Council of the European Union
General Secretariat

PUBLIC

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

Brussels, 13 November 2025

WK 15443/2025 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) 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: Authorisation, impersonation fraud and blocking of transactions

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: Authorisation, impersonation fraud and blocking of transactions

PUBLIC

1. Introduction

This note treats outstanding topics on fraud which will be discussed at the political trilogue on 26 November. The note covers blocking of transactions, authorisation, and impersonation fraud. The Presidency has, based on discussions with the European Parliament (EP) – both at the political trilogues and at the interinstitutional meetings (ITMs) – worked on a number of potential compromises between the EP and the Council.

2. Liability for not blocking payment instruments (Article 51(2) – line 671), not blocking transactions (Article 65 – no specific line), for not freezing funds (Article 69 – no specific line), and for not blocking a unique identifier (Article 83(5a) – line 877a)

This section covers liability for not blocking payment instruments, payment orders, freezing funds, or blocking a unique identifier reported as fraudulent through the data sharing arrangements. These topics are still considered as outstanding issues to be included in discussions at the upcoming political trilogue.

The Presidency has in the exchanges with the EP argued that blocking of instruments should not be made mandatory, instead it would be more proportionate to make blocking of transactions mandatory. For now, the EP has not agreed to this Council proposal. However, the EP has asked whether it would be possible to instead add a provision to Article 65 on blocking of payment orders, stating that a PSP can be held liable if the PSP fail to block a transaction in cases where there were objectively justified reasons to believe this transaction was fraudulent. This could be based on the transaction monitoring mechanism (TMM) or other relevant information available to the PSP.

The Presidency has also argued that it is not proportionate to make PSPs liable for failing to block a unique identifier that has been reported as fraudulent through the data sharing arrangements in Article 83/83a (line 877a). Furthermore, the Presidency has argued that the blocking of a unique identifier would not be proportionate since it would only be based on the assessment of the PSPs with no courts involved. This could potentially lead to a shadow ban of the unique identifier even in cases where the PSU was innocent or where the PSU might not have been a fraudster but could have unintentionally acted as a money mule. With the EP's drafting an innocent PSU would have to get a new unique identifier before it could again take part in the digital payment system. On the other hand, fraudsters might have several unique identifiers at their disposal. As such, the Presidency has argued that this

PUBLIC

proposal would not be proportional and does not contain adequate safeguards. If a unique identifier has been reported as fraudulent it should be incorporated in the risk assessment in the TMM of the PSPs, but it should not risk being a shadow ban of that PSU which the PSU would not even be aware of.

The EP has preliminarily at technical level agreed that if liability for PSPs is included in Article 65 and 69, implying that the PSP would be held liable for not blocking or freezing a transaction when there are objectively justified reasons to suspect fraud, the EP's proposal in Article 83(5a) would be covered. While the Presidency believes this would be a more proportionate solution than the EP amendments to art. 51(2) and 83(5a), the Presidency has argued that adding liability to Article 65 and 69 could lead to excessive de-risking and it should thereby not be perceived as the Presidency has agreed to introduce liability in these two articles.

The Presidency notices that, since freezing of funds in Article 69 is not currently mandatory, it would not be suitable to introduce liability here. However, as a compromise, the Presidency suggests that liability should instead only be linked to Article 65. In this way PSP's can be held responsible if they fail to block a transaction if there were objectively justified reasons to believe the transaction was fraudulent.

The Presidency would thus like to ask whether this compromise could be an acceptable way forward, to address the EP's wish to expand liability for PSPs in cases of fraud.

Q1: Can Member States, in the context of a broader compromise, accept that PSPs would be held liable for not blocking transactions where there were objectively justified reasons to believe that the transaction was fraudulent? Furthermore, do Member States think that a stronger wording than "objectively justified reasons" should be used and in such case, which wording?

Q2: Would Member States prefer the EP's original proposal for blocking of a unique identifier with liability for not doing so (line 877a), rather than adding liability for not blocking a payment order (or not freezing funds) in Article 65 (and 69)? If so, which safeguards could be added to avoid a shadow ban of a PSU?

