Council of the European Union
General Secretariat

PUBLIC

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

**Brussels, 31 March 2025**

**WK 4230/2025 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: | Presidency Discussion Note: Discussion on fraud-related issues in the Payment Services Regulation (authorisation, liability, burden of proof, gross negligence) |

POLAND25.EU

Polska Prezydencja w Radzie UE
Polish presidency of the Council of the EU
Présidence polonaise du Conseil de l'UE

PUBLIC

**Payment services package proposals (PSD3/PSR)**
*Brussels, 4 April 2025*

# Presidency Discussion Note
# Discussion on fraud-related issues in the Payment Services Regulation (authorisation, liability, burden of proof, gross negligence)

## I. Authorisation

In the PRY non-paper on fraud-related issues prepared for the 21 February CWP, we proposed two options for moving forward on the issue of authorisation. Either (as in Option 1) to revert to the European Commission's version of Article 49(1) (with the word *permission* replaced by the word *consent*) and clarify that a transaction must be both initiated and authenticated by the payer in order to be considered authorised, or (as in Option 2) not to consider a payment transaction as authorised, if the payer was manipulated into initiating the payment transaction through social engineering. As in all previous discussions on this issue, the opinions of Member States were divided, however, the majority of Member States opted for Option 1, which we considered to be the way forward. There were also some further amendments suggested in relation to Option 1, e.g. one Member State asked to clarify that a transaction is unauthorised if the payment order inserted by the PSU is modified by a third party without the PSU's knowledge and consent (i.e. the PSP's liability would cover cases such as man-in-the-middle/browser attacks). Another Member State pointed out that the current wording (under Option 1) only considers such transactions as unauthorised if the transaction is carried out by a third party after the personal security credentials have been fraudulently obtained, which would not include simple theft. Another Member State suggested clarifying that a payment transaction should only be considered unauthorised if consent has not been given or has not been given in the agreed manner, e.g. if SCA has not been used where required. The Presidency proposes to include these explanations in Recital 69a. Moreover we introduced amendments to Article 49(3)–(7) to make the terminology consistent with Article 49(1)–(2).

**See the proposed wording in Recital 69a and Article 49 PSR in the Annex**

***Q1.*** *Could Member States accept the proposed wording of Recital 69a and Article 49 PSR?*

## II. Liability

In their written comments following the 21 February CWP, the majority of Member States did not support the introduction of caps on PSP's liability, arguing that the PSP is liable in specific circumstances, where it is in its power to avoid or minimise the damage. If the PSP fails to do so, there is no reason to limit its liability. In addition, such limits could act as a disincentive for PSPs to implement and further develop mitigation measures, which would be seen as a 'consumer unfriendly' approach. Many Member States were of the opinion that caps could be useful if Option 2 was supported, but if a compromise was to be based on Option 1 in Article 49, additional caps would be a very unbalanced approach. In view of this, the Presidency does not intend to introduce caps on PSPs liability.

On the basis of the discussion at the 21 February CWP and subsequent written comments, the Presidency noted that several Member States questioned the proposed amendments to Article 59(1), which would require two specific elements in the fraud to be considered as bank employee impersonation fraud (i.e. the name and telephone number or e-mail address). These Member States argued that the current proposed wording would allow PSPs to avoid liability in cases where an e-mail address is used in combination with part or an incorrect version of the PSP's name, or where the fraudster uses a PSP's telephone number to mislead the consumer, without explicitly or fully mentioning the PSP's name. It was also pointed out that the proposal would weaken consumer protection and significantly reduce the scope of the provision.

The majority of Member States did not oppose extending the scope of Article 59(1) to fake websites and applications. However, some Member States suggested that the reference to bank employee impersonation fraud in more general terms would be sufficient, without specifying different elements of fraud. It was pointed out that excluding specific fraud methods from this Article would help to avoid potential problems of interpretation and prevent the provision from becoming unworkable over time as fraud techniques evolve.

