Council of the European Union
General Secretariat

PUBLIC

**Interinstitutional files:**
**2023/0209 (COD)**
**2023/0210 (COD)**

**Brussels, 01 July 2025**

**WK 9112/2025 INIT**

**LIMITE**

**EF**
**ECOFIN**
**CODEC**

*This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.*

**WORKING DOCUMENT**

| | |
|---|---|
| From: | General Secretariat of the Council |
| To: | Working Party on Financial Services and the Banking Union (Payment Services/ PSR/PSD)<br>Financial Services Attachés |
| Subject: | Payment services package proposals (PSD3/PSR): WP on 7 July 2025<br>- Presidency note in preparation of the first trilogue |

Danish Presidency
Council of the European Union

PUBLIC

# Working Party on Financial Services and the Banking Union

## Payment services package proposals (PSD3/PSR)

Date: 7 July 2025

Brussels, 7 July 2025

**Preparatory note for the first PSD3/R trilogue**

PUBLIC

## 1. Introduction

In June 2023, the Commission presented two proposals – the Payment Services Directive (PSD3) and Regulation (PSR). The rules aim to support consumer protection and rights as well as enhance opportunities to develop better financial products for consumers, ensuring that EU's financial sector is fit for purpose and capable of adapting to the digital transformation – including the risks and opportunities it presents.

The European Parliament (EP) agreed on initiating inter-institutional negotiations during the Plenary in April 2024. The Council adopted its mandate under the Polish Presidency on 18th of June 2025 and both institutions are as of now ready to enter the interinstitutional negotiations. The kick-off trilogue is planned for 9th of July in Strasbourg.

The aim of the Council working party on 7th of July is to prepare for the first political trilogue in which it is expected that the co-legislators will agree on the split between topics which are considered political and topics which can be delegated directly to technical level. Generally, the Presidency plans to focus the subsequent political trilogues on the key political topics while leaving technical discussions to the technical meetings. However, the Presidency are aware that some technical topics are of sensitive nature. The Presidency is hoping for Member States support regarding this approach.

This note contains a proposal for the split between the main political, secondary political and technical topics. In addition, it describes the different positions between the co-legislators on each of the identified political topics. The Presidency seeks Member States input on the proposed split and would also kindly ask Member States to already now indicate areas within the proposed political topics were flexibility can be shown.

After the first political trilogue, the Presidency intends to progress as much as possible on the technical and secondary political topics in technical meetings. This underlines the importance of delegating the relevant provisions to the technical level. Delegations will be informed after each batch of technical meetings on the progress made via 4CTs. At these occasions, the Presidency will seek Member States' input to the changes– also via 4CTs – to ensure that Member States support the direction of travel. As regards the political trilogues, the Presidency will conduct a preparatory Council working party. The agenda as well as the flash will by all means be distributed before and after each trilogue.

PUBLIC

## 2. Categorisation of topics

The Presidency has categorised topics from the two legislative proposals within a three-tier system: Main political topics, secondary political topics and technical topics.

The purpose of the categorisation is to indicate which topics the Presidency suggests treating in political trilogues, and which topics the Presidency believes could be delegated to technical level.

The categorisation follows the below stated principles:

- **Main political topics (tier 1)** are the most sensitive and potentially controversial topics in the package, and where the initial negotiating mandates of the EP and the Council differ from one another.

- **Secondary political topics (tier 2)** are topics which have the below stated nature:
  - Political topics, where the co-legislators' positions are closer to each other
  - Political topics with significant technical aspects
  - Technical topics with significant political aspects

- **Technical (tier 3)** are topics which have the below stated nature:
  - Technical topics likely to be less politically controversial.
  - Topics where co-legislators' positions to a great extent align or topics where no amendments have been made.
  - In some instances, new articles from either the EP or the Council which the Presidency would not consider necessary to handle in a political trilogue.

The Presidency suggests that tier 1 topics are dealt with in political trialogues, while tier 2 and tier 3 topics are proposed to be dealt with in coming technical meetings. In relation to this, the Presidency would like to reiterate, that technical topics can have political ramifications. A topic being initially delegated to technical level may therefore be elevated to political level at a later stage should there be a need for political guidance.

