Council of the European Union
General Secretariat

PUBLIC

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

Brussels, 04 April 2025

WK 4475/2025 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.

REQUEST FOR CONTRIBUTION

From:	General Secretariat of the Council
To:	Working Party on Financial Services and the Banking Union (Payment Services/ PSR/PSD) Financial Services Attachés
Subject:	Consolidation of comments to the Presidency Questionnaire on PSR Art. 49 84 Ddl 24 March 2025 Replies from 20 MS

Ddl 24 March Cob

From: ES, SK, SE, PT, NL, MT, LV, LU, LT, IT, IE, HR, FI, EL, DK, DE, CZ, BG, BE, AT ***Updated: 02/04/2025 15:42***

PUBLIC

Note from the Presidency: The areas in light blue represent the provisions that are still under discussion and analysis - mainly the issues discussed at the Council Working Party meetings in January and February. Written contributions from Member States following these meetings are still being analysed.

Commission proposal	Legacy text of previous presidiencies	PL PRES drafing suggestions	MS drafting suggestions and comments
CHAPTER 4			DK (MS drafting suggestions and comments): Considering that the Presidency is working on incorporating the comments from the last WPs, we have limited our comments in this section. We support the work on this section and are optimistic that the Presidency will find a good compromise on fraud and fraud preventive measures based on the last meetings and written comments from these meetings. Generally, we support expanding the liability of PSPs. We also support expanding on requirements for ECSPs – however, it is important that those requirements are realistic and adjusted to the specific actors (telcos and digital platforms).

PUBLIC

Authorisation of payment transactions			
Article 49			
Authorisation			
			SK (MS drafting suggestions and comments): The Articles of this document are of great importance to us and we did articulate our stances on various provisions discussed below in the previous working parties. However, as the provisions are under discussion and will have to be closely assessed in the coming working parties, we will refrain from commenting on them at this stage.
1. A payment transaction or a series of payment transactions shall be authorised only if the payer has given its permission for the execution of the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the account servicing payment service provider, after the execution of the payment transaction.			FI (MS drafting suggestions and comments): FI: As a general remark, we are not commenting on the blue parts of the text as we are currently waiting for the PCY's next compromise proposal. EL (MS drafting suggestions and comments): **EL:** we agree with the Presidency's suggestion in returning to the European Commission's version of Article 49(1) (but with the word *permission* replaced by the word *consent*) and at the same time clarifying that in order for a transaction to be considered

			authorised, it needs to be both initiated and authenticated by the payer. As the above mentioned Option 1 of the February paper wk02161 was supported by the majority of MS (16 MS), we propose to introduce the following drafting "*A payment transaction shall not be deemed as authorised where the transaction was initiated by a third party using the personal security credentials of the payment service user fraudulently obtained".*
2. Access to a payment account for the purpose of account information services or payment initiation services by payment service providers shall be authorised only if the payment service user has given its permission to the account information services provider or, respectively, to the payment initiation service provider, to access the payment account and the relevant data in that account.			
3. In the absence of permission, a payment transaction or access to a payment account by			

PUBLIC

an account information service provider or a payment initiation service provider shall be considered to be unauthorised.			
4. Account servicing payment service providers shall not verify the permission given by the payment service user to the account information service provider or payment initiation service provider.			
5. The permission referred to in paragraphs 1 and 2 shall be expressed in the form agreed between the payer and the relevant payment service provider. Permission to execute a payment transaction may also be expressed via the payee or the payment initiation service provider.			
6. The procedure for giving permission shall be agreed between the payer and the relevant payment service provider.			
7. The payment service user may withdraw permission to			

PUBLIC

execute a payment transaction or to access a payment account for the purpose of payment initiation services or account information services may be withdrawn by the payment service user at any time. The payment service user may also withdraw permission to execute a series of payment transactions, in which case any future payment transaction shall be considered to be unauthorised.			
Article 50			
Discrepancies between the name and unique identifier of a payee in case of credit transfers			
1. In case of credit transfers, the payment service provider of the payee shall, free of charge, at the request of the payment service provider of the payer, verify whether or not the unique identifier and the name of the payee as provided by the payer			LU (MS drafting suggestions and comments): LU: consistency with the requirements set in IPR should be ensured. Further clarifications might be necessary for transactions where no IBAN is used.

