Council of the European Union
General Secretariat

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

Brussels, 24 April 2025

WK 5225/2025 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

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, 29 April 2025

Presidency Discussion Note on fraud prevention

Platform on combatting fraud

In their responses following the 19 March CWP, many Member States were generally in agreement with the proposed new wording of the article with accompanying recitals with regard to the creation of a dedicated platform on combatting fraud in the area of payment services in the Union. There were, however, divergent opinions regarding the platform participants and their status. Some Member States proposed new entities to be included in the list, while others opted to simplify the provisions in L1, deleting further details. In order not to leave out any participants who could contribute to the work of the Platform, the Presidency proposes to leave this matter to the European Commission's discretion, while including an open-ended list of such entities in the recitals. We believe that this approach will provide the necessary flexibility in this regard.

Moreover, in light of the new Article 59a(3) regarding the cooperation with ECSPs, we inserted a reference to the voluntary code of conduct to be facilitated pursuant to that provision. One Member State pointed out that the proposal focuses on advising the Commission, signalling a considerable focus on the role of the Commission as the central problem-solver. This Member State suggested giving participants in the Platform a more active role in advising each other as well, sharing best practices and presenting initiatives on combatting fraud, without necessarily having the Commission involved directly. Another Member State reported that it would be preferable to include a clarification in the recitals that the platform should not duplicate but rather support the activities of other (current or future) national or European initiatives to combat fraud, in order to benefit from synergies. Some Member States also expressed their preference to reintroduce the recently deleted transparency and reporting obligations of the Platform, arguing that the regular publication of the Platform's discussions and outputs may be relevant for market stakeholders to accommodate identified best practices and emerging techniques for combatting fraud, and that both the EP and the Council should be regularly informed about the work of the Platform in order to be able to judge its effectiveness.

See the proposed wording of Article 83aa and Recitals 105a, 105b and 105c PSR in the annex.

> ***Q1.*** *Could Member States accept the proposed wording of the provisions concerning the Platform on combatting fraud?*

Spending limits and 'cooling-off' periods

In the comments sent to the Presidency after the 19 March CWP, many Member States agreed with the direction of the amendments proposed by the Presidency. However, some Member States requested that the provisions more clearly explain that the PSU will be able to choose both per-day and per-transaction limits simultaneously. Some Member States pointed out that it should be clarified that PSUs should be able to personalise and adjust cooling-off periods if needed. A few Member States questioned the recently introduced maximum 12-hour delay period for the increase in spending limits to come into effect. These Member States argued that the minimum length of the delay was left open, which would lead to the PSP being required to apply a delay of 0 to 12 hours, making the cooling-off period redundant. It was therefore suggested that a minimum period (rather than a maximum), and the possibility for PSUs to adjust it if needed, should be introduced into the provisions. One Member State proposed adding a similar condition as is provided for in Article 51(1) to Article 51(1a), stating that the requirement to apply SCA should be necessary in the event of opt-out, if done remotely (not in the PSP's physical locations). Another Member State drew attention to the fact that in the current version of the provisions it is not possible for PSUs to opt out of the application of spending limits, which would be desirable, especially for business PSUs. One Member State suggested further

amending paragraph 1a to clarify that PSPs must not unilaterally change (and not just increase) the spending limits agreed with PSUs. In addition, in Recital 73b we clarified that initial limits are the same for instant and other types of credit transfers and that subsequent requests for increase or decrease in the limit would be on the request of the PSU. We have also included in Article 20(b)(vii) that the payment service provider shall provide to the payment service user the information about possible spending limits, the length of the cooling-off period and explanations how the PSU can modify it or opt-out of its application.

In addition, in previous discussions some Member States had pointed out inconsistencies between the proposed provisions and the IPR. In the responses to the Presidency's questionnaire, the majority of Member States agreed that the PSR provisions should override the IPR provisions as they provide enhanced security for PSUs. Some Member States asked for this to be clearly stated in the text.

See the proposed wording of Recital 73b and Article 20(b)(vii), Article 51(1), (1a) and (6) PSR in the annex.

