Council of the European Union
General Secretariat

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

Brussels, 13 March 2025

WK 3365/2025 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:	Presidency Discussion Note on fraud prevention measures

POLAND25.EU

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

Payment services package proposals (PSD3/PSR)
Brussels, 19 March 2025

Presidency Discussion Note on fraud prevention measures

Platform on combatting fraud

In the PRY non-paper on fraud prevention measures for the 28 January CWP, we proposed creating a dedicated platform on combatting fraud in the area of payment services in the Union. The idea was to bring together experts and representatives from various organisations and parties involved in the fraud chain, in order to enable, among other things, the development of new tools aimed at better combatting and preventing fraud. The proposal met with widespread support from Member States, although some improvements were proposed. The majority of Member States were of the opinion that the key aspects of the platform, such as its purpose or diverse, non-exhaustive composition, should be regulated in L1, whereas the details could be left to L2. It was also mentioned that the measures taken should improve not only cross-border, but also cross-sectoral cooperation. Some Member States requested that representatives of competent authorities should be added to the Platform to ensure appropriate information flow and coordination on EU-level and national initiatives. Other Member States suggested the addition of representatives of ECSPs, telcos, platforms, and consumer organisations, while others preferred to apply broader language, in particular for private sector representatives, and not to list them to ensure greater flexibility. After consulting the EBA, in order not to overlap with the responsibilities the EBA already has, the Presidency proposes also amending the proposal such that the EBA is not a member, but an observer to the Platform.

See the proposed wording in Article XXX [Platform on combatting fraud] with accompanying Recitals (XXX, XXY, XXZ) PSR in Annex.

> *Q1. Could Member States accept the proposed drafting of Article XXX and Recitals XXX, XXY and XXZ PSR?*

Spending limits and 'cooling-off' periods

In the comments sent to the Presidency after the 28 January CWP, the vast majority of Member States were in favour of including spending limits and cooling-off periods in PSR as a useful measure for fraud prevention. Most Member States were, however, of the opinion that spending limits should not be voluntary, but rather offered as a default option with the possibility for PSU to opt out if desired. The Presidency also noted the need reported by some Member States to enable the PSUs to protect themselves and therefore not restrict the possible limits to either per-day or per-transaction limits, but to clarify that the PSU should also be able to choose both types of limits simultaneously. It was further suggested that the cooling-off periods should also be a default option, with any subsequent opting out subject to the delay period. Several Member States asked also to precisely specify the delay limit in L1.

As regards the proposed amendments to Article 51 that result from the Member States' comments, it has to be noted that some of them create a potential conflict between Article 51 PSR and provisions introduced by the IPR in the SEPA Regulation. However, taking into account that PSR introduces more holistic provisions (as compared to the SEPA Regulation) and in line with the majority of Member States, the Presidency suggests the following amendments:

- Article 51(1) – the proposal to set spending limits by default by removing the reference to 'at the request of the PSU' in Article 51(1) – compared to Article 5a(6) SEPA as amended by IPR that includes such a reference.

- Article 51(1) – the proposal to remove the word 'either' – compared to Article 5a(6) SEPA as amended by IPR that includes such a word. The removal of this word may improve the consumer choice with regard to spending limits.
- Article 51(1a) – the proposal introducing the requirement for PSP to include cool-off periods – compared to the above provisions and recital 19 of the IPR which provides that: "(19) In order to allow PSUs greater discretion when making use of instant credit transfers, a PSU should be able to set an individual limit fixing a maximum amount, either on a daily or per transaction basis, that it can send by means of instant credit transfer. PSUs should be able to modify or lift those individual limits at any time, without difficulty and with immediate effect."

Moreover a few Member States opted for clarifying that any increase in spending limits or opting out of the application of a delay period would require the application of SCA, and the PSU should immediately be notified thereof by the PSP. To this end one Member State indicated that it would also be preferable to mention that an increase in a spending limit should require SCA only when done remotely, which would not be the case if the PSU requested an increase in a spending limit in physical locations of the PSP.

See the proposed wording in Recital XX and Article 51(1, 1a, 1b) PSR in Annex.

Q2. Could Member States accept the proposed drafting of Recital XX and Article 51 (1,1a,1b) PSR?

