection Regulation (EU) 2016/679
ICT	Information and communication technology
IFR	Interchange Fee Regulation (EU) 2015/751
Instant Payments Regulation	Regulation on instant credit transfers in euro (EU) 2024/886
MiCAR	Markets in Crypto-Assets Regulation (EU) 2023/1114
MOTO	Mail Order/Telephone Order transactions
NCA	National Competent Authority
Original Commission Draft	European Commission's legislative proposals for PSD3 and the accompanying PSR (June 2023)
PISP	Payment initiation service provider
PSD1	Payment Services Directive 2007/64/EC
PSD2	Second Payment Services Directive (EU) 2015/2366
PSD3	Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC
PSP	Payment service provider
PSR	Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) 1093/2010
PSU	Payment service user
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SEPA Regulation	Single Euro Payments Area Regulation (EU) 260/2012
TPP	Third party provider



Americas

- **Boston**
- **Denver**
- **Greater Washington, D.C.**
  - Baltimore
  - Washington, D.C. and Northern Virginia
- **Houston**
- **Los Angeles**
- **Miami**
- **Minneapolis**
- **New York**
- **Philadelphia**
- **Northern California**
  - San Francisco
  - Silicon Valley
- **Latin America**
  - Brazil
  - Mexico

Europe, Middle East and Africa

- **Amsterdam**
- **Brussels**
- **Dublin**
- **Germany**
  - Berlin
  - Düsseldorf
  - Frankfurt
  - Hamburg
  - Munich
- **London**
- **Luxembourg**
- **Madrid**
- **Milan**
- **Rome**
- **Paris**
- **Middle East**
  - Dubai
  - Riyadh

Asia Pacific

- **Greater China**
  - Beijing
  - Hong Kong
  - Shanghai
- **South East Asia**
  - Ho Chi Minh City
  - Jakarta
  - Singapore
- **Tokyo**

www.hoganlovells.com