

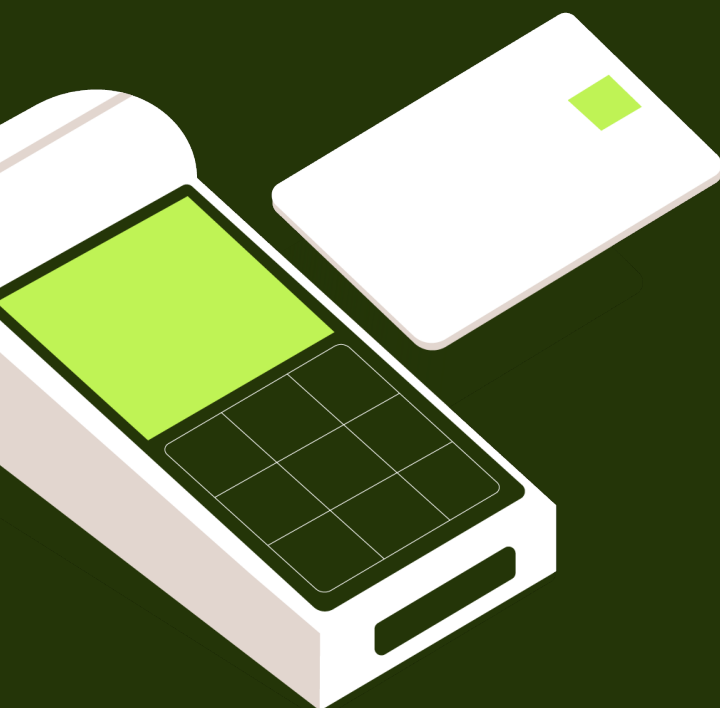


Hogan  
Lovells

# PSD3 Impacts

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Glossary of Terms</b>	<b>5</b>
<b>3</b>	<b>Legislative process to date and expected timing</b>	<b>5</b>
<b>4</b>	<b>Authorisation/Re-authorisation and changes to the E-money regime</b>	<b>6</b>
<b>5</b>	<b>Transaction Monitoring and Data Sharing</b>	<b>8</b>
<b>6</b>	<b>Scope of Application and Exemptions</b>	<b>9</b>
<b>7</b>	<b>Access for PSPs to payment systems and services</b>	<b>11</b>
<b>8</b>	<b>TPP Access</b>	<b>12</b>
<b>9</b>	<b>TPP Dashboard</b>	<b>13</b>
<b>10</b>	<b>Strong Customer Authentication (SCA)</b>	<b>14</b>
<b>11</b>	<b>Confirmation of Payee</b>	<b>16</b>
<b>12</b>	<b>Impersonation Fraud</b>	<b>18</b>
<b>13</b>	<b>Liability</b>	<b>20</b>
<b>14</b>	<b>Surcharging</b>	<b>22</b>
<b>15</b>	<b>EBA Powers of Intervention</b>	<b>23</b>



# 1 Introduction

Given the sea change of payment services directive 2015/2366 (“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.

This briefing summarises the impact of the draft proposals thematically, highlighting the areas where the dialogue 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:

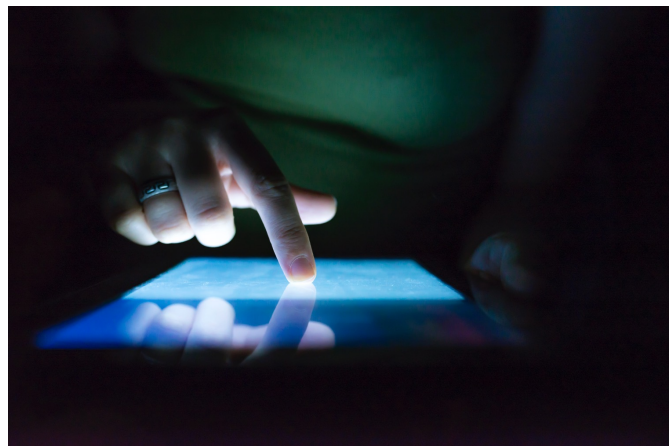
- E-money institutions will need to consider their approach to safeguarding due to the merging of the e-money and payments regimes and will have to register their distributors with regulatory authorities.
- Consumer-facing payment service providers (“PSPs”) will need to grapple with an increased liability 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 for potentially for longer than the 13-month protection first introduced under PSD1.
- Corporate-facing account servicing payment service providers (“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 payment service users (“PSUs”) are not left behind as well as third party provider (“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.



## 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.



PSD3 area of focus	Area of Impact					
	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 Communication Service Providers				✓	✓	✓
Access to payment systems/services				✓		
TPP Interface	✓	✓		✓	✓	
TPP Dashboard	✓	✓	✓	✓	✓	
SCA		✓		✓	✓	✓
Confirmation of Payee		✓	✓	✓	✓	✓
Impersonation Fraud (Consumer only)		✓	✓	✓	✓	✓
Surcharging	✓ (if it impacts financial projections)		✓		✓	
EBA Intervention	✓					



## 3 Legislative process to date and expected timing

When considering what the final text for PSD3 will look like, it is important to look at the EU legislative process.