PUBLIC

## 3. Division of topics

To structure the discussion, the Presidency have divided the main political (tier 1), secondary political (tier 2), and technical topics (tier 3) into the following subjects:

- Fraud (art. 49-89, PSR)
- PSR (apart from art. 49-89)
- PSD3

## 3.1 Fraud

The Presidency propose to include five main fraud related topics for further political discussions in subsequent political trilogues: (i) the definition of authorised transactions, (ii) liability in case of impersonation fraud, (iii) role and liability of electronic communication service providers and providers of intermediary services, (iv) fraud preventive measures, and (v) gross negligence. The fraud preventive measures encompass many of the articles in the fraud section. Some of them could, if perceived as standalone articles, be delegated to technical discussions at the first trilogue. Nevertheless, the Presidency believes that fraud preventive measures encompass the core of the fraud topic and should therefore generally be perceived as part of the "fraud-package" implying that it consequently also should be treated in the same way as the remaining fraud related topics. However, the Presidency believes that the platform on combatting fraud (art. 38b), strong customer authentication (art. 85, 85a, 86, 87 and 88) as well as access and technical interoperability for payment services on mobile devices (art. 88a in EP version) could be delegated to technical meetings after the first trilogue due to the technical aspects of these topics.

The Presidency propose the following topic groupings in relation to fraud related section:

PUBLIC

| **Fraud (art. 49 to 89 PSR)**<br>(Excluding deletions of reporting requirements mentioned in the simplification topic in 3.2. PSR) | |
|---|---|
| **Main political (tier 1)** | **Secondary political (tier 2)** |
| **Definition of authorised transactions**<br>(art. 49 and 3(34a) in EP version)<br><br>**Liability for impersonation fraud**<br>(art. 59)<br><br>**Involvement of providers of electronic communication and intermediary services**<br>(art. 59(5) and 59a in Council version and art. 3(55a) in the EP version)<br><br>**Fraud preventive measures:**<br>- Verification of Payee (art. 50 (and 57))<br>- Spending limits, cooling off, blocking payment instruments, mobile phone apps (art. 51)<br>- Burden of proof (art. 55)<br>- Blocking of transactions (art. 65)<br>- Freezing of funds (art. 69(2a))<br>- Transaction monitoring and data sharing (art. 83 and 83a)<br>- Information campaigns (art. 84)<br><br>**Gross negligence**<br>(recital 82 in COM and Council versions and art. 59(5c) and recital 82a in EP version) | **Platform on combatting fraud**<br>(art. 83b)<br><br>**SCA**<br>(art. 85, 85a, 86, 87, 88)<br><br>**Access and technical interoperability for payment services on mobile devices**<br>(art. 88a in EP version) |

PUBLIC

### 3.1.1 Definition of authorised transactions (tier 1)

The **Commission** has in its proposal for art. 49(1) generally kept the definition from PSD2 with the word "*consent*" from PSD2 exchanged with the word "*permission*" in the proposal for PSR which the Commission justifies in recital 69. Further, the Commission elaborates in art. 49(5) that the permission "*shall be expressed in the form agreed between the payer and the relevant payment service provider*".

The definition of authorised transactions has been thoroughly discussed in the **Council**. The discussion ultimately concluded in following the objective approach by not including the intent of the payer in the definition, hence, keeping the definition from PSD2 – including keeping the word "*consent*" instead of "*permission*" as suggested by the Commission. Further, the Council has proposed to add a new definition of unauthorised transactions (art. 49(1a)) specifying that a transaction "*shall not be deemed as authorised where the transaction was initiated or modified by a third party who is acting without the consent of the payment service user*".

The **EP** has chosen a subjective approach where the intent of the payer is concerned. While the definition in art. 49(1) has not been amended, a new definition of authorisation has, however, been proposed in art. 3(34a). The EP suggests that for a transaction to be authorised it should be authenticated by the payment service user (PSU) and the PSU should do this "*freely and with full knowledge of all relevant facts*". In recital 79a the EP elaborates that all relevant facts include the amount, recipient and purpose of the transaction however, this list seems to be open ended. The recital further specifies that the assessment of the intention should happen in accordance with national law.

### 3.1.2 Liability for impersonation fraud (tier 1)

In recital 79 and 80 the **Commission** argues that fraud has evolved since PSD2 and that the number of 'social engineering' cases, where consumers are misled into authorising a payment transaction, has significantly increased in recent years. Consequently, the Commission believes that it is no longer possible, as was the case in PSD2, to limit refunds to unauthorised transactions only. Thus, the Commission suggests in art. 59(1) that consumers, who are victims of bank employee impersonation fraud, should be entitled to receive a full refund on the condition that the fraud has been reported to the police and notified to the PSP – unless the payer acted fraudulently or with gross negligence, cf. art. 59(3). The Commission justifies this by arguing that PSPs have more means than consumers to put an end to these fraud cases. On the other hand,, the Commission states that it would be disproportionate and financially very costly to have a systematic refund right for every fraudulent transaction – both authorised and as well as unauthorised.