> ***Q2.*** *Could Member States accept the proposed wording of Recital 73b, Article 20(b)(vii), Article 51(1), (1a) and (6) PSR?*

Security of the activation of a mobile application on a new device

The comments made by Member States following the 19 March CWP indicated broad support for the proposed provisions on the security of the activation of a mobile application on a new device. Many Member States have accepted the proposed wording in its entirety, which is why the Presidency is suggesting only a few further amendments related to points raised by some Member States, mainly to bring the wording in line with the rest of Article 51. For example, one proposal was to add that, where a delay period is in place, any subsequent opting out of its application should be subject to the delay period, or that the delay period should have the same timeframe as set out in Article 51(1a). One Member State pointed out the need to amend the wording, as a transaction is not executed, but rather initiated, through the application. This Member State also suggested including in Article 51(5b) a time limit for PSPs to react after being notified by a PSU that they did not activate the mobile application linked to their payment account themselves. A recital explaining these provisions has also been proposed.

See the proposed wording of Recital 73c and Article 51(5) and (5b) PSR in the annex.

> ***Q3.*** *Could Member States accept the proposed wording of Recital 73c and Article 51(5) and (5b) PSR?*

Freezing of funds by the payee's PSP and blocking of the use of the payment instrument and refusal to execute a payment order in the event of reasonable grounds to suspect fraud

The Presidency noted that there was broad support for the proposal to add tools for the payee's PSP to freeze funds in the event of a suspected fraudulent transaction. However, some Member States pointed out that a timeframe of two days might not be adequate. Nevertheless, there were divergent opinions on whether to make it shorter or longer; therefore, the Presidency decided not to change the timeframe. One Member State pointed out that a provision should be added on informing the payee if the funds are blocked – the payer will claim that the money has been transferred but the payee will not see it in their balance yet, which can often be problematic in trade and have undesirable consequences (e.g. buying tickets for a sports match or a ski pass in an auction, where a delay of two working days could mean that it is too late).

In their written comments, a significant number of Member States also considered that a similar timeframe should be introduced for the payer's PSP with regard to the blocking of transactions (amendments introduced in Article 51(3)). To this end the Presidency introduced also some further amendments with the aim of aligning the wording in Article 51 and 69(2a). At the same time, another Member State pointed out that the interplay of such time periods should be clarified with regard to Article 69 in order to ensure legal certainty (amendments introduced in Article 51(2) and Article 69(2a) PSR).

In addition to the drafting improvements in Recital 69d, an explanation has been added, in line with one Member State's comment, that any unusual transaction could be an early indication of fraud, which should alert the PSP and should be further investigated.

See the proposed wording of Recital 69d, Article 51(2) and (3) and Article 69(2a) PSR in the annex.

The written comments sent to the Presidency following the 19 March CWP indicated significant support for the proposals on blocking the use of the payment instrument and refusing to execute a payment order in the event of reasonable grounds to suspect fraud. Nevertheless, some improvements were suggested. Some Member States pointed out that in Article 65(1a) the word '*and*' should be changed to '*or*' in the reference to '*transaction monitoring mechanism and any other relevant information*' as valid reasons for blocking. A few Member States indicated that the reference to instant credit transfers in Article 65(2) should apply to all Member States' currencies, not just the euro. One Member State suggested some further amendments to harmonise the wording in Article 65(1a). Another Member State advised that in Article 65(2), second subparagraph, the wording '*provide or make available*' is not appropriate for the type of information mentioned and suggested using only the word '*provide*'. Moreover one Member State requested redrafting of Article 65(1) and (1a) to provide that both provisions (i.e. the obligation to execute authorized payment transactions and the possibility for the PSP to refuse a payment) are without prejudice to the obligation to refrain from executing transactions under art. 71 AMLR.

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

> ***Q4.*** *Could Member States accept the proposed wording of Recital 69d, Article 51(2) and (3), Article 65(1), (1a) and (2) and Article 69(2a) PSR?*

Obligation of the PSP to conduct transaction monitoring

In their written comments following the 19 March CWP, a significant number of Member States signalled that the shared liability between PSPs and PSUs as proposed in Article 83(1a) is too complex and might prove difficult to apply in practice. It was pointed out that PSPs will have discretionary power to decide on the share of liability for each party and this might be disadvantageous to PSUs, i.e. result in PSUs having to bear the lion's share of the losses. It would also create major problems for dispute resolution bodies, because evaluating a PSU's possible negligence together with a PSP's failure to use transaction-monitoring mechanisms would be extremely difficult. Some Member States pointed out that the idea of sharing liability in some cases of gross negligence would be rational, but not if the PSP has not applied efficient transaction-monitoring mechanisms. Proper monitoring should be a prerequisite for the PSP before any shared liability can be applied. One Member State also suggested that it is not appropriate to have a reference to gross negligence in Article 83, as PSPs tend to systematically use gross negligence to escape liability and there is a risk that PSPs will be encouraged to use gross negligence to escape the obligation to carry out adequate and robust transaction monitoring, which would ultimately undermine the effectiveness of the transaction monitoring. In the light of the above, the Presidency decided to delete the recently proposed provisions on shared liability. In addition, in Article 83(2), second subparagraph, one Member State suggested removing the reference to the name of the beneficiary in point (c), as it is already covered by the information of the payee provided for in point (a). There was also a suggestion to narrow the scope of the data which can