Some Member States felt that the notion of '*without any delay*' was too strict and that the timeframe should in any case start from when the fraud is actually discovered by the PSU. It was also suggested that the PSP should request the information from the PSU (the obligation should not be placed on the PSU to proactively provide this, as it may be difficult for the PSU to assess exactly what information the PSP needs) and that it would be important to ensure that there are no unrealistic expectations as to what kind of evidence the PSU can be expected to have. To this end, some further amendments to Article 59(1) have been proposed, in line with the provision in Article 55(3).

In addition, some Member States pointed out that, if Option 1 was chosen, the protection offered in Article 59 would need to be strengthened, as there are many different types of impersonation fraud, leading to significant financial losses and a lack of confidence in various entities. To this end, the Presidency would like to point out that in their written comments sent after the CWP of 26 November 2024, the majority of Member States agreed that the PSP should bear liability in case of bank-employee impersonation fraud, as this type of fraud undermines consumers' trust in their PSP and also affects society's faith in electronic payments. However, banks do not have the resources and capabilities to prevent all forms of fraud and therefore cannot be held liable for all fraud losses.

One Member State strongly disagreed with the obligation to report impersonation fraud to the police, if Option 1 was chosen. Another Member State pointed out that the current Article 59 imposes more obligations on the PSU than on the PSP (such as reporting the fraud to the police and providing supporting evidence). Another Member State suggested that the obligation to report a fraud to the police could be placed on the PSP instead, as this would be a significant step forward for vulnerable citizens.

**See the proposed wording in Recitals 79 and 80a and Article 59(1) PSR in the Annex**

> ***Q2.*** *Could Member States accept the wording of Recitals 79 and 80a and Article 59(1) PSR or would Member States be in favour of referring to bank employee impersonation fraud in more general terms, without specifying different elements of fraud?*
>
> ***Q3.*** *Would Member States be in favour of shifting the obligation to report fraud to the police from the PSU to the PSP?*

On the basis of the Member States' replies to the questionnaire on fraud sent out after the 21 February CWP, the vast majority of Member States agreed to amend Article 60(1) in order to include dispute resolution bodies (courts and ADR bodies) among the entities empowered to reduce the liability of the payer. In order to make it clear that such bodies can only reduce the liability if they have mandate to do so in the first place, the Presidency would like to add the words '*dispute resolution bodies in accordance with their requisite powers*'. We would like to propose that the same wording also applies in the case of NCAs, as some Member States pointed out during the discussion that not all NCAs have these powers.

**See the proposed wording in Article 60(1) in the Annex**

The same high level of support was given to the proposal to include in Article 55(3) the amendment that the PSU shall provide the PSP with all the relevant information requested by the PSP and which the PSU can reasonably be expected to have with regard to the events leading up to the disputed payment transaction. To this end we consider the Article 55(3) to be agreed upon.

In order to refer to all the proposals presented during the 21 February CWP, we would like to clarify that the proposed amendments to Article 56(6) regarding the PSP's liability for unauthorised payment transactions, applied only to Option 2. As a consequence of the choice of Option 1, they will not be included in the text.

> ***Q4****. Could Member States accept the wording of Article 60(1) PSR?*

## III. Burden of proof and gross negligence

In their written comments following the 21 February CWP, the majority of Member States supported the proposed drafting to Article 55(2) – the addition that where a PSU denies having authorised a transaction, the use of SCA in itself is not necessarily sufficient to prove authorisation by the payer. To this end, we consider the Article 55(2) to be agreed upon.

Member States were still somewhat divided on how to best explain the concept of gross negligence in the PSR. While some of them supported the text proposed by the Presidency, many asked for further amendments to make it sufficiently clear that gross negligence should be always assessed based on the vulnerability with regard to individual characteristics of the PSU and of the situation, i.e. on a case by case basis. Therefore it was raised by some Member States to include in Recital 82 only a comprehensive and open-ended list of guidelines, without providing specific examples. Otherwise the mention of such examples would restrict the room of manoeuvre of ADR or courts and imply that in practice such situations cannot longer be discussed on a case-by-case basis. Other Member States asked to harmonise this recital, as examples were listed both in the main text and in the list in the recital. Yet other Member States asked to delete some indications of circumstances to be taken into account when assessing gross negligence, as they were unclear or too broad (such as subcategorising gross negligence based on PSU's characteristics).