Security of the installation of a mobile application

Ahead of the 21 February CWP, BE provided a non-paper with a proposal to further reinforce the security of the installation of mobile applications. It was proposed that the following obligations should be imposed on the PSP: (i) it should notify the PSU in a safe manner of the installation onto a new device of a mobile application linked to its bank account and (ii) it should offer an additional step in the procedure for the installation of a new mobile application.

Based on the written comments of Member States sent to the Presidency after the CWP in February, we note some support for the BE proposal, although at the same time we also observe that many Member States reported the need to further modify the proposed provisions. There were, for instance, some doubts regarding the procedure for installing the application onto a new device itself. As the installation of an application is always possible, it was suggested that the provisions should rather specify it towards the application's activation or logging in process. Some Member States were of the opinion that the draft was too detailed and should be more general, or otherwise not included in L1, but rather in EBA RTS. Another Member State suggested that instead of defining the process for the secure activation of this new device, the scope of SCA could be broadened to include the activation of a new device/application as the 'possession' aspect of SCA. A few Member States found that it was not necessary for the proposal to be included in the PSR, arguing that the scenario already fell under the requirements of the SCA. There was also some support for introducing a cooling-off period with regard to the activation of the banking application on a new device, but more as an option than as a mandatory measure. Keeping in mind the divergent opinions presented by Member States, the Presidency would like to propose introducing some amendments to the BE proposal.

See the proposed wording in Article 51(5, 5a, 5b, 5c) PSR in Annex.

Q3. Would Member States support the proposed drafting of Article 51(5, 5a, 5b, 5c)? If not, please provide drafting suggestions.

Freezing of funds by the payee's PSP

In line with suggestions from some Member States during the 28 January CWP, in the PRY non-paper prepared for the 21 February CWP we proposed adding tools for the payee's PSP to freeze funds in the

event of a suspected fraudulent transaction. The proposal was widely supported, although a few Member States suggested deleting the reference to the transaction monitoring mechanism, since there could be other sources from which the indication for reasonable grounds to suspect a fraudulent payment transaction could come, and therefore the provisions should not be limited in this regard. Some Member States pointed out that a timeframe should be included within which a payee's PSP must decide whether a transaction can indeed be classified as fraudulent, and that the payer's PSP should be informed of the suspension of the transaction. Some Member States also requested a change in the last sentence of Recital 69d with regard to the liability of PSP.

See the proposed wording in Recital 69d and Article 69(2a) PSR in Annex.

Q4. Could Member States accept the proposed amended drafting of Recital 69d and Article 69(2a) PSR?

Q4.1 Do Member States see the need to include similar timeframe on the payer's PSP side with regard to transaction blocking?

Blocking of the use of the payment instrument and refusal to execute a payment order in the event of reasonable grounds to suspect fraud

On the basis of the written comments sent to the Presidency following the 28 January CWP, the Presidency noted significant support for the proposals presented in advance of the meeting (in particular for Recital 69e, 69f, Article 53(3), which we regard to be agreed upon). Nevertheless, some improvements were suggested. Some Member States pointed out that the requirement of agreeing on the refusal to execute a payment order under Article 65(1a) should be mandatory in any case, and not only 'if agreed upon in the framework contract'. Moreover, it was suggested that the requirement should apply to payment transactions in general, and not necessarily only to 'authorised' payment transactions. Some Member States proposed amendments to the wording 'reasonable grounds to suspect fraud against the payment service user' (Art. 65(1a)) to also cover cases where the PSU act as an accomplice to the fraudster (e.g. money mule). Other Member States indicated that if the payer's PSP has duly justified and reasonable grounds for suspecting fraud, there should be no discretionary right of that PSP regarding refusal to execute the payment transaction. One Member State pointed out that in Article 65(2) regarding instant credit transfers, where the PSP within 10 seconds should notify the payer of the refusal and provide reasons for the refusal, the timeframe of 10 seconds may be too short to provide such reasons, and it would be more workable to stipulate that for instant credit transfers the PSP must notify of the refusal within 10 seconds and provide the reasons for the refusal without undue delay. It was also suggested, for purposes of clarification, that the wording 'correcting any factual mistakes that led to the refusal' in Article 65(2) should be amended to 'correcting the decision to refuse to execute the transaction', since an affected PSU would ultimately want to overturn the decision, not just the facts upon which the decision was based. Moreover, we noted some suggestions to align the wordings of Article 51(2) and Article 65 PSR as regards the event, when the payment instrument is used by the payment service user for activity that is prohibited by other relevant Union or national law.