be shared under point (a) to data on the payer's identity and contact details, so as to exclude "the environmental and behavioural characteristics which are typical of the payer in the circumstances of a normal use of the personalised security credentials", as this would be too far-reaching.

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

Q5. *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 19 March CWP, many Member States supported the amendments proposed by the Presidency with regard to information sharing. However, at the same time a noticeable number of Member States were concerned about GDPR compliance issues. The Presidency therefore decided to introduce a closed list of data to be shared, which is in line with the opinion presented at the meeting by the CLS. It also serves legal certainty: if there is an obligation to share, but it is not clear which types of data the obligation concerns, the PSPs will not know what they are meant to share. Some Member States requested that the possibility of sharing information with national authorities be better reflected in the actual Level I text, and not only in the recitals. One Member State suggested that data sharing should be possible not only to comply with Article 83(1), point (c), but also to exchange data with national authorities and with supervisory authorities, which should be reflected in Article 83(1). Another Member State called for clarity on the relationship between Article 83a(1) and (1a), as they appeared to have nearly the same content. Another Member State pointed out that for GDPR compliance reasons it is imperative that the data lists in Articles 83 and 83a PSR match. There were also a few suggestions for improving the wording.

See the proposed wording of Recital 103a, Article 83(1) and Article 83a PSR.

Q6. *Could Member States accept the proposed wording of Recital 103a, Article 83(1) and Article 83a PSR?*

Annex

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. However, any unusual transaction could constitute an early indication of fraud, which should alert the payment service provider and should be further investigated. 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 a ~~the~~ decision to ~~block or~~ postpone a payment transaction or to block a payment instrument should not involve the payment service provider in liability ~~of any kind~~.

Recital 73b ~~XX~~

In order to allow the payment service user to protect itself, the payment service provider and the payment service user should ~~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. Limits agreed initially in the framework contract should be the same for different types of credit transfers, so that payment services users are not unknowingly prevented from having the same access to instant credit transfers as to other types of credit transfers. Subsequently, payment services users shall be able to request an increase or a decrease of the limits applicable to instant credit transfers as provided for in Regulation (EU) 260/2012.

Recital 73c [new]

As payment services become increasingly digital, many payment service providers are offering payment service users the possibility of using mobile applications to initiate payment services. While these mobile applications are useful and beneficial to payment service users, they also pose a fraud risk. To prevent this risk, the process of activating a mobile application on a new device should require the application of strong customer authentication. The payment service provider and the payment service user should agree on a delay for the activation of the application to take effect in order to allow the payment service user to intervene if they are not the one activating the mobile application. The payment service user should have the right to opt out of the application of such a delay period, in which case the application of strong customer authentication should be required.
The payment service provider should also notify the payment service user in a secure manner of the activation of a mobile application linked to their payment account on a new device. The purpose of the notification is to increase the vigilance of the payment service user and should enable the payment

service user to alert the payment service provider if they have not installed the mobile application themselves. In that case, the payment service provider should ensure that the intended mobile application does not allow access to the payment account of the payment service user or the initiation of payment transactions.

Recital 103a

Timely sharing of relevant fraud data amongst payment service providers and also 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 should ~~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 money laundering ~~ML~~ and terrorist financing ~~TF~~ is being carried out, and should not lead to jeopardizing an AML/CFT investigation.

Recital 105a ~~XXX~~ [on Platform on combatting fraud]

When developing measures to combat fraud in the area of payment~~s~~ 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 ~~P~~platform on combating fraud (the 'Platform'). The Platform should be composed of experts, which could be ~~representing the abovementioned sectors both the public and private sectors. Experts may be~~ selected, for example, from ~~should include, at least,~~ representatives of relevant European bodies, national competent authorities, ~~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, providers of online platforms, telecommunication providers, internet service providers, experts representing card schemes, merchants, ~~and~~ consumer organisations, and dispute resolution bodies. ~~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 105b ~~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 105c ~~XXZ~~

The Platform should advise the Commission on developing ~~the development~~ and the~~,~~ monitoring of 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, as well as ~~. The Platform should advise the Commission~~ share information on measures to combat fraud in the area of payment~~s~~ services, including mitigation measures, and ~~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. The Platform should carry out its tasks in accordance with the principle of transparency. It should also take into account the work of existing initiatives to combat payment fraud, avoiding duplication, and work closely with them.