Besides the above, the Presidency would also like Member States' input as to whether the provisions on freezing of funds should be aligned with the blocking on payment orders by making the freezing of funds mandatory as well. Such change could be presented to the EP as a way to strengthen this fraud preventive measure in the context of an overall

PUBLIC

compromise. This would be in line with Article 71 of the AMLR[1] which states that: "*Obliged entities **shall refrain** from carrying out transactions which they know or suspect to be related to proceeds of **criminal activity** or to terrorist financing (…)*". The Commission argues that this would also cover fraud cf. Article 2(1)(i) of directive 2018/1673 where "fraud" is defined as a "criminal activity". Due to this, Article 71 of AMLR should be interpreted as an obligation for both a sending or a receiving PSP to not carry out a transaction where fraud is suspected. A similar wording could be used in the context of PSR, if Member States are to accept such amendment.

Q3: Can Member States, in the context of a broader compromise, support making freezing of funds mandatory in cases where there are objectively justified reasons for suspecting fraud?

3. Definition of authorisation (Article 3(34a) and 49)

The Presidency has argued that the EP's amendment to the definition of authorised transactions in Article 3(34a) should be discussed in conjunction with Article 59. This should be done to ensure an objective approach in for the definition of authorisation, in order to provide certainty as to when a payment is final and valid. Therefore, it has been possible to continue the discussions on Article 49 at technical level, while the discussion of the content of Article 3(34a) is still reserved for political trilogues.

The Presidency notes that Member States have indicated no flexibility towards the EP proposal in Article 3(34a) on the definition of authorisation. The proposal is considered as too broad due to the inclusion of subjective elements. 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*" (line 247a). In recital 79a (line 89a) 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 of the payer should happen in accordance with national law.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401624

PUBLIC

Inclusion of full knowledge of especially the purpose of a transaction is a difficult criterion for the PSPs to assess, when evaluating whether a transaction is authorised or not. However, the Presidency would like to suggest a compromise for the definition of authorisation. PSPs could include specific information regarding the amount and the recipient as part of the authentication process. The Presidency would thus like to propose a supplement to the definition of unauthorised transactions (Article 49), where the Presidency believes it would be more appropriate to place the drafting. The proposed drafting takes out the subjective elements of the EP text such as "freely", "full knowledge" and "purpose" and only includes the recipient and amount.

Article 49(1a) (line 902)
Compromise drafting suggestion in **red**

"*A payment transaction shall not be deemed authorised where:*

- *the transaction was initiated or modified by a third party who acted without the consent of the PSU, including by using fraudulently the personal security credentials of the PSU;* ***or where***
- ***the consent of the PSU was obtained by a third party through deceptive means resulting in the fact that when consenting to execute the transaction the PSU was not in possession of the correct information on the amount of the transaction or on the recipient of the transaction.***"

Q4: Can Member States support the suggested drafting for a definition of unauthorised transactions?

4. Impersonation fraud (Article 59(1))

The Commission has in its proposal for PSR included a refund right in relation to authorised transactions in Article 59. This includes specific cases where a PSP has been impersonated. The discussions on impersonation fraud have so far been reserved for the political level only.

The Presidency has argued that discussions regarding the scope of liability for PSPs should take place in the context of Article 59. Should the EP accept this, it would mean that the intention with the EP's proposal in Article 3(34a) would be included as part of the discussion of impersonation fraud. This implies that the EP's intention to broaden the liability for PSPs should be perceived as broader than what is now included in their amendment to Article 59.

PUBLIC

The EP has proposed to expand Article 59 to also cover impersonation of other relevant public or private entities.

The EP's amendments to Article 59 were also discussed at the Council Working Party on 8 September 2025. Here, Member States expressed the view that the EP's text could not be accepted. This was mainly because PSPs do not have control over how public or private entities communicate with consumers.

In the Council Working Party on 2 October 2025, the Presidency included a question as to which kinds of safeguards could be included, if the liability of PSPs were to be expanded. Here, it was clearly stated by Member States that the PSR should only impose requirements on PSPs and that any requirements regarding how public or private entities communicate is not a viable safeguard and should be avoided. In this sense, Member States at the last working party rejected the idea of expanding the scope regardless of further safeguards.