Whilst not a rule, the Council usually reaches a general approach before the Parliament has an agreed text. As a result, the Parliament often looks at the Council general approach and bakes into its own text grounds for negotiation during trilogues.

This 'convention' was not followed during PSD3, where as a result of the European elections, the Parliament had to expedite its position to reach an agreement before the end of the mandate. Failing to reach a Parliament position carries a number of risks ranging from the file becoming a political orphan, i.e. lost in the new mandate, or that the new file takes a completely different direction as a result of a new negotiating team and composition of Parliament. As a result of this expedited process, the Parliament reached a position before the Council. What this means in practice is that the ordinary buffer that is built in is not there and as such some of the pre-cooked trilogue discussions will not have been had. It is important to note that the Council dynamic is different which is why this approach is not reciprocated.

## 2 Glossary of Terms

AISP	Account Information Service Provider
API	Authorised Payment Institution
ASPSP	Account Servicing Payment Service Provider
EBA	European Banking Authority
EMI	Electronic Money Institution
NCA	National Competent Authority
PSP	Payment Service Provider
PSU	Payment Service User
SCA	Strong Customer Authentication
TPP	Third Party Provider

At present, the Council discussions are ongoing and whilst the Hungarian Presidency was bullish about concluding PSD3, after the first two working groups it too is resigned to the reality that this may not be completed in their mandate. This is a large blow in the timeline. Poland is the next presidency and it looks as though the Polish presidency will conclude this file. If this is the case, then our estimation is that a general approach would only realistically be found in Q2 of 2025 after which trilogues can begin.

Where Parliament has not had sight of the Council text, there will be a risk that trilogues could be much longer if there are new matters that have not been discussed previously or if there are wildly different positions. Acknowledging this, we consider that in a best case scenario, there may be an H1 2025 agreement in trilogues. At present there is an 18 month implementation period (although this may be altered in trilogues) if this continues to be the case, then we can expect PSD3 to only come into effect in Q1 2027.



# 4 Authorisation/ Re-authorisation and changes to the E-money regime



## What is changing?

### *Authorisation Information (PSD3 Art 3)*

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

- a description of arrangements for the use of information and communication technology (“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.

## 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 years to demonstrate compliance with the incoming prudential requirements.

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

The European Parliament’s Text (the “EP Text”) proposes to confirm that licensed APIs/EMIs should only be required to submit additional information introduced by PSD3, and clarifies that non-compliance 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 Second Electronic Money Directive (EMD2) 2009/110/EC – 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 EBA).

### *Transition (PSD3 Art 44,45)*

APIs and EMIs will have two years 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 two-year transitional period provides a certain amount of respite in terms of time pressure – but for some EMIs, this could be a huge exercise.

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





# 5 Transaction monitoring and Data Sharing

(PSR Arts 83 and 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 Data Protection Impact Assessment (“DPIA”) between PSPs under the General Data Protection Regulation (“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 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 relationship), the minimum risk-based factors that must be considered under the monitoring system, and requires Regulatory Technical Standards 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 payment service users 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 name, personal identification number, organisation number, modus operandi and other transaction information to be shared as well.

It also proposes the EBA set 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.

## 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

### 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 draft and EP Texts seek to capture technical service providers and electronic communication service 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 7)*

PSD3 introduces a light touch registration regime for ATM deployers in the form of 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 Art 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))

Both the original draft and EP Text reveal moves to extend the scope of the payments regime to technical service providers and electronic communications service providers via indirect application.

- The Commission Text seeks to make technical service providers that provide and verify the elements of SCA outsourced service providers (and subject to audit and access rights).
- The EP Text seeks to impose obligations on electronic communications service providers in connection with impersonation fraud.

In either case, neither 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 Art 2 – 3)*

In terms of the regulatory perimeter, PSD3 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 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 Parliament proposes the addition of a new optional exemption where, for payment transactions used for the execution of trading and settlement services using e-money tokens as defined in Article 3(1), point (7) of the Markets in Crypto Assets Regulation 2023/1114 (Regulation (EU) 2023/1114) (“MiCA”), the PSP has already been authorised as a crypto-asset service provider (CASP) in a Member State for those services under Title V of MiCA.



## What is the impact?

Parties more tangentially connected to the payments world (TM 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 proposed PSR goes 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 account; and

- where the applicant presents an excessive risk profile or a disproportionately high compliance cost for the credit institution.

The proposed PSR 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, non-discriminatory 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 given on 4 months’ notice, re-introduces the need to notify an NCA of refusal/closure, and proposes EBA guidelines to specify permitted grounds for refusal.

## 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 should start thinking about what excessive risk or cost might look like.

# 8 TPP Access

(PSR Articles 35–39, 44–45)

## Overview

- Much of the Regulatory Technical Standards 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 the dedicated interface is unavailable, ASPSPs will 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.