Article 20 Information and conditions

[…]

(b) on the use of the payment service: […]

(vii) whether there is a possibility to agree on spending limits for the use of the payment instrument in accordance with Article 51(1) with information on the length of a delay for any resulting increase in spending limits to come into effect and description how the payment service user can adjust or opt-out of the application of a delay period; […]

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. The payment service user shall have the right to opt out of the application of spending limits. 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, or both, 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 P~~payment service providers shall not unilaterally modify ~~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 a minimum of six hours ~~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 adjust or 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, if done remotely, 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~~ By way of derogation from Article 69(1), 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. The payer's payment service provider shall without undue delay, as necessary, and within a maximum of two working days, assess ~~ascertain~~ whether the reasons to block the payment instrument are still justified ~~transaction is in fact fraudulent~~.

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 initiate ~~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 of a minimum of six hours for the activation of the application to take effect. The payment service user shall have the right to adjust or opt out of 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, if done remotely, 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 without undue delay ensure that the

intended mobile application does not make it possible to access the payment account of the payment service user or initiate ~~execute~~ payment transactions.

6. For the purposes of this Regulation, the provisions in para. (1) and (1a) shall also apply to credit transfers in scope of the Regulation (EU) 260/2012. In the event of a conflict between this Article and the provisions of Regulation (EU) 260/2012, this Article shall apply.

Article 65 Refusal to execute a payment order

1. Where all of the conditions set out in the payer's framework contract are met, and without prejudice to the obligation to refrain from executing the transaction under article 71 AMLR, 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 relevant Union law provides otherwise. ~~the execution of the payment transaction would be prohibited by other relevant Union or national law~~.

1a. By way of derogation from paragraph 1 and without prejudice to the obligation to refrain from executing the transaction under article 71 AMLR ~~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 or ~~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 or ~~and~~ on any other relevant information available to the payment service provider, the payer's payment service provider suspects that the transaction is fraudulent ~~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 payer ~~payment service user~~.

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

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. By way of derogation from paragraph 2 and without prejudice to the obligation to refrain from executing the transaction under article 71 AMLR, 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, assess ~~ascertain~~ whether the reasons for such postponement are still justified ~~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 and the payee of the assessment that is being conducted.

3. […]

Article 83 Transaction monitoring mechanisms

1. Payment service providers shall have transaction monitoring mechanisms in place that:
(a) support the application of strong customer authentication in accordance with Article 85;
(b) exempt the application of strong customer authentication based on the criteria under Article 85(11), subject to specified and limited conditions based on the level of risk involved, the types and details of the data assessed by the payment service provider;
(c) enable payment service providers to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services;
(d) enable payment service providers to inform competent national authorities for the purpose of a possible criminal investigation;
(e) enable payment service providers to establish accountability towards supervisory authorities.

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 payment service provider shall bear liability for the damage incurred. 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 and~~,~~ 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), and with the relevant national authorities, to the extent strictly necessary to comply with the obligations under Article 83(1), point (d), ~~The data shall be exchanged~~ where the payment service provider has reasonable and objective grounds to suspect fraudulent behaviour by a payment service user. The catalogue of data to ~~that may~~ be shared shall be limited to the data listed in Article 83(2). ~~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 pPayment service providers 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).~~
~~1b.~~ 1a. […]
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].
[…]

Article ~~XXX~~ 83aa [Platform on combatting fraud]

1. The Commission shall establish a Platform on combatting fraud in the area of payment~~s~~ services in the Union (the 'Platform'). Its composition shall ~~include at least~~ be a broad and balanced mix of representatives and experts from both the public and private sectors ~~of both public and private sector experts~~, who have proven knowledge and experience in the field of payment services fraud. ~~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);~~
~~(iiiv) 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;~~
~~(x) 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) issue recommendations to the Commission and the European Board of Digital Services for the purpose of the drawing up of the voluntary code of conduct referred to in Article 59a(3);
(~~b~~c) 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~~d) ~~advise the Commission~~ share information ~~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;~~
(~~d~~g~~e~~) ~~advise the Commission~~ share information ~~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.~~

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