PUBLIC

match, and shall communicate the outcome of this verification to the payment service provider of the payer. Where the unique identifier and the name of the payee do not match, the payment service provider of the payer shall notify the payer of any such discrepancy detected and shall inform the payer of the degree of that discrepancy.			
2. The payment service providers shall provide the service referred to in paragraph 1 immediately after the payer provided to its payment service provider the unique identifier and the name of the payee, and before the payer is offered the possibility to authorise the credit transfer.			
3. Payment service providers shall ensure that the detection and notification of a discrepancy as referred to in paragraph 1 does not prevent payers from authorising the credit transfer concerned. If the payer, after being notified about a			

PUBLIC

detected discrepancy, authorises the credit transfer and the transaction is executed in accordance with the unique identifier given by the payer, that transaction shall be deemed to have been executed correctly.			
4. Payment service providers shall ensure that payment service users have the right to opt out from being offered the service referred to in paragraph 1 and shall inform their payment service users of the means to express such opt-out right. Payment service providers shall ensure that payment service users that initially opted out from receiving the service referred to in paragraph 1, have the right to opt in to receive that service.			
5. Payment service providers shall inform their payment service users that authorising a transaction despite a detected and notified discrepancy or that opting out from receiving the service referred to in			

PUBLIC

paragraph 1 may lead to transferring the funds to a payment account not held by the payee indicated by the payer. Payment service providers shall provide that information at the same time as the notification of discrepancies or when the payment service user opts out from receiving the service referred to in paragraph 1.			
6. The service referred to in paragraph 1 shall be provided with respect to payment orders placed through electronic payment initiation channels and through non-electronic payment orders involving a real-time interaction between the payer and the payment service provider of the payer.			
7. The matching service referred to in paragraph 1 shall not be required where the payer did not input himself the unique identifier and the name of the payee.			
8. This Article shall not apply to instant credit transfers			

PUBLIC

denominated in euro falling within the scope of Regulation XXX (IPR).			
Article 51			
Limits and blocking of the use of the payment instrument			
1. Where a specific payment instrument is used for the purposes of giving permission, the payer and the payer's payment service provider may agree on spending limits for payment transactions executed through that payment instrument. Payment service providers shall not unilaterally increase the spending limits agreed with their payment service users.	1. ~~The payer and the payer's payment service provider shall offer to the payment service user the possibility to may~~ 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 means of payment or ~~another~~ payment instrument. These limits can be specific for each means of payment and each	1. ~~The payer and~~ Upon the request of ~~the payer's payment service provider shall offer to the payment service user the possibility to may~~ Tthe payment service user, ~~and~~ the payment service provider shall offer to the payment service user the possibility of setting a limit of a maximum amount that can be sent for each ~~agree in the framework contract on spending limits for payment transactions executed through a credit~~	ES (MS drafting suggestions and comments): The concept "means of payment" is introduced without a prior definition. We consider that this could result confusing, and, thus, we propose to remove this concept or to clearly define it. PT (MS drafting suggestions and comments): **Comments:** As this Article was discussed in the 19th of March CWP, PT will consider sending subsequent written comments on the newly proposed draft put forward by the PRES PL, which differs from the one presented here. NL (MS drafting suggestions and comments):

	payment instrument. ~~Payment service providers shall not unilaterally increase the spending limits agreed with their payment service users.~~ 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 shall require the application of strong customer authentication in accordance with Article 85 (1)(d).	~~transfer or a means of payment or~~ ~~another~~ 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 not unilaterally increase the spending limits agreed with their payment service users.~~ 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 shall	We support the introduction of a spending limit as a default. •As we have often noted, this is one of the most important measures against fraud. We are more in favour of making the cool-off period obligatory, so that consumers wont opt-out easily. Consumers can be tricked easily into opting out of this, so preventive measures should be in place in case a consumer chooses to opt out. LV (MS drafting suggestions and comments): We support. LU (MS drafting suggestions and comments): LU: in the absence of a definition for " means of payment" it is not clear what should be understood under "limits for each means of payment and each payment instrument" A reference to payment instruments seems sufficient. EL (MS drafting suggestions and comments): **EL:** We agree with the drafting suggestions for the possibility of setting up spending limits. Also clarify that the PSU should also be able to