In their written comments after the 21 February CWP, many Member States supported the shift of liability to the PSP, if the PSP had not blocked a transaction in the event of reasonable grounds for suspecting fraud. At the same time, many Member States also pointed out that the proposed amendment to Art. 51(2) could cause excessive derisking by PSPs who may block a payment instrument even if there are only slight suspicions of fraud, in order to avoid any liability whatsoever. Such an approach could seriously hamper the efficient flow of payments and could eventually be detrimental to consumers. It was also raised that the assessing of such a suspicion is case-dependent, and the failure to apply such measure correctly could be a matter of dispute, as it is not always straightforward to determine whether a specific payment is 'suspect'. Therefore the Presidency proposes deleting the recently proposed last sentence of Article 51(2).

See the proposed wording of Articles 51(2) and 65(1a, 2) PSR.

Q5. Could Member States accept the wording of Articles 51(2) and 65(1a, 2) PSR?

Interplay with AMLR

In their written comments after the 28 January CWP, the vast majority of Member States agreed with the proposed drafting of Recital 69c and Article 69(1) and (2) with regard to clarifying the interplay with Regulation (EU) 2024/1624 (AMLR). In particular, there was a proposal to clarify that the AMLR also applies where the payer's PSP has reasonable grounds to suspect that the payer may be a victim of fraud and that the requirements in Article 69 PSR on the maximum execution time are without prejudice to the payer's PSP or the payee's PSP obligations under other relevant Union or national legislation in the field of anti-money laundering and anti-terrorism financing (e.g. the AMLR or the Funds Transfer Regulation). To this end the Presidency regards the drafting of Recital 69c and Article 69(1) and (2) as agreed upon.

Obligation of the payee's PSP to conduct transaction monitoring

In the non-paper prepared for the 28 January CWP, the Presidency proposed reflecting in the recitals to the PSR the provisions of Article 83(1a) PSR introduced by the HU PCY as regards the obligation of both the payer's and the payee's PSP to conduct transaction monitoring. As the amendments included in Recitals 100 and 102 were not challenged by the vast majority of Member States, the Presidency regards their text as stable.

With regard to Article 83(2), a few Member States were of the opinion that the list of data to be monitored should be inexhaustive, although the majority agreed with the wording already provided by the Presidency. There were, nevertheless, some suggestions for improving the text, e.g. to further specify session data and device data, and to add them also with respect to the payee. One Member State also suggested harmonising data requirements under Article 83 and 83a.

In their written comments following the 21 February CWP, the majority of Member States supported the proposed wording regarding the shifting of liability to the PSP when the PSP fails to fulfil its transaction monitoring obligations. Some Member States proposed further improvements to the text, e.g. including a provision relating to negligent behaviour of the PSU, since under the current wording the PSP would bear all costs even if the PSU had acted with gross negligence, which could lead to unbalanced outcomes. One Member State suggested clarifying that the burden of proving that there was no breach of transaction monitoring obligations should fall on the payment service provider. The drafting also required more clarity, especially concerning when a responsibility exists, since an obligation to monitor is already in place and should be respected.

See the proposed wording in Article 83 para. (1a) and (2) PSR.

Q6. Could Member States accept the wording of Article 83(1a) and (2) PSR?

Anti-fraud information sharing

In their written comments sent to the Presidency after the 28 January CWP, the majority of Member States confirmed that the catalogue of data specified in the proposed Article 83a(1) PSR should not be exhaustive. Some requested that this should be even further clarified in the text. One Member State pointed out that the list in Article 83a(1) only mentions the data of the payee, and not of the payer, and proposed changing this to the more general wording of 'payment service user', which would add value and flexibility to the crime preventive activities. Another Member State asked for further clarification regarding whose contact details, as mentioned in point (i) of the list, may be shared.

Moreover, some Member States noted that the participation in fraud data sharing should be made mandatory, while other Member States reiterated the importance of the GDPR in relation to the PSR.