**See the proposed wording in Recital 82 in the Annex**

In their written comments following the 21 February CWP, the majority of Member States did not support the proposed drafting to Article 56(1) – to add a prohibition for PSPs to set off any claims stemming from the same payment transaction against a payer's claim for refund. In light of this, the Presidency withdraws the proposed amendment and leave Article 56(1) unchanged (as in EC's version).

> ***Q5.*** *Do Member States agree with the proposed drafting to Recital 82 PSR? If not, please provide an alternative wording.*

PUBLIC

**Annex** (the newly introduced amendments are underlined)

**Recital 69a**

(69a) Authorisation is based on an intention or a contribution in fact. If the payment service user uses its security credentials in a responsible manner when executing a payment transaction, the validity and authenticity of the authorisation will be easier to assess. The set of payment transactions can be divided into two distinct categories, those that are considered authorised and those that are not, called unauthorised. The payment transaction operates as a process and requires the active participation and approval of the payment service user.
A payment transaction or a series of payment transactions should be assessed as authorised only if the payer has given its consent for the execution of the payment transaction in a manner agreed on between the payer and the account servicing payment service provider. It should not be deemed to be authorised where the transaction was initiated or modified by a third party who is acting without the consent of the payment service user, e.g. where the third party is using the personal security credentials of the payment service user fraudulently obtained.

**Recital 79**

(79) Consumers should be adequately protected in the context of certain fraudulent payment transactions that they have authorised without knowing these transactions were fraudulent. The number of 'social engineering' cases where consumers are manipulated ~~misled~~ into authorising a payment transaction to a fraudster has significantly increased in recent years. 'Spoofing' cases where fraudsters pretend to be employees of a customer's payment service provider and misuse the payment service provider's name, e-mail address, ~~or~~ telephone number, website or mobile application to gain the customers' trust and trick them into carrying-out some actions, are unfortunately becoming more widespread in the Union. Those new types of 'spoofing' fraud are blurring the difference that existed in Directive (EU) 2015/2366 between authorised and unauthorised transactions. Means through which the consent may be assumed to be granted are also becoming more complex to identify, as fraudsters can take control of the whole consent and authentication process including of the strong customer authentication completion. The conditions under which the customer authorised a transaction by giving his or her consent ~~permission~~ to it should be taken into due consideration, including by courts, to qualify a transaction as being authorised or unauthorised. A transaction may indeed have been authorised in circumstances where such authorisation was granted on manipulated premises affecting the integrity of the consent ~~permission~~. It is therefore no longer possible, as was the case in Directive (EU) 2015/2366, to limit refunds to unauthorised transactions only. It would however be disproportionate and financially very costly to payment services providers to open every fraudulent transaction, authorised or unauthorised, to a systematic refund right. It might also cause moral hazard and a reduction in the customer's vigilance.