The **Council** has decided to slightly amend the wording in the article from *bank employee impersonation fraud* to *bank impersonation fraud*. To ensure that the text is fit for the future, the Council has decided to delete the references as to how bank impersonation fraud is

PUBLIC

carried out. The Council has done this by not explicitly mentioning the necessity for the fraudster to specifically use the name, e-mail address or telephone number of the PSP.

The **EP** have decided to retain art. 59. However, given that the relevant transactions, where impersonation fraud has taken place would likely be deemed unauthorised according to the EPs definition of authorised in art. 3(34a), art. 59 in the EPs proposal could turn out to be redundant. No matter the approach, the EP expands the consumers refund rights, by extending them to not only cover bank employee impersonation fraud, but also impersonation of employees of any other relevant entity of a public or private nature.

### 3.1.3 Involvement of electronic communication service providers and providers of intermediary services (tier 1)

In art. 59(5) the **Commission** has included a new cooperation requirement for electronic communication services providers (ECSP's) in case of bank employee impersonation fraud (cf. art. 59(1)). The Commission proposes that when informed about this type of fraud by the PSP, the ECSP should cooperate closely 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 **Council** has decided that the obligations towards ECSPs should be expanded upon and moved to its own separate article. The Council has decided to include a new art. 59a which incorporates and expands upon the principles of art. 59(5) in the Commission's proposal. The Council has included a reference to the European Electronic Communications Code (art. 2(4), point (b), of Directive (EU) 2018/1972) to specify the actors included in the scope of the requirements. Regarding the obligation to cooperate, the Council has decided to require ECSPs, which are interpersonal communication services, to establish or participate in communication channels with PSPs to ensure effective communication. The Council has furthermore proposed a voluntary code of conduct in the context of the Digital Services Act (Regulation (EU) 2022/2065), as well as art. 59a(3) in the Council text requires that ECSPs "*shall take all reasonable organizational and technical measures to detect and prevent fraud within their sphere of competence*". Finally, the Council has also included several recitals (80, 81, 81a to 81g) which expands upon the rules and obligations applicable to ECSPs and providers of intermediary services under existing Union law.

The **EP** has in its text proposed a new definition of ECSPs (art. 3(55a). According to this new definition, ECSPs are providers within the scope of either (a) Directive (EU) 2018/1972 (European electronic communications code); or (b) Regulation (EU) 2022/2065 (Digital Services Act (DSA)). The EP has furthermore expanded upon the Commission's proposal in art. 59(5) as well as new provisions in art. 59(5a) and (5b) has been included. In 59(5) the EP has added that ECSPs should be liable towards the consumer's PSP for the full amount of a fraudulent authorised transaction "*if the electronic communications service providers do not*

PUBLIC

*remove the fraudulent or illegal content, after being informed of its occurrence*" (in recital 81 and 81a (EP version)). The EP also refers to liability of ECSPs and online platforms. Online platforms have however not been defined by the EP in PSR but are captured by the definition of ECSPs which among others include all actors within the scope of the Digital Services Act. The EP further requires ECSPs to educate their customers regarding fraud.

Lastly, in the main provisions the **EP** has included in art. 59(5b) a requirement which includes both PSPs, ECSPs and digital platform service providers. The requirements are added to have measures in place, which safeguards the security of payments as well as prevent and mitigate fraudulent transactions including non-authorised transactions and APP-fraud. In art. 84(1a)(subparagraph 2 and 3) the EP has added further requirements for both PSPs and ECSPs to "*take adequate prevention and robust technical safeguards to prevent cases where fraudsters replicate and misuse the payment service provider's name, mail address or telephone number for misleading payment service users into making fraudulent transactions*", and to "*safeguard the security and confidentiality of communications (…) including with regard to calling line identification and electronic mail address*".

**3.1.4 Fraud preventive measures (tier 1)**

The **Commission** has in its proposal included a new provision (art. 50) on verification of payee's, which has also been included in the Instant Payments Regulation (IPR). Both the **EP** and the **Council** have kept this option. However, the Council has decided to refer to the provisions of IPR (SEPA) instead, with the argument of ensuring consistency. The Commission also includes a new provision (art. 57) stating that PSPs are liable towards PSUs if the PSP fails to notify the payer of a detected discrepancy between the unique identifier and the name of the payee provided by the payer. The **EP** has generally kept this while the **Council** has adjusted the wording.

In art. 51 the **Commission** has proposed that PSPs may apply spending limits and may reserve the right to block a payment instrument. Both the **EP** and the **Council** require the PSPs to offer spending limits. The EP further requires PSPs to block payment instruments in case of objectively justified risks. The EP has also added that if the PSP fails to do so, despite reasonable grounds for suspecting fraud, the payer shall not bear any financial consequences, except where the payer has acted fraudulently. The **Council** has furthermore added requirements for installation of banking mobile phone apps as well as mandatory cooling off periods to ensure a sufficient time lag between the request to change a spending limit and until it takes effect.