Some Member States indicated that the three-year maximum period specified in Article 83a(2) for retaining data obtained from an information exchange is too short, as some types of fraud may take a long time to detect and then to investigate, and suggested that this should be replaced with a 5-year limit.

A great majority of Member States supported the drafting proposal to enable the sharing of fraud-related information between PSPs and public authorities and to leave room for Member States to define the 'relevant national authorities' at national level. Some minor wording suggestions were proposed in order to further improve the text.

At the same time, in their written comments after the 21 February CWP, the majority of Member States opposed or had serious doubts regarding the proposal of shifting liability to the PSP, where the exchange of fraud data does not take place. Therefore the Presidency proposes deleting the second sentence of Article 83a(1a) – the amendment that was recently proposed.

<u>See the proposed wording of Recital 103a and Article 83a para. (1), (1a), (2) and (6) PSR.</u>

> *Q7. Could Member States accept the proposed wording of Recital 103a and Article 83a para. (1), (1a), (2) and (6) PSR?*

Annex (newly-introduced amendments are underlined)

Recital 69d

It is important to ensure that payment service providers' transaction monitoring mechanisms are effective in preventing fraud, while mitigating the impact on legitimate payment transactions and customer detriment deriving from delays in the execution of legitimate payment transactions or the blocking of such transactions. For the purpose of this Regulation, the fact that a payment order is unusual should not automatically constitute grounds for suspecting that the payment transaction is fraudulent, nor should it by itself constitute reasonable grounds to suspect fraud.
In assessing whether there are reasonable grounds to suspect fraud in relation to a payment transaction, the payment service provider should take into account the specific circumstances of the individual transaction, together with the payment service provider's wider assessment of evolving fraud risk based on the payment service provider's transaction monitoring or ~~and~~ on any ~~other~~ relevant information available to the payment service provider.
Where the payment service provider has duly justified and reasonable grounds to suspect fraud, a refusal in good faith to execute or the decision to block or postpone a payment transaction should not involve the payment service provider in liability ~~of any kind~~.

Recital 103a

Timely sharing of relevant fraud data amongst payment service providers and with payment service providers and relevant national authorities to enhance their transaction monitoring mechanisms plays an important role in achieving the objective of timely detection and prevention of fraudulent payment transactions. In some cases, different data sharing frameworks under other relevant Union legislation may apply to the data being shared. To ensure legal certainty regarding the conditions under which payment service providers shall ~~can~~ share fraud-related information for the purpose of fraud prevention, including ~~also~~ with the relevant national authorities, the conditions under which such data sharing is allowed under this Regulation should be specified. Information sharing should be subject to robust safeguards, in conformity with Regulation (EU) 2016/679 in relation ~~relating~~ to confidentiality, data protection and the use of information. This should be without prejudice to the requirements under the AMLR not to disclose that a suspicious transaction has been reported to the FIU or that an internal analysis into ML and TF is being carried out, and should not lead to jeopardizing an AML/CFT investigation.

Recital XX

In order to allow the payment service user to protect itself, the payment service provider and the payment service user shall agree in the framework contract on a limit of a maximum amount that can be sent for each means of payment, including credit transfers, and for each payment instrument. Furthermore, it should be possible for the payment service user to set different limits for each means of payment and each payment instrument. This should be agreed upon between the payment service user and the payment service provider in the framework contract.

Article 51 Spending ~~L~~limits, ~~and~~ blocking of the use of the payment instrument and the secure activation of a mobile application

1. ~~Upon request of the payment service user,~~ The payment service user and the payment service provider shall agree in the framework contract ~~on spending limits for payment transactions executed through a credit transfer or a~~ shall offer to the payment service user the possibility of ~~setting~~ on a limit of a maximum amount that can be sent for each means of payment, including for credit transfers, ~~or another~~ and for each payment instrument. It shall be possible for the payment service user to set different ~~These~~ limits ~~can be specific~~ for each means of payment and each payment instrument, which may be ~~either~~ on a per-day or per-transaction basis, at the sole discretion of the payment service user. Payment service providers shall ensure that the payer is able to modify the spending limits set prior to the placing of a payment order. An increase of the spending limit by the payer, if done remotely, shall require the application of strong customer authentication in accordance with Article 85 (1)(d).