		require the application of strong customer authentication in accordance with Article 85 (1)(d). *[**PRES comment**: The proposal presented at the January CWP meeting.]*	choose both types of limits simultaneously either per-day or per-transaction limits
	1a. The payment 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, the payment service provider shall be able to require a proper delay for any resulting increase of spending limits to come into effect.~~ Where a payment service user's payment order exceeds,	1a. The payment 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, the payment service provider may ~~shall be able to~~ require a reasonable ~~proper~~ delay specified in the framework contract for any resulting increase of spending limits to come	ES (MS drafting suggestions and comments): We agree with the proposal to keep a cooling off period when agreed in the framework contract. In order to prevent cases where the opt out is carried out under the manipulation of a fraudster, we propose to clarify that the opt out must be carried out through a procedure agreed between the PSU and the PSP: *The payment service provider shall enable the payer to opt out from the application of such a delay period **following the procedure agreed with the PSP.*** PT (MS drafting suggestions and comments): **Comments:**

	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.	into effect. 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. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	As this Article was discussed in the 19th of March CWP, PT will consider sending subsequent written comments on the newly proposed draft put forward by the PRES PL, which differs from the one presented here. NL (MS drafting suggestions and comments): 1a. The payment 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, the payment service provider may ~~shall be able to~~ require a reasonable ~~proper~~ delay specified in the framework contract for any resulting increase of spending limits to come into effect. Such delay shall have a minimum of at least 4 hours ~~not exceed [xx]. The payment service provider shall enable the payer to opt out from the application of such a delay period.~~ LV (MS drafting suggestions and comments): We support. EL

			(MS drafting suggestions and comments): **EL:** We agree with the drafting suggestions towards the possibility of setting up spending limits as well as with the application of a delay. Especially, regarding the delay, we believe that there should be some merit in analyzing the possibility of introducing this cooling off period requirement not only in changing spending limits, but on more actions i.e. high risk actions such amending personal information, change on SCA elements, device registration. In 2022, the Bank of Greece issued guidelines towards the PSPs for implementing measures to eliminate fraud in electroninc payments, where the delay is included as an option. We have also observed that a proper delay applied after a mobile device registration is also effective against fraud. DK (MS drafting suggestions and comments): Such delay shall not exceed 24 hours [we think this should not be less than 12 hours but would prefer 24 hours]. It should also be made sure that the PSP cannot let the period be 0 hours.

		1b. 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.	ES (MS drafting suggestions and comments): We agree with the inclusion. LV (MS drafting suggestions and comments): We support.
2. If agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may	2. ~~If~~ As 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, in	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, in	PT (MS drafting suggestions and comments): **Comments:** As this Article was discussed in the 19th of March CWP, PT will consider sending subsequent written comments on the newly proposed draft put forward by the PRES PL, which differs from the one presented here. NL (MS drafting suggestions and comments): The last sentence should be included to prevent unnecessary derisking.

be unable to fulfil its liability to pay.	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.	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. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	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, 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		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	IT (MS drafting suggestions and comments): **IT.** We suggest to align the wording in art 51, par 3 to recital 69e by adding a clear reference to the prohibition of disclosure laid down in art. 73 AMLR, instead of making a general reference to prohibitions by other relevant Union or national law. The wording should be the one that follows: "3. In such cases the payment service provider shall inform the payer of the blocking

prohibited by other relevant Union or national law.		information ~~would compromise objectively justified security reasons or~~ is prohibited by other relevant Union or national law. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	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 is prohibited by **Article 73 AMLR or by** other relevant Union or national law."
4. The payment service provider shall unblock the payment instrument or replace it with a new payment instrument once the reasons for blocking no longer exist.	4. The payment service provider shall not execute ~~unblock~~ the refused 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.	4. The payment service provider shall ~~not execute~~ unblock the ~~refused~~ 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~~. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
	~~5. By way of derogation from Article 65(2), the~~		ES (MS drafting suggestions and comments):