Art. 55 deals with the burden of proof which the **Commission** and the **EP** proposes generally should be on the PSP however, the EP has included some requirements in art. 59(3) for cases within the remit of art. 59(1). Specifically, it is proposed that the consumer may not refuse to cooperate with the PSP in its investigation nor can the consumer refuse to provide relevant information to the PSP. The **Council** has in art. 55(3) and 59(1) included, that the

PUBLIC

PSU/consumer should provide the PSP with all the relevant information requested by the PSP, that the PSU/consumer can reasonably be expected to have.

In art. 65 the **Commission** and the **EP** have proposed the possibility to block payment orders. The **Council** has proposed to make the blocking mandatory "*where, based on the transaction monitoring referred to in Article 83 or on any other relevant information available to the payment service provider, the payer's payment service provider has duly justified and reasonable grounds to suspect that the transaction is fraudulent, the payer's payment service provider shall suspend the execution of a payment transaction.*". The **Council** and the **EP** have both added the option of freezing of funds in art. 69(2a).

In art. 83 the **Commission, the EP, and the Council** all propose an exhaustive list with some variations for data to be included in the transaction monitoring mechanism. In the **Council** version the PSP would be liable towards the PSU in case of fraud if the transaction monitoring did not take place in a specific transaction. The Commission further proposes in art. 83 that PSPs may be able to share information about the unique identifier of potential fraudsters. Both the **EP** and the **Council** has added more data which shall be shared. This is reflected in art. 83 in the EP text and in art. 83a in the Council text. The **EP** has in art. 83(5a) added that if a specific unique identifier has been reported to the PSP as fraudulent or being involved in transactions demonstrably confirmed as fraudulent the PSU should not bear any loss in case of fraud if the PSP fails to block the unique identifier.

In art. 84 the **Commission** propose that PSPs shall educate both their employees and their customers on fraud risks and trends. Both the **EP** and the **Council** have added a new paragraph specifying that also Member States have a responsibility in raising awareness regarding this topic. The EP has furthermore added that ECSPs and PSPs should cooperate free of charge with the Member States in this regard.

**3.1.5 Gross negligence (tier 1)**

Gross negligence is a core concept for allocation of liability after fraud has taken place. The concept is thus mentioned by the **Commission** with regards to both authorised, fraudulent transactions (cf. art. 59 on bank employee impersonation fraud) and in relation to transactions where the PSU denies having authorised the transaction. The Commission proposes in recital 82 a descriptive clarification for the interpretation of gross negligence aiming to ensure a more consistent understanding of the concept. The Commission argues that when assessing gross negligence, all circumstances should be taken into account. The Commission argues that gross negligence should generally be evaluated according to national law. However, to assist a more uniform understanding of the concept the Commission text explains in recital 82 that gross negligence involves conduct exhibiting a significant degree of carelessness and further provides two examples of gross negligence.

PUBLIC

In the **Council,** the discussions have aimed towards securing further guidance in recital 82 for a uniform interpretation of the concept while still respecting the discretion of national or EU courts and/or dispute resolution bodies. The Council has thus made a non-exhaustive, non-cumulative, and non-binding list of criteria which the relevant bodies can use to assess possible gross negligence. The list includes both criteria aimed at the actions of the PSU as well as the PSP.

The **EP** has also decided to make some amendments to recital 82, including two new examples and the deletion of one example from the Commission's proposal. However, the EP also proposes in recital 82a and in art. 59(5c) that "*the EBA shall issue technical guidelines (…) regarding the concept of gross negligence in the context of this Regulation and respecting the national legal frameworks on that matter*". The EP thus suggests to further harmonize the interpretation of gross negligence.

**3.1.6 Platform on combatting fraud (tier 2)**

The **Council** has added an obligation for the Commission to set up a platform on combatting fraud which should encompass the relevant entities in the fraud chain from both the public and private sector with the aim of advising the Commission and sharing information amongst one another. This obligation is not part of the **Commission's** original proposal nor the EP's proposal.

**3.1.6 Strong Customer Authentication (SCA) (tier 2)**

A few observations regarding the main differences between the **EP** and the **Council** text concerning the provisions related to strong customer authentication (SCA) would be that paragraph (3) and (4) in art. 85 has been deleted in the Council text. The Council has also decided to require the elements of SCA to be from two different categories while the EP has kept the wording from the Commission's proposal while explicitly adding that the inherence category encompasses both environmental and behavioural characteristics. The Council has furthermore included a new provision 85a on merchant-initiated transactions. Lastly, the EP has deleted art. 87 on outsourcing of SCA to technical services providers. The Presidency is not aware of the rationale of this deletion, which therefore awaits EP clarification.

