Council of the European Union
General Secretariat

PUBLIC

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

Brussels, 11 November 2025

WK 15277/2025 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:	Presidency
To:	Working Party on Financial Services and the Banking Union (Payment Services/ PSR/PSD) Financial Services Attachés
Subject:	Working Party on Financial Services and the Banking Union (PSD/PSR) 17.11.25 - Preparatory note for the Political trilogue on the 26th of November: Other fraud related topics (Article 49 to 89)

Danish Presidency
Council of the European Union

PUBLIC

Working Party on Financial Services and the Banking Union

Payment services package proposals (PSD3/PSR)

Date: 17 November 2025

Brussels, 17 November 2025

Preparatory note for the Political trilogue on the 26th of November: Other fraud related topics (Article 49 to 89)

PUBLIC

1. Introduction

This note treats outstanding topics other fraud related topics. These topics are not expected to be discussed at the political trilogue on 26 November, but will be further discussed at technical level. The note is divided into different topics including alignment between Article 56 and Article 60 regarding liability for unauthorised transactions and SCA.

2. Strong Customer Authentication (SCA) (Article 85)

For the articles related to strong customer authentication there are still three remaining issues. **First**, regarding whether SCA should be applied when accessing payment account information (online) in Article 85(1)(b) and through AISPs in Article 86(4). Both of which the EP has suggested to delete. The **second** issues concern the inherence category in Article 85(12). Generally, the EP has been open to the Council's arguments regarding SCA. However, the EP has flagged the issues treated in this note as important to them. In the Council working parties the EP's amendments regarding SCA have earlier been rejected. Consequently, the Presidency would like to present the following compromise proposals which hopefully address some of the concerns of the Member States.

3.1 SCA in case of accessing payment account information

The EP believes that SCA should not be necessary when accessing payment account information. The EP has generally preferred a more risk-based approach and do not find that the risk level involved justifies mandatory SCA. The Presidency has put forward the argument that payment account information could potentially be used by fraudsters to convince their victim that they are from their PSP. Therefore, SCA is appropriate in such situation.

The Presidency would like to point out that in Article 97 of PSD2[1] accessing account information was not on the list for mandatory SCA. Furthermore, in the RTS on SCA[2] it is explicitly mentioned in Article 10 that when a PSU is limited to only accessing the balance of a payment account or transactions executed within the last 90 days SCA is not mandatory. Two further exceptions are also included. Thus, Article 10(2) of the RTS specifies that SCA

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389

PUBLIC

shall only be mandatory where the PSU is accessing the information for the first time or where the PSU has not made access to the information within the last 90 days.

Article 10 in the RTS on SCA:

"1. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 and to paragraph 2 of this Article and, where a payment service user is limited to accessing either or both of the following items online without disclosure of sensitive payment data:

(a) the balance of one or more designated payment accounts;

(b) the payment transactions executed in the last 90 days through one or more designated payment accounts.

2. For the purpose of paragraph 1, payment service providers shall not be exempted from the application of strong customer authentication where either of the following condition is met:

(a) the payment service user is accessing online the information specified in paragraph 1 for the first time;

(b) more than 90 days have elapsed since the last time the payment service user accessed online the information specified in paragraph 1(b) and strong customer authentication was applied."

In this regard, it seems like the EP text is closer to the current state of play, where the EBA would still be able to identify specific situations where SCA could be mandatory when accessing payment account information. On the other hand, the Commission and Council text would be stricter than today by requiring SCA every single time a PSU is accessing payment account information.

Thus, the Presidency would like to ask whether Member States could show flexibility towards the EP's position. The Presidency believes that there are three possible ways to handle this:

1. **By deleting the requirement** to perform SCA when accessing account information online. In this case the EBA would probably include a similar article in the new RTS in SCA as the one above in Article 10 of the current RTS.

PUBLIC

2. **Inserting the text from Article 10 of the current RTS into level 1.** In this case the Presidency would ask Member States if the text should be amended.