	~~payment service provider may refuse to execute the payment transaction for objectively justified reasons relating to the suspicion of unauthorised or fraudulent payment transactions, including where based on transaction monitoring mechanisms.~~ ~~In such cases the payment service provider shall inform the payment service user in accordance with Article 65(1).~~		We do not agree with the removal of this paragraph, since it is key to prevent fraud that the PSPs have clear means to refuse the transactions where there are objective reasons to suspect.
Article 52			
Obligations of the payment service user in relation to payment instruments and personalised security credentials			

PUBLIC

The payment service user entitled to use a payment instrument shall:	1. The payment service user entitled to use a payment instrument shall:		DE (MS drafting suggestions and comments): **Remark** The paragraphs shall not be numbered, since paragraphs 2 and 3 are deleted.
(a) use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which shall be objective, non-discriminatory and proportionate;			
(b) notify the payment service provider, or the entity specified by the payment service provider, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.			
For the purposes of point (a) the payment service user shall, as soon as in receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe.			

PUBLIC

	2. The payment service user may request information and help from the payment service provider in order to avoid fraudulent transactions and to apply properly the available preventive and safeguard processes and elements.	~~2. The payment service user may request information and help from the payment service provider in order to avoid fraudulent transactions and to apply properly the available preventive and safeguard processes and elements.~~ *[**PRES comment:** The provision has been deleted based on the Member States' comments to the questionnaire circulated within the November CWP. Member States deem this paragraph redundant and unecessasry as:* *i) it relates rather to the obligation of the PSP,* *ii) it may be found in other provisions of this Regulation,*	ES (MS drafting suggestions and comments): We agree with the deletion. SK (MS drafting suggestions and comments): We do not oppose deletion. LV (MS drafting suggestions and comments): We support. IT (MS drafting suggestions and comments): **IT:** we agree with the deletion. HR (MS drafting suggestions and comments): We agree with the deletion of this provision. AT (MS drafting suggestions and comments): We support the deletion of this paragraph.

PUBLIC

		iii) this Article relates to the obligations of the PSP, which seems not to be the case of this proposal.]	
	3. In case of suspicous fraudulent transaction the payment service user shall take all reasonable steps to report the incident to the police and fully inform the payment service provider.	~~3. In case of suspicous fraudulent transaction the payment service user shall take all reasonable steps to report the incident to the police and fully inform the payment service provider.~~ *[**PRES comment:** The provision has been deleted based on the Member States' comments to the questionnaire circulated within the November CWP. Member States deem this paragraph redundant and unecessasry as:* *i) this obligation imposed on the PSU is too strict,*	ES (MS drafting suggestions and comments): We do not agree with the deletion. The requirement to the PSU to report the incident to the police seems a proportionate exigence to reduce fraud. If this requirement is not included here, we would suggest to add a reference to the need to report the incident to the police in the definition of gross negligence. SK (MS drafting suggestions and comments): We support the deletion. SE (MS drafting suggestions and comments): We support the deletion of article 52.3. We find a general obligation for the PSU to file a police report excessive. LV

		ii) Article 52(b) already covers the scope of this proposal.]	(MS drafting suggestions and comments): We support. IT (MS drafting suggestions and comments): **IT:**We agree with the deletion. HR (MS drafting suggestions and comments): We propose to keep this provision that obliges PSU to report the incident to the police, as such a requirement gives additional weight to the case and we believe that it can reduce the number of frauds committed by PSUs themselves.
Article 53			
Obligations of the payment service provider in relation to payment instruments			
1. The payment service provider issuing a payment instrument shall:			IE (MS drafting suggestions and comments): We can support the intention around obligations for PSPs proposed in Article 53 but we are of the view that such obligations need to