**3.1.8 Access and technical interoperability for payment services on mobile devices (tier 2)**

The **EP** has included a new art. 88a describing that ECSPs and mobile device manufacturers must allow payment front-end providers fair, reasonable, and non-discriminatory access to technical features (e.g. Near Field Communication) needed for payment processing. Such providers and manufacturers shall publish general conditions of effective interoperability and access. To ensure the integrity of the hardware and software features, the providers and manufacturers may apply proportionate security measures if duly justified.

PUBLIC

**Procedural questions:**

**Question 1:** Main political topics (tier 1): Do Member States agree on the proposed identification of the above-mentioned fraud related articles as main political topics which should be further discussed in upcoming political trilogues?

**Question 2:** Secondary political topics (tier 2): Do Member States agree that the topics proposed as tier 2 can be delegated to the technical level at the kick off trilogue?

**Question 3:** Technical topics (tier 3): The Presidency believes that the remaining topics not mentioned in this note could be delegated to the technical level. Have Member States identified any additional topics currently implied as pertaining to the technical category (tier 3) as either main or secondary political topics?

**Substantial questions:**

**Question 4:** Where do Member States see room for flexibility in the Council mandate in relation to the EP's proposals for the fraud related topics?
*(Comments could be for any topic not necessarily just the main political topics. Especially comments on topics which have been discussed less in the Council would be appreciated)*

**Question 5:** Have Member States identified any main concerns with parts of the EP's proposal on fraud related items?
*(Comments could be for any topic not necessarily just the main political topics. Especially comments on topics which have been discussed less in the Council would be appreciated)*

PUBLIC

## 3.2 PSR (remaining articles)

The Presidency propose the following topic groupings in relation to the remaining articles in PSR:

| **PSR (art. 1-48 and 90-112 PSR)**<br>(including simplification topics across PSD3/R) | |
|---|---|
| **Main political (tier 1)** | **Secondary political (tier 2)** |
| **Surcharging**<br>(art. 28)<br><br>**Transparency for card schemes**<br>(art. 31a) | **Access to account: refusal grounds**<br>(art. 32)<br><br>**vIBAN**<br>(art. 32a)<br><br>**Supervisory and investigatory powers**<br>(art. 91)<br><br>**Simplification**<br>- Alignment between relevant articles of Open Banking and FIDA (Title 3, chapter 3)<br><br>- Alignment between MiCA and PSD3/PSR. (PSR EP proposal art. 2(2ha) and Council proposal art. 2.2, 3(60-63), 69(1), 70, 91(5)(d), 106, 108(1b), 108a, 110b. PSD3 EP proposal art. 34(1ca) and Council proposal art. 2(37), 3(3a), 9(1), 13(2a) and recitals 16 and 31)<br><br>- Reporting requirements (art. 81, 83, PSR) and (art. 39, PSD3)<br><br>- Number of delegated acts (across PSD3 and PSR) |

### 3.2.1 Surcharging (tier 1)

The **Commission**, in recital 52, argues that *"Evidence gathered during the review of Directive (EU) 2015/2366 shows that the current rules on charges are appropriate and had a positive impact. There is no compelling need for further alignment of charging practices between*

PUBLIC

*Member States, as the existing surcharging ban already applies to a very large share of payments in the Union"*

Art. 28(3), conclude that *"The payee shall not request charges for the use of payment instruments for which interchange fees are regulated under Chapter II of Regulation (EU) 2015/751 and for credit transfers, including instant credit transfers, and direct debit transactions within the Union."*

The **Council** has not proposed changes to art. 28.

The **EP** has expanded the ban on surcharging from the above mentioned to include all payment instruments. In effect, the new article 28(3) by the EP reads: *"The payee shall not request charges for the use of payment"*. This also leads the EP to delete the Member State option to expand the limit on surcharging to additional payment instruments. In addition, the EP has included an obligation in art. 28(3a) for regulated ATM operators to provide information on any fixed fees.

**3.2.2 Transparency for card schemes (tier 1)**

The **Council** has introduced a new article 31a(i) concerning transparency requirements on card schemes and processing entities' rules and fees, hence introducing some minimum requirements for hitherto unregulated part of the payment eco-system. In addition, article 31a(ii) introduce similar transparency requirements for acquirers towards their merchant clients.

Neither the **Commission** nor the **EP** have introduced similar articles.