1a. ~~The Pp~~ayment service providers shall not unilaterally increase the spending limits agreed with their payment service users. ~~Where agreed in the framework contract between the payment service provider and the payment service user~~ Payment service providers shall ~~may~~ require a ~~reasonable~~ delay of maximum 12 hours ~~specified in the framework contract~~ for any resulting increase in spending limits to come into effect. Payment service users shall have the right to opt out of the application of a delay period. ~~Such delay shall not exceed [xx]. The payment service provider shall enable the payer to opt out from the application of such a delay period.~~ Where a delay period is in place, any subsequent opting out of its application shall be subject to the delay period. The opt-out shall require the application of strong customer authentication in accordance with Article 85 (1)(d).

1b. Payment service providers shall immediately notify payment service users, in an agreed manner, when a spending limit is modified or when the opt-out referred to in the previous paragraph is exercised.

1c. Where a payment service user's payment order exceeds, or leads to exceeding of the maximum amount, the payer's payment service provider shall not execute the payment order and shall inform the payment service user of the reasons thereof and how to modify the maximum amount.

2. ~~As~~ If agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument ~~or refuse the execution~~ for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, when the payment instrument is used by the payment service user for activity that is prohibited by other relevant Union or national law, or in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil its liability to pay. ~~Where such blocking does not take place despite reasonable grounds for suspecting fraud, the payer shall not bear any financial consequences, except where the payer has acted fraudulently.~~

3. In such cases the payment service provider shall inform the payer of the blocking of the payment instrument and the reasons for it in an agreed manner, where possible before the payment instrument is blocked and at the latest immediately thereafter, unless providing such information ~~would compromise objectively justified security reasons or~~ is prohibited by other relevant Union or national law.

4. The payment service provider shall ~~not execute the refused~~ unblock the payment instrument ~~transaction~~ or replace it with a new payment instrument once the reasons for blocking no longer exist, ~~unless the payment service user confirms his / her consent in a safely manner~~.

5. Where the payment service provider offers the payment service user the possibility to execute payment services by means of a mobile application, the payment service provider shall require strong customer authentication to activate the application on a new device.

The payment service provider shall require a delay for the activation of the application to take effect. The payment service user shall have the right to opt out of the application of such a delay period. The opt-out shall require the application of strong customer authentication in accordance with Article 85 (1)(d).

5a. The payment service provider shall immediately notify the payment service user, in an agreed manner, of the activation of a mobile application linked to its payment account on a new device. The notification shall include instructions in case the payment service users have not installed the mobile application themselves.

The procedure for the notification referred to in this paragraph shall be agreed between the payment service user and the payment service provider.

5b. Where the payment service user notifies the payment service provider that they have not activated the mobile application linked to their payment account in accordance with the procedure referred to in paragraph 5a, the payment service provider shall ensure that the intended mobile application does not make it possible to access the payment account of the payment service user or execute payment transactions.

Article 65 Refusal to execute a payment order

1. Where all of the conditions set out in the payer's framework contract are met, the payer's payment service provider shall not refuse to execute an authorised payment transaction, irrespective of whether the payment order is placed by a payer, including through a payment initiation service provider, or by or through a payee, unless the execution of the payment transaction would be prohibited by other relevant Union or national law.

1a. By way of derogation from paragraph 1~~exception from the above~~, ~~if agreed in the framework contract~~, the payer's payment service provider shall ~~may~~ refuse to execute a~~n authorised~~ payment transaction where, based on the transaction monitoring referred to in Article 83 and on any other relevant information available to the payment service provider, the payment service provider has duly justified and reasonable grounds to suspect ~~fraud against the payment service user~~ that the transaction is fraudulent.

For the purpose of this Regulation, the fact that a payment order is unusual shall not by itself constitute reasonable grounds to suspect fraud.

Without prejudice to Article 69(1), where based on the transaction monitoring referred to in Article 83 and on any other relevant information available to the payment service provider, the payer's payment service provider suspects that the payer may be a victim of fraud, the payer's payment service provider shall, without undue delay, notify the payer, in an agreed manner, of any information or action needed from the payer to enable the payment service provider to decide whether there are reasonable grounds to suspect that the transaction is fraudulent ~~fraud~~. The notification shall give the payer sufficient information to enable the payer to understand the risks that the payment service provider has identified. The payment service provider shall make all reasonable efforts to contact the payment service user.