However, some Member States did come with suggestions for how potential liability could be fairly distributed, if the scope of Article 59 should be expanded. Below, the Presidency will elaborate on these different tools: **Caps, claim excess, shared liability/liability as a percentage of defrauded amount, and the one strike-principle**. These safeguards could potentially be applied simultaneously. If Member States show flexibility to extend the scope of Article 59 to impersonation of other entities while including one or multiple of the suggested safeguards, it should then be decided whether these safeguards should be applied to Article 59 in general (including PSP impersonation fraud), or only to the cases covered by the potentially extended scope (i.e. only to impersonation of potential other entities).

Below you can see a description of the specific safeguards.

4.1 Caps

In the UK, hard caps are put in place for reimbursements for APP fraud. This hard cap is set at £85,000, corresponding to almost EUR 100,000. This would mean that PSPs would only be required to cover the part of the defrauded amount below £85,000. However, the Presidency finds that if such a safeguard is to be supported, it could be set much lower – e.g. €10,000-20,000 – if deemed necessary by the Member States.

Another way to make use of caps could also be to make a cumulative cap instead of a transaction-based hard cap. E.g. if a cumulative cap of EUR 30,000 is applied, a victim could be defrauded once for this amount or several times up to this amount. Any amount going above this cumulative cap would not have to be refunded by the PSP.

PUBLIC

Q5: If caps are to be included as a safeguard, would a hard cap, a cumulative cap, or potentially both be preferable?

Q6: Which amount do Member States find appropriate for a hard and cumulative cap?

4.2 Claim excess

A claim excess is another way to distribute the consequences of fraud, as it is way to align incentives and thereby avoid moral hazard. It also ensures that PSPs will not have to handle cases with relatively low amounts involved. This helps to avoid situations where an investigation would be more expensive than just providing a reimbursement, which could lead to abuse of the reimbursement possibilities.

In the UK it is voluntary for PSPs to decide whether they will apply a claim excess. The maximum amount of the claim excess is £100. This level was decided upon since it was believed that it would minimise the financial harm for consumers, but at the same time also encourage them to exercise due caution before making a payment order. In cases where a vulnerable customer is involved (which is evaluated by the PSP within a specified set of criteria), the PSP is not allowed to collect the claim excess. However, in a PSR context it could be decided that PSPs should be allowed to collect a claim excess from all customers and that this claim excess should exceed a high threshold e.g. EUR 1,000.

Q7: Which amount do Member States find appropriate for a potential claim excess be set?

4.3 Shared liability/liability as a percentage of defrauded amount

Another way of sharing the burden could be to decide on a percentual threshold, which the PSP could be liable for. In this way, the PSU would be incentivised to be vigilant and exercise caution when executing transactions. This could e.g. be 50 % of the total defrauded amount, or it could be 50 % of the amount within the thresholds of the potential hard caps and claim excesses as mentioned above in section 4.1 and 4.2 (e.g. 50 % of any amount within the range of €1,000 to €20,000). In this scenario the consumer would be covering any amount up to the maximum claim excess, any amount above the hard cap and 50 % of the amount within those thresholds.

PUBLIC

The percentage of the share of liability for PSPs could also be calibrated in another way, where e.g. the PSP would be liable for 80 % of the defrauded amount of the transaction the first time a PSU is a victim of impersonation fraud, 60 % the second time and so on down to 0%. The intervals should by all means be set appropriately.

Liability could also be shared between the payer's and the payee's PSP. While the payer's PSP have a better understanding of the payer's everyday use of their payment instruments this places the payer's PSP in a good position to hinder fraud through the transaction monitoring mechanism (TMM). However, the payee's PSP did in fact allow a fraudster to become a customer and should cf. the Council position also apply their own TMM. The payee's PSP therefore also has a responsibility in preventing fraudulent transactions. Thus, the payer's and the payee's PSP could be required to share the burden of liability for impersonation fraud.

Q8: If shared liability is to be added as a safeguard, would it then be preferable to share it 50/50 (or at another percentage), or would it be preferable to let PSPs be liable for a decreasing percentage of the amount depending on the number of times their customer has been defrauded?

Q9: Should liability be shared between the payer's and the payee's PSP? If so, should the liability be shared 50/50?

4.4 One strike-principle

A further suggested safeguard is the "one strike-principle". Here, a consumer would only be able to claim a refund for the same type of impersonation fraud once. This suggestion has earlier been refused in the Council due to practical issues, which includes relevant questions, e.g. what would happen if the PSU switches PSP (or makes use of several PSPs), and how it is assessed whether the fraud in question is the same type of fraud as last time the customer was defrauded. Further, it has been argued that someone falling victim to fraud once would also be more vulnerable for fraud in the future. Since fraudsters would now know that this is a person who has already fallen for a fraudster's manipulation. They could therefore target the same person again. Finally, some Member States argued that this mechanism might

PUBLIC

create unfair discrepancies in how much customers are being refunded after being victims to fraud[2].