**3.2.3 Access to account: refusal grounds (tier 2)**

The **Commission,** in recital 35, states, that *"Payment institutions need to be able to open and maintain an account with a credit institution to meet their licensing requirements as regards safeguarding of customer funds."* In recital 36, the Commission furthermore adds that *"Credit institutions should therefore provide a payment account to payment institutions, and to applicants for a license as a payment institution, as well as to their agents and distributors, except in exceptional cases where there are serious grounds to refuse access."*

Both the **EP** and the **Council** have deleted and added multiple parts of the article, with several alterations being aligned while others are not. E.g., the **EP** has deleted art. 32(1)(e), while the **Council** deleted art. 32(1)(d)-(e). In addition, the EP has also included a refusal ground tied to national competent authorities' refusal to grant a payment institution license.

**3.2.4 Virtual IBAN (tier 2)**

The **Council** has introduced a new article 32a, that introduces a definition of what constitutes a virtual IBAN and elaborates that a virtual IBAN is to be considered as an IBAN under the

PUBLIC

SEPA regulation. Furthermore, the Council has introduced a review clause in art. 108(1a) to decide whether further legislative measures are necessary.

Neither the **Commission** nor the **EP** have introduced similar articles.

**3.2.5 Supervisory and investigatory powers (tier 2)**

The **Commission** does in art. 91 seek to ensure that competent authorities have the appropriate powers at their disposal to enforce the regulation.

The **EP** has made no amendments to the Commission's proposal for art. 91.

The **Council** on the other hand has made numerous amendments to the article. In particular, the Council has changed art. 91(3) (article 91(5), Council text) from being exhaustive to non-exhaustive. Moreover, the Council has introduced 18 additional paragraphs to the article to support the understanding of the supervisory and investigatory powers.

**3.2.6 Simplifications (tier 2)**

- *Alignment between relevant articles of Open Banking and FIDA*

Regarding the interplay with the regulation on access to financial data (FIDA), the **Commission** in recital 55, is primarily concerned with remuneration aspects of data access. This as data access through open banking will be free of charge to the third-party providers, while remuneration is envisioned for access to data other than payment data from payment accounts. Specifically on the permission dashboard, the **Commission** argues on open banking, that the envisioned permission dashboard shall *"enable open banking users to manage their open banking permissions in a convenient way, ASPSPs are required to offer them a "dashboard" allowing the withdrawal of data access from any given open banking provider."*

The **Council** has in art. 43(2)(e) on data access management added that the dashboard should *"be consistent with the Regulation (EU) [..../....] of the European Parliament and of the Council [FIDA] dashboards and allow payment service users to manage data permissions pursuant to this Regulation and [FIDA] through a single dashboard."*

Likewise, the **EP** has in article 43(2)(da) added that the dashboard shall *"be consistent with the FIDA dashboards and allow data holders to manage data permissions stemming from both that Regulation and this Regulation through a single dashboard upon the request of the user."*

- *Alignment between MiCA and PSD3/PSR*

The entry into force of the Markets in Crypto-Assets Regulation (MiCA), combined with the classification of electronic money tokens (EMTs) as "funds" under MiCA, has introduced a regulatory overlap with the existing framework under PSD2. As a result, entities that issue or handle EMTs must now potentially obtain both a MiCA license and separate authorisation as

PUBLIC

a payment institution under PSD2. The **Commission** did not address these regulatory frictions in its initial proposals for PSR/PSD3.

To address the growing convergence between MiCA and PSD3/R, the **Council** has introduced several amendments to PSD3 and PSR to harmonise the two frameworks. In the PSR, the Council introduced definitions aligned with MiCA of EMTs, crypto-asset service providers (CASPs), self-hosted addresses, custodial wallets in article 3(60–63). The Council further aligned supervisory powers with MiCA and the FiDA, empowering national competent authorities (NCAs) to take extensive enforcement actions in article 91(5(d). Importantly, the Council amended MiCA via Article 110b to permit PSD-licensed payment institutions to offer EMT services equivalent to their licensed payment services through a simple 40-day notification procedure to competent authorities. In PSD3, the Council has introduced a definition of "electronic money token" (Art. 2(37), Recital 16), aligned with MiCA, ensuring that references to electronic money also cover EMTs unless explicitly excluded. CASPs providing payment services in EMTs has been brought within the scope of PSD through recitals 16, 31, and article 3(3a). Article 3(3a) provides a tailored and exhaustive list of documentation for CASP's under PSD3 to prevent duplication with information already submitted under MiCA. Safeguarding obligations in article 9(1) for EMT issuers are excepted from PSD3, deferring instead to the safeguarding obligations in MiCA article 54. In article 13(2a) the deadline for NCAs to process applications from MiCA-licensed entities is set to 60 days.