PUBLIC

			be balanced to stop non-execution of transactions by PSPs being the default position. There is generally an asymmetrical power relationship between PSP and PSU – so non-execution should also come with actions for the PSP toward the PSU, e.g. speedy execution of 'false positives' without significant PSU input or similar. With regard to the PSU, due consideration needs to be given in the drafting to avoid placing any specific burdens on the PSU and allowing inaction on the part of the PSU to be classified as 'gross negligence'
(a) make sure that the personalised security credentials are not accessible to parties other than the payment service user that is entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in Article 52;	(a) make sure that the personalised security credentials are not accessible to parties other than the payment service user that is entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in Article 52(1);	(a) make sure that the personalised security credentials are not accessible to parties other than the payment service user that is entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in Article 52~~(1)~~; ***[PRES comment:*** *The amendment resulting*	LV (MS drafting suggestions and comments): We support.

PUBLIC

		from the changes to Article 52.]	
(b) refrain from sending an unsolicited payment instrument, except where a payment instrument already given to the payment service user is to be replaced;			
(c) ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to Article 52 point (b), or to request unblocking of the payment instrument pursuant to Article 51(4);	(c) ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to Article 52(1) point (b), or to request unblocking of the payment instrument pursuant to Article 51(4);	(c) ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to Article 52~~(1)~~ point (b), or to request unblocking of the payment instrument pursuant to Article 51(4); *[**PRES comment:** The amendment resulting from the changes to Article 52.]*	LV (MS drafting suggestions and comments): We support.
(d) provide the payment service user with the possibility to make a notification pursuant to Article 52 point (b) free of charge	(d) provide the payment service user with the possibility to make a notification pursuant to	(d) provide the payment service user with the possibility to make a notification pursuant to	LV (MS drafting suggestions and comments): We support.

PUBLIC

and only charge any possible replacement costs directly attributed to the payment instrument;	Article 52(1) point (b) free of charge and only charge any possible replacement costs directly attributed to the payment instrument;	Article 52~~(1)~~ point (b) free of charge and only charge any possible replacement costs directly attributed to the payment instrument; ***[PRES comment:*** *The amendment resulting from the changes to Article 52.]*	
(e) prevent all use of the payment instrument once a notification pursuant to Article 52 point (b) has been made.	(e) prevent all use of the payment instrument once a notification pursuant to Article 52(1) point (b) has been made;	(e) prevent all use of the payment instrument once a notification pursuant to Article 52~~(1)~~ point (b) has been made; ***[PRES comment:*** *The amendment resulting from the changes to Article 52.]*	LV (MS drafting suggestions and comments): We support.
(f) For the purposes of point (c), the payment service provider shall provide the payment service user upon its request with the means to prove, for 18 months after notification, that the payment			

PUBLIC

service user made such a notification.			
2. The payment service provider shall bear the risk of sending a payment instrument or any personalised security credentials relating to it to the payment service user.			
	3. The payment service provider shall seek to:	~~3. The payment service provider shall seek to:~~	ES (MS drafting suggestions and comments): We agree with the changes proposed.
	(a) provide the payment service user using mobile application with a	~~(a) provide the payment service user using mobile application with a~~	
	i. push notification to the payment service user's mobile device when his/her payment instrument is being used,	~~i. push notification to the payment service user's mobile device when his/her payment instrument is being used,~~	
	ii. push a controll notification regarding any changes to the balance of the payment service user's payment accounts;	~~ii. push a controll notification regarding any changes to the balance of the payment service user's payment accounts;~~	
	(b) alert customers via at least one mean or media	~~(b) alert customers via at least one mean or media~~	

	as to the new payment fraud methods occurring, no later than every 6 months in accordance with Article 84(1),	~~as to the new payment fraud methods occurring, no later than every 6 months in accordance with Article 84(1).~~ ~~Do spr. Jak się ma z art. 84(1)~~	
	(c) educate the payment service user and help him/her to use the payment instrument safely.	~~(c) educate provide the payment service user with clear instructions on how and help him/her to use the payment instrument safely.~~ *[**PRES comment**: Based on Member States comments to the CWP November questionnaire and expressed therein doubts, the PRES suggests to delete the whole paragraph as it raises interpretative doubts and is to some extent duplication of provisions in Article 84.]*	