**Recital 80a**

(80a) Cases of bank employee impersonation (spoofing) fraud affect the good repute of the bank financial entity, of the banking financial sector as a whole and may cause significant financial damages to Union consumers, affecting their trust in electronic payments and in the banking financial system. A good-faith consumer who has been the victim of such manipulated transactions, namely 'spoofing' fraud where fraudsters pretend to be employees of a customer's payment service provider and misuse the payment service provider's name, e-mail address, ~~or~~ telephone number, website or mobile application should therefore be entitled to a refund of the full amount of the fraudulent payment transaction from the payment service provider on a shared-damage basis, unless the payer has acted fraudulently or with 'gross negligence'. As soon as the consumer becomes aware that he or she has been a victim of that type of spoofing fraud manipulation, the consumer should without undue delay report the incident to the police, preferably via online complaint procedures, where made available by the police, and to his or her payment service provider and provide the payment service provider with all the relevant information requested by the payment service provider and that the payment service user can reasonably be expected to have regarding the events leading to the disputed payment transaction~~, providing supporting evidence~~. No refund should be granted where those procedural conditions are not fulfilled. Although the payment service provider may have perceived the payment transaction as authorised, the customer was the victim of a fraud, so in order to establish customer protection and maintain trust in the financial system, a properly designed damage sharing can ensure a real balance between the interests of the consumer and the payment service provider in such manipulation cases. Without prejudice to the right of customers to bring action in courts, the rules of refunds based on shared compensation between the payer and the payment service provider can only be considered as a temporary (preliminary) way.

**Recital 82**

(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness that should be assessed depending on the individual circumstances of the case~~.; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties; sharing account credentials with the person without the right of disposal, i.e. is not eligible to use the payment instrument; if the loss of a payment instrument is not reported to the payment service provider immediately after the loss is discovered; where the payment service user has ignored a clear, concrete and case-specific warning by the payment service provider about how to react in the type of fraudulent situation which then occurred and led to the damage; where the payment service user has failed to check if the elements which are dynamically linked and displayed during the strong customer authentication in accordance with Article 85 are correct.~~

When assessing the possible gross negligence on the part of the payment service user, account should be taken, for example, ~~to all the factual circumstances shall be taken into account. For this purpose, one or more of the following circumstances may be taken into account, such as the (a) payment service user's behaviour or communication with third parties, where relevant; (ab)~~ of the innovativeness and~~,~~ complexity of the fraud, ~~and~~ the means or strategies used by third parties to

illegally take over the payment service user's personalised security credentials; ~~of payment instruments owned by the payment service user~~; ~~(c) innovativeness, complexity of fraud~~; ~~(bd)~~ whether the payment service user has previously fallen victim of the same type of fraud; ~~(ce) in case the fraudster's means or strategies constitute a new type of fraud,~~ whether the payment service providers have complied with ~~fulfilled~~ their obligations under Article 84, ~~with particular~~ including with regard to their most vulnerable groups of customers; ~~(df)~~ whether the payment service user has taken adequate steps in order to properly ensure the confidentiality of their personalised security credentials. ~~of the payment instruments~~;

~~(eg) the known characteristics of the payment service user that might make the user more likely to fall victim to fraud, for example the user's age, or level of education or profession;~~

~~(fh) in the event that the payment service user used its means of identification, the circumstances, whether and what the payment service user saw in its messages asking to enter its security credential that confirmed the disputed payment or where the payment service user has failed to check if the elements which are dynamically linked and regarding the amount and the payee that were displayed during the strong customer authentication in accordance with Article 85 are correct, and, where the applicable, the circumstances why the payment service user authenticated the payment without having regard to the information displayed during the authentication process;~~

~~(i) whether the personalised security credentials of the payment instrument have been appropriated by third parties, while the payment service user was using the payment instrument according to its purpose;~~

~~(gj) whether the payment service providers offered clear, concrete and case specific bespoke warnings against currently used frauds methods that were brought directly to the attention of payer, that are transaction specific, and payment service providers actions, taken in order to familiarise the payment service user with the risks and methods of fraud in the electronic space, as well as the meaning and legal consequences of the safe misuse of identification means and payment instruments issued by the payment service user, the disclosure of their personalised security data, etc. the specificity and nature of any intervention made by the sending payment service provider in the payment flow, whether the payment service user failed to have regard to specific, directed interventions made by their payment service provdider, and whether those interventions offered a clear assessment of the probability that an intended payment was fraudulent.~~

~~This list is not exhaustive and does not prejudice the discretion of national courts and/or ADR entities. The circumstances as mentioned are not cumulative and are not binding.~~

~~The fact that a payment service user consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again victim of the same type of fraud could, depending on the circumstances of the case, be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent *modus operandi*.~~

**Article 49 [Authorisation]**

1. A payment transaction or a series of payment transactions shall be authorised only if the payer has given its ~~permission~~ consent for the execution of the payment transaction ~~including as regards the amount of the payment transaction and the payee~~. A payment transaction may be authorised

by the payer prior to or, if agreed between the payer and the account servicing payment service provider, after the execution of the payment transaction.