The **EP** has likewise sought to mitigate regulatory duplication. In PSR, article 2(2)(ha), is introducing an exemption for EMTs trading and settlement transactions carried out by MiCA-regulated entities. This measure seeks to avoid dual compliance obligations for CASPs already subject to comprehensive supervision under MiCA. In PSD3, the EP has proposed article 34(1)(ca)) that allows Member States to exempt MiCA-authorised CASPs from most PSD licensing and supervision obligations when providing trading and settlement services with EMTs.

- *Reporting requirements*

Several reporting requirements are included in the PSR and PSD3. As a result of a non-paper from a Member State concerning this topic, the **Council** decided to delete such requirements from article 81(1)(subparagraph 3) regarding operational and security risks as well as article 83(5) regarding participation in information sharing arrangements. Lastly, the notification duty in art. 39, PSD, has been made voluntary for Member States to implement.

- *Number of level 2/3 mandates*

During the negotiations in the Council several Member States have indicated that the proposal for PSD3/PSR contains a high number of delegated acts or guidelines, and some have indicated that they are not willing to support any new level 2 or 3 mandates. Further,

PUBLIC

before the Financial Services Committee (FSC) meeting in June 2025 the **Commission services** shared a non-paper on the number of level 2 mandates which they argue is a concern for stakeholders and carries a compliance cost for the industry. Of the 430 level 2 empowerments adopted in the financial services area in the last legislative cycle the Commission services had identified a preliminary list for discussion of 122 acts where they believed the adoption could be postponed.

The Presidency has identified the following mandates (RTS, ITS, delegated acts, guidelines in the **Commission's** proposal: **PSR**: art. 2(7), 2(8), 32(5), 39(2), 48(8), 82(2), 82(3), 84(3), 89(1)(a to g), 91(6), 104(8). **PSD3**: art. 3(5)(a to d), 7(6), 9(7), 13(1), 18(5), 18(6), 30(5), 31(5), 40.

The **Council** has added a new RTS in **PSR**: art. 16(2) and 31(1a), 32(7)(subpara 2 and 3), 38(2)(a and b), added further context to 39(2), 85a, and 105(2). **PSD3**: some further context to art. 9(7), PSD3, and has added a new mandate in art. 36(4a)(a to d).

The **EP** has added references to new mandates in **PSR**: art. 3, added context in art. 32(5), 43(2a), 59(5c), added context in 89(1) as well as added three new points to the list in 89(1)(ga to gc).

PUBLIC

**Procedural questions:**

**Question 6:** Main political topics (tier 1): Do Member States agree on the proposed identification of the above-mentioned articles as main political topics which should be further discussed in an upcoming political trilogue?

**Question 7:** Secondary political topics (tier 2): Do Member States agree that the topics proposed in this section as tier 2 can be delegated to the technical level at the kick off trilogue?

**Question 8:** Technical topics (tier 3): The Presidency believes that the remaining topics not mentioned in this note could be delegated to the technical level. Have Member States identified any additional topics currently implied as pertaining to the technical category (tier 3) as either main or secondary political topics?

**Substantial questions:**

**Question 9**: Considering the simplification agenda more generally the Presidency would like to ask Member States if they have concerns regarding the number of level 2 mandates in PSD3/PSR and if so, if there are specific level 2 mandates Member States consider redundant?

**Question 10:** Where do Member States see room for flexibility in the Council mandate in relation to the EP's proposals for the topics in PSR (apart from fraud)?
*(Comments could be for any topic not necessarily just the main political topics. Especially comments on topics which have been discussed less in the Council would be appreciated)*

**Question 11:** Have Member States identified any main concerns with parts of the EP's proposal on non-fraud related items?
*(Comments could be for any topic not necessarily just the main political topics. Especially comments on topics which have been discussed less in the Council would be appreciated)*

PUBLIC

## 3.3 PSD3

The preliminary list of topic groupings for the topics under PSD3 are as follows:

| **PSD3**<br>(excluding targeted amendments to better align MiCA with PSD3/PSR which is included under the simplification topic) | |
|---|---|
| **Main political (tier 1)** | **Secondary political (tier 2)** |
| | **Definition of agents**<br>(Recital 45, art. 2(28), and art. 19)<br><br>**Safeguarding**<br>(art. 9) |

### 3.3.1 Definition of agents (tier 2)

The definition and regulation of agents acting on behalf of payment institutions is important because it directly affects consumer protection, market integrity, and regulatory oversight. Clear regulation ensures that agents act within a well-defined legal framework and under the responsibility of the licensed institution, thereby reducing risks such as fraud, money laundering, and operational failures.