The obligation in the previous ~~third~~ subparagraph shall not apply in the case of instant credit transfers. [moved for clarity]

Where it is not possible for the payer's payment service provider to contact the payer within the timelines specified in Article 69(1), and in the case of instant credit transfers, the payment service provider shall assess, based on the transaction monitoring referred to in paragraph 1, and on any other relevant information available to the payment service provider, whether or not to execute the payment order.

~~The obligation in the third subparagraph shall not apply in the case of instant credit transfers.~~

2. *~~1.~~ Where the payment service provider refuses to execute a payment order or to initiate a payment transaction, the payer's payment service provider shall notify the payer and, where applicable, the payment initiation service provider, of the refusal and~~, if possible,~~ the reasons for that refusal and the procedure for correcting the decision to refuse to execute the transaction ~~any factual mistakes that led to the refusal~~ ~~to the payment service user~~, unless prohibited by other relevant Union or national law.*

The payment service provider shall provide or make available the notification in an agreed manner ~~at the earliest opportunity~~ and without undue delay, and in any case within the periods specified in Article 69. In the case of instant credit transfers in euro, the payer's payment service provider shall provide or make available the notification of the refusal within 10 seconds of the time of receipt of the payment order by the payer's payment service provider, and provide the reasons for the refusal without undue delay, unless prohibited by other relevant Union or national law.

The framework contract may include a condition that the payment service provider may charge a reasonable fee for such a refusal if the refusal is objectively justified, but not in the case of a refusal due to a suspected fraudulent transaction.

~~2. Where all of the conditions set out in the payer's framework contract are met, the payer's account servicing payment service provider shall not refuse to execute an authorised payment transaction irrespective of whether the payment order is placed by a payer, including through a payment initiation service provider, or by o through a payee, unless prohibited by other relevant Union or national law.~~

~~3. Where the conditions laid down in Article 71(1) of Regulation (EU) 2024/1624 are met, if agreed in the framework contract, the payment service provider may reserve the right to refuse to execute a payment transaction where the risk assessment conducted by the payment service provider pursuant to Article 71(1) of Regulation (EU) 2024/1624 indicates a high risk of fraud to the payment service user.~~

~~4. Before refusing to execute a payment order, or in the case of an instant credit transfer, immediately after the refusal of the payment order, the payment service provider shall notify the payer of the refusal and the reasons for it, in an agreed manner at the earliest opportunity, and in any case within the periods specified in Article 69, or, in case of instant credit transfers in euro, within 10 seconds of the time of receipt of the payment order by the payer's payment service provider. Information about the reasons for refusal may not be provided if this would compromise objectively justified security.~~

Article 69 Payment transactions to a payment account

1. […]

2a. If, based on the transaction monitoring ~~mechanisms~~, referred to in Article 83, or on any relevant information available to the payment service provider, there are ~~indicate~~ reasonable grounds to suspect a fraudulent payment transaction from either the payer's payment service provider or the payee's payment service provider, ~~then~~ the payee's payment service provider may postpone making the funds available to the payee. The payee's payment service provider shall without undue delay~~, as necessary,~~ and within a maximum of two working days, ascertain whether the transaction is in fact fraudulent, and either make the funds available to the payee or, if the transaction is deemed fraudulent, return the funds to the payer's payment service provider. The payee's payment service provider shall notify the payer's payment service provider of the assessment that is being conducted.

3. […]

Article 83 Transaction monitoring mechanisms

1. […]

1a. The payment service provider of the payer shall carry out the transaction monitoring referred to in paragraph 1 prior to the execution of a payment transaction. Without prejudice to Article 69(2), the payment service provider of the payee shall also carry out transaction monitoring of received payment transactions.

Where such monitoring does not take place in a specific transaction, the payer shall not bear any financial consequences from that specific transaction, except where the payer has acted fraudulently.

Where the payer has acted with gross negligence, the liability for the damage incurred shall be shared between the payer and the payer's payment service provider. The exact share of liability shall depend on the scope of the fault of each party.

The burden to prove that there was no breach of this Article shall be on the payment service provider.