~~2. A payment transaction shall not be deemed as authorised where the payer was manipulated through social engineering into initiating the payment transaction in favour of a third party which was not the intended payee, or where the transaction was initiated by a third party using the personal security credentials of the payment service user fraudulently obtained.~~ [moved to Recital 69a]

~~3. By way of derogation from paragraph 1, and without prejudice to paragraph 2, where the payer has given a mandate authorising the payee to place a payment order for a payment transaction or a series of payment transactions, and where the mandate is based on an agreement between the payer and the payee for the provision of products or services, the payment transactions initiated by the payee on the basis of such a mandate shall be deemed as authorised if they comply with the mandate given by the payer.~~

~~4. By way of derogation from paragraph (1), and without prejudice to paragraph (2), where a payment transaction is initiated by or through the payee in the context of a card-based payment transaction and the exact amount is not known to the payer at the time of the authentication of the payment transaction, the payment transaction shall be deemed authorised only where, prior to the initiation of the payment transaction, the payer agreed that the final amount may increase or decrease after authentication, and, in case of increase, this does not exceed the payer's reasonable expectation.~~

2~~(5) 3~~. Access to a payment account for the purpose of account information services or payment initiation services by payment service providers shall be authorised only if the payment service user has given its ~~permission~~ consent to the account information services provider or, respectively, to the payment initiation service provider, to access the payment account and the relevant data in that account.

3. In the absence of consent ~~permission~~, a payment transaction or access to a payment account by an account information service provider or a payment initiation service provider shall be considered to be unauthorised.

4. Account servicing payment service providers shall not verify the consent ~~permission~~ given by the payment service user to the account information service provider or payment initiation service provider.

5. The consent ~~permission~~ referred to in paragraphs 1 and 2 shall be expressed in the form agreed between the payer and the relevant payment service provider. Consent ~~Permission~~ to execute a payment transaction may also be expressed via the payee or the payment initiation service provider.

6. The procedure for giving consent ~~permission~~ shall be agreed between the payer and the relevant payment service provider.

7. The payment service user may withdraw consent ~~permission~~ to execute a payment transaction or to access a payment account for the purpose of payment initiation services or account information services may be withdrawn by the payment service user at any time. The payment service user may also withdraw consent ~~permission~~ to execute a series of payment transactions, in which case any future payment transaction shall be considered to be unauthorised.

**Article 59 [Payment service provider's liability for impersonation fraud]**

| |
|---|
| 1. Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer's payment service provider using the name ~~and~~ or e-mail address or ~~name and~~ telephone number or website or mobile application of that payment service provider unlawfully and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without undue ~~any~~ delay, reported the fraud to the police and notified its payment service provider when becoming aware of the fraud, providing the payment service provider with all the relevant information requested by the payment service provider and that the payment service user can reasonably be expected to have regarding the events leading to the disputed payment transaction ~~providing supporting evidence available to the consumer~~.<br>[…] |

**Article 60 [Payer's liability for unauthorised payment transactions]**

| |
|---|
| 1. By way of derogation from Article 56, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument. |
| The first subparagraph shall not apply where any of the following occurred: |
| (a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or |
| (b) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced. |
| The payer shall bear all of the losses relating to any unauthorised payment transactions if those losses were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 52 with intent or gross negligence. In such cases, the maximum amount referred to in the first subparagraph shall not apply. |
| Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 52, national competent authorities or dispute resolution bodies, in accordance with their requisite powers, or payment service providers may reduce the liability referred to in this paragraph, taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated. |