The **Commission** has, in its PSD3 proposal for recital 45, elaborated on how payment institutions may expand their services, including via agents and distributors, which must act transparently and inform end users that they are acting on behalf of a payment institution. The Commission has generally kept the same definition of agents in article 2(28) as in PSD2, while adding a new definition of distributors. Article 19 introduces more detailed obligations for payment institutions intending to operate through agents. These include providing competent authorities with information about the agent's identity, internal controls, and management, and demonstrating the fitness and propriety of responsible persons. Agents may only begin operations once registered. Any change in agent use must be reported without undue delay. The same rules apply with the relevant modifications to distributors of electronic money services under Article 20.

The **Council** has introduced several key changes to the definition and regulatory treatment of agents and distributors in PSD3, aiming to establish a clearer legal framework to mitigate operational and compliance risks. These changes respond to intense discussions within the Council, particularly around the borderline between agents and other third parties. The Council has elaborated on the definition of agents in article 2(28), while the definition of distributors had been deleted. To further clarify who qualifies as an agent, the Council

PUBLIC

introduces article 18a stating that a person may only be considered an agent if they either (a) enter into possession of funds on behalf of the institution, or (b) are directly involved in the provision of payment services. This narrows the scope and prevents broad or ambiguous application of the agent concept. Regarding electronic money services, recital 45 and Article 20 clarify that entities merely distributing or redeeming e-money, are not considered agents if they do not perform actual payment services. The Council also prohibits agents from issuing e-money, though they may redeem it on behalf of the institution.

The **EP** largely follows the Commission's approach, making no changes to the definitions of agents or distributors in Articles 2(28) and 2(36), and keeping Articles 19 and 20 largely intact. However, new recitals (45a) and (45b) introduce clarifications, as agents acting for acquirers do so only on behalf of one acquirer, not for all services to the user; and marketplaces or platforms that do not control or hold funds should not automatically be classified as agents.

**3.3.2 Safeguarding (tier 2)**

Safeguarding is essential to protect users' funds in case a payment institution fails financially. It reduces consumer risk and helps maintain trust in the payment system.

The **Commission** proposes harmonised safeguarding rules under Article 9, requiring payment institutions and e-money providers to segregate or insure customer funds. Funds must be deposited in separate accounts or invested in secure, low-risk assets if not transferred within one business day. Institutions must avoid concentration risk by not relying on a single safeguarding method or provider. For mixed-purpose funds, safeguarding applies proportionally. The proposal also sets a deadline for safeguarding e-money funds and introduces stricter asset quality rules. The EBA is tasked with developing regulatory technical standards to further detail risk management and segregation procedures.

The **Council** proposal builds on the Commission's safeguarding framework but adds key clarifications and new provisions. Most notably, the Council introduces a requirement for payment institutions to inform users which Member State's insolvency law and courts apply in case of insolvency (Article 9(1)). It also adds Article 9(1a), allowing funds held in settlement accounts with designated payment systems to be considered safeguarded if properly insulated. Additionally, the Council permits safeguarding via post office giro institutions under specific conditions (Article 9(1)). The Council also expands the EBA's mandate in Article 9(7) to include reconciliation of funds in settlement accounts. These additions aim to enhance transparency, operational flexibility, and user protection in insolvency scenarios.

The **EP's** position on safeguarding largely aligns with the Commission's proposal but introduces two key additions. First, it emphasizes the need for payment institutions to have the option to safeguard users' funds at central banks. If a central bank refuses this, it must justify the decision to the institution. Second, the EP highlights the risk that credit institutions may refuse or terminate accounts for payment institutions, which undermines diversification.

PUBLIC

Therefore, credit institutions should be required to provide a justified explanation when doing so. The EP also adds to article 9(2), that the obligation to avoid concentration risk should apply "where appropriate" and expands the EBA's mandate in article 9(7).

**Procedural questions:**

**Question 12:** Main political topics (tier 1): Do Member States agree on the proposed identification of no articles in PSD3 as main political topics?

**Question 13:** Secondary political topics (tier 2): Do Member States agree that the topics proposed as tier 2 can be delegated to the technical level at the kick off trilogue?

**Question 14:** Technical topics (tier 3): The Presidency believes that the remaining topics not mentioned in the note could be delegated to the technical level. Have Member States identified any additional topics currently implied as pertaining to the technical category (tier 3) as either main or secondary political topics?

**Substantial questions:**

**Question 15:** Where do Member States see room for flexibility in the Council mandate in relation to the EP's proposals for the topics in PSD3?
*(Comments could be for any topic not necessarily just the main political topics. Especially comments on topics which have been discussed less in the Council would be appreciated*)

**Question 16:** Have Member States identified any main concerns with parts of the EP's proposal on PSD3?
*(Comments could be for any topic not necessarily just the main political topics. Especially comments on topics which have been discussed less in the Council would be appreciated)*