1b. *Without prejudice to this Article, the provisions of Chapter 4 of this Regulation are applicable in cases when the payment service user is entitled to a refund from the payment service provider of a fraudulent payment transaction based on the liability shift in this Article.* ~~*The payment service provider shall operate transaction monitoring mechanisms in order to track the payment service user's transactions executed on his payment accounts with that payment service provider and to have access to, collect, analyse and consolidate the following data with a view to identifying the payment service user's usual transactions in order to prevent and detect potentially fraudulent transaction, support the application of strong customer authentication:*~~

~~*a) the amount of the payment transactions,*~~

~~*b) the payment instruments used by the payment service user,*~~

~~*c) the types of transactions carried out by the payment service user,*~~

~~*d) the dates of the transactions executed,*~~

~~*e) based on the process/execution arrangements and policy/principles/ of payment service providers the electronic transactions executed by the payment service user, including the environmental and behavioural characteristics which are usual of the payment service user in the circumstances of a normal use of the personalised security credentials.*~~

~~*The data referred to in points a) to e) shall be aggregated in order to identify the usual behaviour of the payment service user.*~~

2. Transaction monitoring mechanisms shall be based on the analysis of previous payment transactions and access to payment accounts online. Processing by the payment service provider of the payer shall be limited to the following data required for the purposes referred to in paragraph 1:

(a) *information on the payer, including the environmental and behavioural characteristics which are typical of the payer in the circumstances of a normal use of the personalised security credentials;*

(b) *information on the payment account, including the payment transaction history;*
(c) *transaction information, including the transaction amount, currency, date, time of execution and unique identifier of the payee;*
(d) *session data, including the device internet protocol address range from which the payment account has been accessed, from which the transaction was initiated and from which the transaction was authenticated;*
(e) *device data, including device identifiers from which the transaction was initiated and from which the transaction was authenticated.*

Processing by the payment service provider of the payee shall be limited to the following data required for the purpose referred to in paragraph 1, as applicable:
(a) information on the payee;
(b) information on the payment account of the payee, including the payment transaction history;
(c) transaction information, including the transaction amount, currency, date, time of execution, as well as the name of the payer and of the beneficiary.
(d) session data;
(e) device data, including device identifiers.

~~*3. Without prejudice to Article 69 and 71 of the Regulation (EU) 2024/1624 of the European Parliament and of the Council, the payment service provider of the payer and the payee shall monitor payment transactions before the execution of the transaction in order to identify unusual transactions.*~~

Article 83a Fraud data sharing

1. Payment service providers shall ~~may~~ exchange ~~the following~~ data with other payment service providers who are subject to an information sharing arrangement as referred to in paragraph (3) to the extent strictly necessary to comply with their obligations in Article 83(1), point (c). The catalogue of data that may be shared shall include, but not be limited to:
(a) the unique identifier of a payment service user ~~payee~~;
(b) the name of the payment service user ~~payee~~;
(c) the personal identification number or organisation number of the payment service user ~~payee~~, where applicable;
(d) payment instrument if applicable;
(e) transaction data, including the transaction amount, currency, date and time of execution;
(f) session data related with the potentially fraudulent transaction, including the internet protocol address-range from which the payment account has been accessed;
(g) device data related with the potentially fraudulent transaction, including device identifiers;
(h) the modus operandi of a fraud or suspected fraud;
(i) contact details, including e-mail address and telephone number of the payment service user.

1a. ~~A pP~~ayment service provider~~s~~ shall ~~may~~ exchange such data with other payment service providers who are subject to an information sharing arrangement as referred to in paragraph 3 where: the payment service provider has reasonable and objective grounds to suspect a fraudulent behaviour by a payment service user. ~~Where such exchange of information does not take place, the payer shall not bear any financial consequences, except where the payer has acted fraudulently~~.
The information referred to in the first subparagraph shall only be exchanged to the extent that it is necessary for the purposes of complying with the obligation under Article 83(1), point (c).
[…]
2. Payment service providers shall not keep data obtained following the information exchange referred to in this paragraph and paragraph 1 for longer than it is necessary for the purposes laid down in Article 83(1a) [but no longer than ~~5~~3 years after the suspected fraudulent transaction has taken place].