In the Council's text one of the elements included in the list of criteria for the evaluation of gross negligence (recital 82) is making use of the same principle though without giving definitive answers as to when it could in fact be considered as gross negligence. This criterion is whether the payment service user has previously fallen victim of the same type of fraud. In the recital 82 concerning gross negligence, it would not necessarily be considered gross negligence to fall for the same type of fraud twice, but if the one strike-principle is implemented it would not be possible to get reimbursed a second time for the same type of fraud. However, this does indicate that the Council believes that whether or not a PSU has been the victim of the same type of fraud at an earlier stage is a relevant factor to assess. For this reason, the Presidency finds it relevant to ask Member States whether this principle should be brought into the text if the scope of Article 59 is extended.

For some of the arguments presented above against the one strike-principle, the Presidency would like to provide the following suggested answers. However, Member States are encouraged to provide alternative answers if they perceive another answer might be more appropriate:

What would happen if a PSU switched PSP?
The Presidency believes that the simplest solution would be to allow consumers a new chance to obtain reimbursement in cases of impersonation fraud when switching PSP. This is due to the fact that PSPs would otherwise have to share information between each other regarding all customers who have already been refunded once. This would seem disproportionate. The Presidency believes that this issue is a shortcoming with the one strike-principle safeguard, since this would incentivize customers to switch PSP only to regain protection.

How is it assessed whether the fraud in question is the same type of fraud as at an earlier occasions or not?
The Presidency believes there are four possible options here:

[2] E.g. someone being initially defrauded of EUR 2,000, and EUR 10,000 at a later stage would only be able to get the refund of EUR 2,000. At the same time as another person who might have been defrauded of EUR 50,000 on one occasion could be refunded the entire amount. This would be even though the EUR 50,000 is a much larger amount than the accumulated amount for the person who was defrauded twice for lower amounts.

PUBLIC

1. A principles-based approach, allowing for PSPs, ADR-bodies and courts to assess. However, this could lead to inconsistencies across Member States.

2. A technology-based approach, implying that it is dependent on the technology used. For example, a spoofed phone call would differ from being tricked by a fraudulent email or text message. A disadvantage of this solution is that there is a risk that the PSR could quickly become outdated due to the development of new technologies.

3. An application of a one strike-principle across Article 59 in general, implying that there will be no need to assess whether it is the same kind of fraud or not. It would instead be concluded that a refund under Article 59 can only be required once.
   If the one strike-principle gains support from Member States, the Presidency believes option 3 would be preferable compared to the previous two options. If the scope of Article 59 is broadened to include other kinds of impersonation fraud, there would thereby not be a need to assess whether it was the same kind of fraud or not. Furthermore, the one strike-principle could be made to reset after a specific period of time has passed after a refund has been made. This could be one year, 10 years (or somewhere in between). After such time period has expired, it would again be possible for PSUs to be refunded for impersonation fraud.

4. Another option could be to let the text of the recital on gross negligence (recital 82 – line 92) be the guiding principle. In this setup we would not include the one strike-principle in the articles but let it remain as part of recital (82) as the text also currently stands.

<u>Regarding the one strike-principle:</u>
Q10: If the one strike-principle is chosen, do Member States have preferences in regard to how it is applied? E.g. should it be possible for a PSU to get a refund again at a later stage (e.g. after a certain number of years), etc? Should it be possible for a PSU to get a refund again if they switch PSP (if not, how should the new PSP become aware that their new customer is not entitled to a refund in the case of fraud?

Q11: How should it be assessed whether the fraud in question is the same type of fraud that the PSU was a victim of at an earlier occasion? (please see the four options presented by the Presidency)

<u>Regarding safeguards in general:</u>

PUBLIC

Q12: Which safeguard or combination of the safeguards listed below would Member States find preferable if the scope of the refund right for impersonation fraud is expanded?

Q13: Which safeguard(s) should be avoided?