3. The third option would be **not to show flexibility**. In this case Member States are encouraged to provide arguments as to why SCA should now be necessary every time a PSU accesses account information online.

The Presidency does notice that exemptions from SCA is generally defined at level 2, cf. Article 89(1)(b). Therefore, the Presidency believes that if flexibility can be shown, the preferred option would be *option 1.*

The EP has on a similar background deleted Article 86(4) which requires AISPs to apply their own SCA every 180 days. Article 86(3) has, however, been kept. Here, account servicing PSPs are required to apply SCA for the first access to payment account data by each AISP.

3.2 Inherence

The EP and Council differ on **two amendments** to the inherence category:

1) Whether two elements from the same category can be used (Article 85(12) – line 902)

Here, the Presidency has argued that the use of two elements from the same category constitutes a security concern. While Article 85(12) specifies that the elements must be independent, Member States have earlier argued that two elements from the same category are not as independent from each other as two elements from different categories. The Presidency has convinced the EP that for at least the knowledge and possession categories, it should not be possible to use two elements from the same category. Hence, the inherence category is still a point for discussion. Consequently, the Presidency would like to test a compromise with Member States. The compromise would allow for two elements from the inherence category, only if the PSP demonstrates to the NCA that the independence of the elements is fully preserved thus keeping a high level of security.

The drafting suggestion for the compromise is provided in the table below.

PUBLIC

Article 85(12)(subparagraph 1) (line 902)
Compromise drafting suggestion in **red**

"*The two or more elements referred to in Article 3, point (35), on which strong customer authentication shall be based* ~~***do not necessarily***~~ *need to belong to different categories,* ~~***as long as their independence is fully preserved***~~ ***except from the category inherence, where a payment service provider can implement strong customer authentication using two elements only from this category, if it demonstrates to the national competent authority that the independence of the elements is at all times fully preserved and the authentication procedure ensures at all times a high level of security****."*

2) Whether environmental and behavioural elements can be considered as inherence (Article 85(12)(subparagraph 2) – line 902a)

The EP has suggested that also environmental and behavioural elements can be considered as inherence. The Presidency has argued that this is very problematic, especially regarding the environmental aspect. Since the environmental elements could also be a part of the transaction monitoring mechanism (TMM) it could lead to the exact same information being used for the purpose of TMM as well as an element of SCA. If the same information is used both places, it would mean that transactions would be less secure than today. By allowing one element of SCA to duplicate information already included in the TMM, SCA would *de facto* be reduced to only one element.

The Presidency would thus like to propose a compromise drafting where only behaviour, but not environment, can be considered as inherence:

Article 85(12)(subparagraph2) (line 902a)
Compromise drafting suggestion in **red**

"The category inherence of strong customer authentication relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these. It does not include environmental characteristics such as the location of the payment service user, the time when the transaction occurs or the device being used."

PUBLIC

Q1: In case of accessing payment account information (Article 85(1)(b)) which of the three options presented by the Presidency can Member States support?

Q2: Can Member States show flexibility toward the EP's deletion of the requirement for AISP's to apply their own SCA once every six months (Article 86(4))?

Q3: Can Member States show flexibility towards the Presidency's proposed compromise with regard to using two elements from the inherence category only if approved by the NCA (Article 85(12)(subparagraph 1)?

Q4: Can Member States show flexibility towards the EP with regard to explicitly allowing for behavioural elements to be included in inherence (Article 85(12)(subparagraph 2)?

3. Liability for unauthorised transactions (Article 56 (and interplay with Article 60) – line 697, 698, 699, 725, and 729)

Regarding Article 56 one Member State has expressed strong concerns with the divergent interpretations of the refund framework for unauthorised transactions. Under PSD2 a refund to the PSU would have to be made within one business day according to Article 73 of PSD2 "(…) *except where the payer's payment service provider has reasonable grounds for suspecting fraud (…)*" (Article 73(1) of PSD2).