## 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” with the requirement to offer an alternative interface without delay in the event 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.

PSPs can apply to the 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.

## 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 opt-out 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.

# 9 TPP Dashboard

(PSR Art 43)

## Overview

- ASPSPs will need to provide a customer-facing 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 opt-out.

## 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 of those consents in the ASPSP domain.

ASPSPs and TPPs will be required to cooperate 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 permission and the duration of that 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.

## 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 one-time, limited access to initiate a payment, for example.

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 under PSD2 to corporate bank accounts, 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.



# 10 Strong Customer Authentication (SCA)

(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., Mail Order/Telephone Order (commonly known as “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).
- 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, 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, inheritance) provided independence is fully preserved.

Paper-based and MOTO transactions are not in-scope 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 without the customer needing to repeat following initial SCA (unless 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 strong customer authentication. SCA cannot depend on access to a smartphone.

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

## What is the impact?

Technical service providers would unlikely want to be considered outsourced service providers, a status which brings with it the rights of access and audit to regulators (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.



# 11 Confirmation of Payee

(PSR Arts 50 and 57)



## Overview

- PSPs must implement a confirmation of payee's service and notify PSUs of any discrepancy between the payee unique identifier and the payee's name they provide, 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 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 PSP liable to the payer PSP if they are the reason for this failure)
- This requirement is not subject to the corporate opt-out; 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 real-time communication.

## What is changing?

PSPs will be required to provide a confirmation of payee service free of charge to its 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.

Payee PSPs will be required to undertake verification at the request of payer 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 non-electronic payment orders involving a real-time 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 SEPA.

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 PSP must refund (or explain) within 10 business days of the claim unless PSU has opted out of using the confirmation of payee service or has behaved fraudulently.

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



## 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 opt-out – but 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 opt-out.





# 12 Impersonation Fraud

(Article 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 goes significantly further in extending this liability to payments that result from ‘any other relevant entity of a public or private nature.’

## 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 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 relevant other 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 text also requires the claimant to submit a police report.

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



## What is the impact?

The PSR proposals are relatively tame in comparison to those of 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 being 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.

While the EP Text also increases the hoops a claimant would have to jump through to make a claim (requiring a police report), it is unclear whether this would have any serious impact on the number of claims.

The Parliament proposal 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 Articles 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 ASPSP has failed to notify discrepancy under CoP; 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 with 10 business days of claim (previously there was no timeline).

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

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

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 longstop period currently in place for a PSU reporting unauthorised, defective, 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.

## What is the impact?

The Parliament's proposals for impersonation fraud and the deadline for making a claim to an ASPSP, will increase considerably the liability which ASPSP's are exposed to.

Corporate banks will not be unaffected by these changes and will need to implement introduction 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.

In either case – it isn't clear how such liability could be imposed on parties not authorised under PSD3.

We expect 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.


## Other liability changes

### Art 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 payee, PSP payee or payer.

It also introduces obligations on e-communication service providers to co-operate closely with payment service providers and act swiftly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC, including with regard to calling line identification and electronic mail address.

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

- requiring electronic communication service 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 to have appropriate organisational and technical measures are in place to safeguard the security of payments users when making transactions; and
  - providing that PSPs, electronic communication service providers and digital platform service providers will have in place fraud prevention and mitigation techniques to fight all fraud types (non-authorised and authorised push payment fraud).
- 



# 14 Surcharging

(Article 28)

## Overview

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

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

## What is the impact?

If the EP Text is retained, 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 welcome in certain quarters. However, this would impact fees that are currently permitted to be charged for corporate cards.



# 15 EBA Powers of Intervention

(Article 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 payment services users 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:

- must 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 national competent authority.

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.

Alicante  
Amsterdam  
Baltimore  
Beijing  
Berlin  
Birmingham  
Boston  
Brussels  
Budapest\*  
Colorado Springs  
Denver  
Dubai  
Dublin  
Dusseldorf  
Frankfurt  
Hamburg  
Hanoi  
Ho Chi Minh City  
Hong Kong  
Houston  
Jakarta\*  
Johannesburg  
London  
Los Angeles  
Louisville  
Luxembourg  
Madrid  
Mexico City  
Miami  
Milan  
Minneapolis  
Monterrey  
Munich  
New York  
Northern Virginia  
Paris  
Philadelphia  
Riyadh  
Rome  
San Francisco  
São Paulo  
Shanghai  
Shanghai FTZ\*  
Silicon Valley  
Singapore  
Sydney  
Tokyo  
Warsaw  
Washington, D.C.

\*Our associated offices

[www.hoganlovells.com](http://www.hoganlovells.com)

“Hogan Lovells” or the “firm” is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses. The word “partner” is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members. For more information about Hogan Lovells, the partners and their qualifications, see [www.hoganlovells.com](http://www.hoganlovells.com). Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm. © Hogan Lovells 2024. All rights reserved. WG-REQ-1516