4.5 Scope of impersonation fraud

As mentioned in the introduction, many Member States believed that the EP's suggested scope of impersonation fraud is too broad. In Article 59(1) the EP has broadened the scope of impersonation from PSP impersonation fraud as in the Commission's proposal, to also cover impersonation of "*any other relevant entity of a public or private nature*".

In recital 79 the EP provides further specification as to how this is to be understood *"(…) a relevant entity which could reasonably be linked to a trusted source of the customer, such as a central bank or government authority (…)*". Here, the EP has provided an explanation as to how the scope is to be understood with regards to **public authorities**. However, no explanation is provided as to which **private entities** could be intended to be covered.

Since Member States have already expressed scepticism towards such an expansion of the scope, the Presidency would like to seek input from the Member States as to whether the scope could be expanded in a more narrowly defined way compared to the EPs suggestion. This could include one or more of the safeguards mentioned above. If the scope is to be expanded the Presidency would suggest that it should cover specific entities, rather than the general expansion suggested by the EP. This would accommodate the EP's proposal to some extent while also keeping the more targeted approach of the Council mandate.

For **public entities** such extension could include one or more of the following public entities:

- Law enforcement agencies and judicial authorities such as the police and the courts.
- Tax authorities
- Public health and public social security authorities

For **private entities** it could be:

- Entities with a license to provide financial services, perhaps limited to where the defrauded consumer is also a customer and can provide evidence of this contractual customer relationship.

PUBLIC

EBA[3], ESMA[4], and EIOPA[5] all provides lists of **providers of financial services** on their websites. These could be used to determine whether an entity is within the potentially extended scope of impersonation fraud, which should be refunded.

Q14: Could Member States support to broaden the scope of Article 59 to any of the specific public entities listed above?

Q15: Could Member States support to broaden the scope of Article 59 to financial services providers? Should it be required that the defrauded consumer has a contractual relationship with the impersonated financial services provider?

4.6 Scope of safeguards

If there is flexibility in regard to expanding the scope in Article 59 to cover other entities than PSPs, it could be relevant to consider the necessary safeguards. Presidency believes it would be beneficial to discuss whether these further safeguards should only apply to the extended scope of impersonated entities discussed above. Alternatively, the safeguards could be applied to both impersonation of the consumer's PSP, as well as those potential other specific entities.

The advantage of having the same rule apply to all cases of impersonation fraud within the scope of the refund rights in Article 59 is that all types of impersonation fraud would then be treated equally. It could be difficult to explain why the safeguards should only be necessary for some kinds of impersonated entities but not for others. Therefore, applying the same safeguards to all relevant entities within the scope may ensure greater consistency and fairness.

On the other hand, a disadvantage is that extending the safeguards to cover additional types of impersonation fraud could result in more restrictive refund options for victims of PSP impersonation fraud. In particular, applying the same safeguards to PSP impersonation fraud - simply because the scope is extended to include, for example, impersonation of tax

[3] https://www.eba.europa.eu/risk-and-data-analysis/data/registers-and-other-list-institutions

[4] https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_upreg

[5] https://register.eiopa.europa.eu/

PUBLIC

authorities - could limit the reimbursement possibilities for consumers in cases of PSP impersonation fraud that were previously agreed upon in the Council.

Lastly, it could be argued that the Council did not introduce additional safeguards for PSP impersonation fraud because PSPs can help to prevent this type of fraud, for instance by educating their customers about how official communication between the PSP and its customers takes place. As many Member States have pointed out in working party meetings, this argument does not apply to impersonation of other entities. Therefore, any further safeguards should only be applied to the potentially extended scope of Article 59 and not applied to impersonation of the PSP itself.

Arguments could thus be made in both directions. The Presidency would therefore appreciate input from Member States as to which cases of impersonation fraud any safeguards should apply if the scope of refund rights for impersonation fraud is extended to also cover impersonation of other specific entities.

Scope of safeguards:
Q16: Should the safeguards cover only the potentially extended scope of entities or should it cover both the potentially extended scope AND the current scope, implying PSP impersonation fraud?

Preferred way forward:
Q17: For the three options listed in this note, which of the options could Member States show most/least flexibility towards?

1) **Adding liability to Article 65 (and potentially Article 69).**
2) **Adding a new indent to Article 49(1a) on unauthorised transactions.**
3) **A targeted expansion of Article 59(1).**