Council of the European Union
General Secretariat

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

Brussels, 13 May 2025

WK 6227/2025 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 Summary 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, 15 May 2025

Presidency Summary Note on fraud prevention

Platform on combatting fraud

In their replies following the 29 April CWP, the majority of Member States were generally in agreement with the proposed text of Article 83aa and the accompanying recitals concerning the creation of a dedicated platform on combatting fraud in the area of payment services in the Union. The Presidency introduced only one further amendment – in Recital 105a we replaced 'experts representing card schemes' with 'experts representing different payment systems or schemes', as suggested by one Member State, in order to keep the list broad.

Spending limits and 'cooling-off' periods

On the basis of the comments made by Member States following the 29 April CWP, the Presidency decided to introduce some further amendments to Recital 73b, Article 20(b)(vii) and Article 51(1), (1a), (6) PSR. In Article 20, we have deleted the reference to the possibility of agreeing on spending limits, to align the text with Article 51, where it is mandatory. For the sake of clarification and in line with one Member State's suggestion, we have also added that the payment service provider shall provide the payment service user with a description of how to modify the spending limits. In Recital 73b, we have aligned the wording with Article 51 and deleted a part of the last sentence as it seemed to be in conflict with the introduced principle that PSR overrides IPR provisions. In Article 51, in line with the suggestions of some Member States, we have deleted the possibility of opting out of the application of spending limits, as it was argued that the existing right to modify the spending limits agreed in the framework contract seemed sufficient to safeguard the PSU's freedom. In addition, the requirement to set a limit may serve as a psychological incentive and reminder for the PSU to set reasonable spending limits. As some Member States were concerned that the deletion of the maximum delay period would give the PSP the ability the possibility for an unlimited delay, we have reintroduced the maximum delay period of twelve hours. In addition, as some Member States suggested that the minimum delay period of six hours was excessively long, we have reduced it to four hours. Two Member States pointed out that the adjustment of the delay period should also be subject to the application of the SCA and to a delay period already in place, so as not to give the fraudster the opportunity to circumvent the provisions and easily reduce the delay period, e.g. to one hour. We have also made some technical amendments to align and improve the wording of Article 51. Finally we have changed the wording in para. 6 , as it was suggested that this provision should not be limited to paragraphs 1 and 1a only, as other paragraphs of Article 51 also contain important provisions that should be applicable.

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

Firstly, the Presidency has introduced some changes to Article 51(5) in order to improve the wording and to align it with the changes introduced to Article 51(1a), as explained above. Secondly, at the request of one Member State, in para. 5 we added words 'or give consent', as the problem appears not only when the order is initiated by the newly registered mobile application, but also when the application is used for giving consent to any transaction or high-risk services using PIN or biometrics. Thirdly, two Member States suggested using different communication channels when activating a mobile application linked to the PSU's payment account on the new device and when notifying the PSU. It was argued that the main problem arises from the fact that the fraudster has illegally obtained the PSU's security credentials and hijacked the communication channel used by the PSP to send the PSU the link to download the application and link it to the PSU's account. In this case, the mere use of the SCA will not be sufficient to prevent the activation link or code from being sent to the fraudster. Finally, in Recital 73b we have added a clarification requested by one Member State to exclude from the application of the SCA and delay period situations, where the activation of mobile applications is

done directly by the PSP at its premises, as is often the case when opening a payment account or when assisting disabled or elderly people.

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

As some Member States have reported that the provisions on the freezing of funds and on the refusal to execute a payment order need to be better aligned with the GDPR, the Presidency proposes some redrafting of Articles 65(1a) and 69(2a) to this end. We have tried to formulate these paragraphs in such a way that the transaction is only suspended/postponed on the basis of the transaction monitoring or other relevant information available to the PSP, but then the additional assessments have to follow until a final decision is taken. In this way, only the initial decision to suspend/ postpone would be based on automated processing, after which further steps (notification, additional information, assessment) would have to follow. In Article 65(1), at the request of some Member States, we have reintroduced the reference to national law. Moreover we have also introduced some amendments to improve or align the wording of the provisions.

Transaction monitoring and fraud data sharing

In their written comments to the Presidency following the 29 April CWP, some Member States requested the reintroduction in Article 83(2) of the reference to environmental and behavioural characteristics typical of the payer in the circumstances of a normal use of the personalised security credentials, as this is an important factor in providing meaningful transaction monitoring mechanisms. In the same article, we modified the wording to emphasize the necessity criterion in personal data processing, which would strengthen the GDPR protection for this article. Some Member States strongly disagreed with the recently proposed new points (d) and (e) of Article 83(1). It was argued that this issue should be left to national law, and that the role of transaction monitoring mechanisms is not to inform the competent national authorities for the purpose of a possible criminal investigation. Moreover, in many EU countries there is a legal principle of secrecy of criminal investigations, so that these new points seem to be in contradiction with national laws. In the light of the above, the Presidency has decided to delete the recently proposed points (d) and (e) as well as any references to them.