[…]
6. For the purposes of this Article [83a], Member States shall ensure that appropriate measures are in place so that payment service providers are also able to share the data referred to in paragraph 1 with the relevant national authorities in accordance with national law.

Recital XXX

When developing measures to combat fraud in the area of payments services, it is of particular importance to carry out appropriate consultations that involve the relevant stakeholders in order to exchange best practices and experiences of individual stakeholders. Consultations should build on the advice of both public- and private-sector experts who have proven knowledge and experience in the relevant areas. For that purpose, the Commission should set up a Platform on combating fraud (the 'Platform'). The Platform should be composed of experts representing both the public and private sectors. Experts should include, at least, representatives of the European Data Protection Board, the Body of European Regulators for Electronic Communications, the European Board for Digital Services, the European System of Central Banks, Europol, the European Retail Payments Board, payment service providers, technical services providers and consumer organisations. Private sector experts should also include representatives of relevant stakeholders and persons with proven knowledge and experience in the field of payment services fraud.

Recital XXY

The Platform should be constituted in accordance with the applicable horizontal rules on the creation and operation of Commission expert groups, including with regard to the selection process. The selection process should aim to ensure a high level of expertise, geographical and gender balance, as well as a balanced representation of relevant know-how, taking into account the specific tasks of the Platform. During the selection process, the Commission should perform an assessment in accordance with those horizontal rules to determine whether potential conflicts of interest exist and should take appropriate measures to resolve any such conflicts.

Recital XXZ

The Platform should advise the Commission on the development, monitoring the implementation of legal acts aimed at combatting fraud in the area of payment services. The Platform should also share information on and analyse trends in fraud in the area of payment services. The Platform should advise the Commission on measures to combat fraud in the area of payments services, including mitigation measures, as well as on ways to improve cross-border and cross-sectoral cooperation on the means of combatting fraud in the area of payment services.

Article XXX [Platform on combatting fraud]

1. The Commission shall establish a Platform on combatting fraud in the area of payments services in the Union (the 'Platform'). Its composition shall include at least ~~be a balanced mix of~~ the following groups:
(a) representatives of:
(i) the European Data Protection Board;
~~(ii) the EBA;~~
(iii) the Body of European Regulators for Electronic Communications (BEREC);
(iii~~v~~) the European Board for Digital Services, established under Article 61 of Regulation (EU) 2022/2065;
(iv) members of the European System of Central Banks;

(vi) Europol;
(vii) the European Retail Payments Board;
(viii) payment service providers;
(viiiix) Technical Services Providers;
(ix) consumer organisations;
(b) experts representing relevant stakeholders, including card schemes, merchants, consumers, businesses, providers of online platforms, telecommunication providers, internet service providers;
(c) experts, appointed in a personal capacity, with who have proven knowledge and experience in the field area of fraud in the area of payment services fraud.

The EBA and the representatives of national competent authorities will possess observer status on the Platform.

2. The Platform shall:
(a) advise the Commission on developing and monitoring the implementation of legal acts aimed at combatting fraud in the area of payment services;
(b) share information on and analyse trends in fraud in the area of payment services, based inter alia on statistics developed by the EBA and the ECB;
(c) advise the Commission make recommendations on measures to combat fraud in the area of payments services, including mitigation measures; that may be taken by all relevant parties, taking into account, among other things:
- *existing measures;*
- *existing legislative frameworks;*
- *levels of risk and exposure;*
- *position in the fraud chain and;*
- *business type;*

(d) monitor the effectiveness of any measures implemented under (c);
(e) share information on new threats and obstacles in preventing fraud;
(dg) advise the Commission make recommendations on ways to improve cross-border and cross-sectoral cooperation on the means of combatting fraud in the area of payment services.

3. The Platform shall take into account the views of a wide range of stakeholders and collaborate with other relevant groups and stakeholders focused on tackling scams and fraud.

3.4. The Platform shall be chaired by the Commission and constituted in accordance with the horizontal rules on the creation and operation of Commission expert groups. In that context, the Commission may invite experts with specific expertise on an ad hoc basis.

5. The Platform shall carry out its tasks in accordance with the principle of transparency. The Commission shall publish the minutes of the meetings of the Platform and other relevant documents on the Commission website.

6. The Platform shall report annually on its activities to the European Parliament and the Council.