However, Article 74 of PSD2 clarifies that a final rejection of a claim can also be made on the grounds of the payer failing with intent or gross negligence to fulfill its obligations set out in Article 69 of PSD2 (regarding the obligations of the payment service user in relation to payment instruments and personalised security credentials). In this case the payer would bear all of the liability:

"*The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 69 with intent or gross negligence. In such cases, the maximum amount referred to in the first subparagraph shall not apply*." (Article (1)(subparagraph 3) of PSD2)

After this initial refund is made, the PSP then has an undefined amount of time to assess whether the PSU acted fraudulently or with gross negligence. If the PSU did so, the PSP could

PUBLIC

then reclaim the refunded amount. However, divergences exist as to how this reclaiming should take place in practice. The two diverging interpretations are:

1) **The PSP will have to apply to the courts** to get the funds back if the PSU denies paying the PSP back. This comes from the preliminary reference that has been raised by a Polish Court (C-70/25 [Tukowiecka]) before the CJEU regarding the interpretation of Article 73 and 74 PSD2. Summed up, the Polish judge states that such rules should be interpreted so that, where the PSP has refunded an unauthorised transaction and then has reason to believe that it occurred due to the user's gross negligence or intent, the PSP should explain these reasons to the user. The PSP should then request the repayment of the reimbursed amount. If the PSU does not voluntarily return the amount, the PSP would be required to take legal action before court against them, as it is assumed that it cannot in any case unilaterally debit the payment account.

2) **The PSP can collect the funds directly from the PSUs account** if the PSU denies paying the PSP back. This approach is included in the EBA Q&A[3] n. 223 on the interpretation of PSD, according to which: "*Once the payer has been reimbursed, the payment service provider will then have the time necessary to look for evidence, (…) (e.g. if after its search for proof, the payment service provider finds evidence showing that the payer failed to keep the personalised security features of the payment instrument safe, the payment service provider would be able to debit the amount mentioned in Article 61(1) from the payer's account)"* (please see (3) in the answer to question 223 in the EBA Q&A).

Having these two very different approaches co-exist goes against a uniform interpretation. In PSR a similar system has been set up with the exception that a specific timeline has been added in Article 56 (which corresponds to Article 73 of PSD2). In the current draft of PSR, the PSP would have one day to refund the payer unless there is a suspicion of the payer acting fraudulently. If so, the PSP would then have 15 days to investigate whether their suspicions were reasonable. This time period is only included for the PSP to investigate whether the payer acted fraudulently or not. However, the investigatory time period in Article 56 does not include the other rejection reasons included in Article 60(1)(subparagraph 3) (which corresponds to Article 74(1)(subparagraph 3) of PSD2), which concern whether the payer failed to "*fulfil one or more of the obligations set out in Article 52 with intent or gross*

[3] https://finance.ec.europa.eu/system/files/2023-06/110222-faq-transposition-psd_en.pdf

PUBLIC

negligence". Article 52 specifies the obligations of the payment service user in relation to payment instruments and personalised security credential.

As such, the Presidency believe that a system where there would be a limited time period for investigating whether the payer acted fraudulently under Article 56 would be created. On the other hand, there would be an indefinite time period for investigating whether the payer failed to fulfil one or more of the obligations set out in Article 52 with intent or gross negligence.

The Presidency believes that it is not consumer friendly to have such uncertainty for the PSU. Thus, the Presidency suggests including in Article 56 references to intent and gross negligence in relation to the PSU's obligations in Article 52.

This would mean that the PSP could make an initial rejection based on a suspicion of intent or gross negligence on top of the existing initial refusal ground of fraudulent behaviour. However, this would also limit the investigation time for PSPs with regard to intent and gross negligence from indefinite to 15 days.