The recently proposed draft, harmonised the lists of data in Articles 83 and 83a by aligning them with the transaction monitoring list, in order to ensure compliance with the GDPR. However, two Member States pointed out that the proposal removed important information from the catalogue of data that can be shared, namely the modus operandi of fraud or suspected fraud. We have decided to reintroduce this point in Article 83a in a more general manner and to clarify in the Recital 103a that a limitation in data sharing should only apply to personal data covered by data protection rules and not to non-personal data, such as information on the modus operandi of a fraud. At the same time, we have excluded from the data to be shared the reference to 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 burdensome and far-reaching and does not seem to relate directly to fraudulent behaviour.

Q1: Do Member States identify any red flags with regard to the fraud prevention provisions proposed in this Note?

Annex

Recital 73b

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 should ~~shall~~ be able to modify ~~request an increase or a decrease of~~ such ~~the~~ limits ~~applicable to instant credit transfers as provided for in Regulation (EU) 260/2012~~.

Recital 73c

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 use of different communication channels and 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 adjust or 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, and through different communication channels, 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. This should not apply to the activation of a mobile application on a new device of the payment service user, if done by the payment service provider at its physical premises.

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. However

to enable an efficient transaction monitoring, such safeguards should only apply for personal data falling under the data protection rules. In contrast, non-personal data, such as non-personalized information on the modus operandi of a fraud or suspected fraud, should be exchanged. This should be without prejudice to the requirements under ~~the~~ Article 73 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

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~~ different payment systems or 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.~~

Article 20 Information and conditions

[…]

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

(vii) ~~whether there is a possibility to agree on~~ the 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 modify the spending limits and 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 modify ~~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~~ If done remotely, ~~P~~payment service providers shall ~~may~~ require a ~~reasonable~~ delay of a minimum of four ~~six~~ hours and maximum of twelve ~~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, which, if done remotely, shall require the application of strong customer authentication in accordance with Article 85 (1)(d). ~~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 adjustment or opting out of its application shall be subject to the delay period in place. ~~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 or give consent to ~~execute~~ payment transactions ~~services~~ by means of a mobile application, the

payment service provider shall require strong customer authentication and the use of different communication channels to activate the mobile application on a new device, if done remotely.

If done remotely, ~~T~~the payment service provider shall require a delay of a minimum of four ~~six~~ hours and maximum of twelve hours for the activation of the mobile 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 adjustment or opting out of its application shall be subject to the delay period in place. The adjustment or 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, and through different communication channels, 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 or give consent to ~~execute~~ payment transactions.

6. ~~For the purposes of this Regulation, t~~The provisions ~~in~~ of this Article ~~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 prevail ~~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 or national 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 under the conditions provided for in this paragraph. ~~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 has duly justified and reasonable grounds to suspect~~s~~ that the transaction is fraudulent ~~payer may be a victim of fraud~~, the payer's payment service provider shall suspend the execution of a payment transaction. ~~, w~~

Without undue delay from the suspension of the transaction, unless prohibited by other relevant Union or national law, the payment service provider shall notify the payer, in an agreed manner, of any information or action needed from the payer to enable the payment service provider to assess, whether the reasons for such suspension are still justified ~~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. Within the timelines specified in Article 69(1), t~~T~~he payment service provider shall make all reasonable efforts to contact the payer before taking a decision regarding the suspended transaction ~~payment service user~~.

The obligation in the previous ~~third~~ subparagraph shall not apply in the case of instant credit transfers. In such cases, or w~~W~~here it ~~is not~~ has not been possible for the payer's payment service provider to receive information from ~~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.

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

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

2. ~~1.~~ Where, on the basis of the assessment in paragraph 1a, 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 from the discovery of the suspicion, assess ~~ascertain~~ whether the reasons for such postponement are still justified. ~~whether the transaction is in fact fraudulent, and~~ Moreover, without undue delay after the discovery of the suspicion, the payee's payment service provider shall notify the payer's payment service provider and the payee of the assessment that is being conducted, unless prohibited by other relevant Union or national law, in order to allow both the payee and the payer to express their views and where necessary, to contest the decision to postpone making the funds available. On the basis of this assessment, the payee's payment service provider shall 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, insofar as necessary to achieve the ~~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, payment instrument, if applicable, currency, date~~,~~ and time of execution, as well as ~~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, insofar as necessary to achieve the ~~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, payment instrument, if applicable, 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), including the payment service provider's account of the reasonable and objective grounds that gave rise to the suspicion of fraudulent behaviour on basis of that data. Information on the environmental and behavioural characteristics which are typical of the payer in the circumstances of a normal use of the personalised security credentials shall be excluded from data sharing under this Article. ~~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].
[…]