This approach would be beneficial both for the PSU and for the PSP. From the PSU's perspective, they would have a prompt and definitive answer in relation to their refund request. Under the current PSR text the PSU has no certainty about how and when the refusal grounds described in Article 60 can be claimed by the PSP to exclude the right of refund. Moreover, setting a final deadline within which the final decision should be made would protect the PSU from the scenario. Without such a deadline, the PSP could, even a long time after the reimbursement, debit the PSUs account or bring the matter to the court in order to reclaim the amount of the transaction. Neither of these actions would be very consumer friendly, especially if the PSP only acts after having acquired evidence of the intent or gross negligence.

Again, it is important to notice that this does not limit liability of PSPs but solely serve the purpose of protecting PSUs from later being debited the amount or being sued for the amount by their PSP.

The Presidency thus suggests the following amendments to Article 56 (line 697, 698, and 699):

PUBLIC

Article 56 (line 697, 698 and 699)
Compromise drafting suggestion in **red**

"1.Without prejudice to Article 54, in the case of an unauthorised payment transaction, the payer's payment service provider shall refund the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the unauthorised transaction, except where the payer's payment service provider has reasonable grounds for suspecting ~~*fraud committed by the payer*~~ *that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52 and communicates those grounds to the relevant national authority in writing.*

2.Where the payer's payment service provider had reasonable grounds for suspecting ~~*fraud committed by the payer*~~*that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52, the payer's payment service provider shall, within* ~~*10*~~*15 business days after noting or being notified of the transaction, do either of the following:*

(a) refund the payer the amount of the unauthorised payment transaction if the payer's payment service provider has concluded, after further investigation, that ~~*no fraud has been committed by*~~ *the payer did not act fraudulently or fail with intent or gross negligence to fulfil one or more of the obligations under Article 52;"*

Q5: Can Member States support the proposed drafting suggestion regarding alignment between Article 56 and Article 60?

4. Other topics

The Presidency invites Member States to share if they have any strong concerns at this point in relation to topics within Article 49 to 89, which has not been covered by the discussion notes for this Council working party.

The Presidency notes that some Member States have commented on the drafting in Article 83 (line 863c). Here, the Presidency notes that its reading of the original proposal from the Council in line 863c was that it would cover both the payer's and the payee's PSP since both of those PSPs are obliged to carry out transaction monitoring cf. line 863a. Since no reference was made to the **payer's PSP** in line 863c but it simply states that **the PSP** shall be liable for not conducting transaction monitoring this was assumed to refer to both PSPs. However,

PUBLIC

some Member States have pointed out in the 4CT that they believe the liability proposed by the Council only covers the payer's PSP and if any further liability is to be imposed it should be discussed in the Council. Consequently, the Presidency would like to ask Member States whether they support that the liability in line 863c covers also the payee's PSP where it does not conduct transaction monitoring in a specific transaction and as a consequence thereof someone is defrauded.

Some Member States have also commented on the sharing of burdens. At the ITMs it was discussed how the PSU should be informed about whether the payee's PSP also conducted transaction monitoring. Here, we concluded that it would be more straightforward for the PSU if their PSP provided the statements from both itself and from the payee's PSP and that a refund only goes through the PSUs own PSP. The payer's PSP should not be required to assess the explanation from the payee's PSP but could just forward this explanation from the payee's PSP to the PSU as part of a final statement including the explanations from both PSPs. Should the payee's PSP not have conducted transaction monitoring, the payer's PSP would then reimburse their PSU, and through the amendment Article 78 (line 835), the payer's PSP would now be entitled to compensation from the payee's PSP. It was decided that it was not necessary to explicitly mention that the payee's PSP need to respond to an inquiry from the payer's PSP since if the payee's PSP fails to provide the explanation and the PSU is entitled to a reimbursement for that reason, then the payer's PSP would still get compensated by the payee's PSP through Article 78. Thus, the payee's PSP has all incentives to provide its account of the transaction to the payer's PSP.

Q6: Can Member States support that liability for not conducting transaction monitoring also covers the payee's PSP, cf. line 863a?

Q7: The Presidency invites Member States to share if they have very strong concerns with particular elements of the fraud related articles in Article 49 to 89.