		3. The payer's payment service provider shall ensure that appropriate means are available at all times to enable the payer to contact the payment service provider where additional information is requested by the payment service provider pursuant to [Article 65(1a)] to assess whether there are reasonable grounds to suspect fraud. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	ES (MS drafting suggestions and comments): We agree with the changes proposed. PT (MS drafting suggestions and comments): PT would favour a minor adjustment in this regard, to enhance clarity and precision. **<u>Drafting suggestion</u>:** 3. The payer's payment service provider shall ensure that**, at least, one of the specified means foreseen in framework contract**~~**appropriate means**~~ are available at all times to enable the payer to contact the payment service provider where additional information is requested by the payment service provider pursuant to [Article 65(1a)] to assess whether there are reasonable grounds to suspect fraud. EL (MS drafting suggestions and comments): **EL:** this can be combined with point 2 c above.
			NL (MS drafting suggestions and comments):

PUBLIC

			The formulation "appropriate means" is rather vague. Is it necessary to specify this further?
Article 54			
Notification and rectification of unauthorised, authorised or incorrectly executed payment transactions			
1. The payment service provider shall only rectify any unauthorised, incorrectly executed payment transaction or authorised payment transaction where the payment service user notifies the payment service provider in accordance with Articles 57 and 59 without undue delay after becoming aware of any such transaction giving rise to a claim, including a claim under Article 75, and no later than 13 months after the debit date.			
The time limits for notification laid down in the first subparagraph shall not apply where the payment service provider has failed to			

PUBLIC

provide or make available the information on the payment transaction in accordance with Title II.			
2. Where a payment initiation service provider is involved, the payment service user shall obtain rectification from the account servicing payment service provider pursuant to paragraph 1 of this Article, without prejudice to Article 56(4) and Article 75(1).			
Article 55			
Evidence on authorisation and execution of payment transactions			
1. Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, the burden shall be on the payment service provider to prove that the payment transaction			

PUBLIC

was authorised, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.			
If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authorised, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.			
2. Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as	2. Where a payment service user denies having authorised an executed payment transaction, ~~the use of a payment instrument recorded by the payment~~		ES (MS drafting suggestions and comments): We agree with the changes proposed. BE (MS drafting suggestions and comments):

appropriate, shall in itself not be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52. The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user.	~~service provider, including the payment initiation service provider as appropriate,~~ the fact that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided shall in itself not be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52. […].		BE: we would like to reiterate our strong support to the wording of the legacy text of previous presidencies. The authentication *is in itself not sufficient* to prove that the payment transaction was authorised by the payer or that the payer acted fraudulently or with gross negligence.
	3. For the purpose referred to in paragraph 1, the payment service user		ES (MS drafting suggestions and comments): We agree with the changes proposed.

PUBLIC

	shall provide the payment service provider with all the relevant information available to him regarding the events leading to the disputed payment transaction.		
	~~Article 55a~~		
	~~Payment service provider's liability for impersonation fraud~~		
	~~In the case of an unauthorised payment transaction where the payer was manipulated through social engineering into initiating the payment transaction in favour of a third party which was not the intended payee referred to in Article 49(2), the payment service provider shall bear the losses of up to a cap of [EUR XXX].~~		SE (MS drafting suggestions and comments): We support the deletion of article 55a.

PUBLIC

Article 56			
Payment service provider's liability for unauthorised payment transactions			
1. Without prejudice to Article 54, in the case of an unauthorised payment transaction, the payer's payment service provider shall refund the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the unauthorised transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud committed by the payer and communicates those grounds to the relevant national authority in writing.			PT (MS drafting suggestions and comments): X Please clarify if the PSP should still (temporarly) refund the PSU if it concludes that the latter comitted fraud.

PUBLIC

2. Where the payer's payment service provider had reasonable grounds for suspecting fraud committed by the payer, the payer's payment service provider shall, within 10 business days after noting or being notified of the transaction, do either of the following:	2. Where the payer's payment service provider had reasonable grounds for suspecting fraud committed by the payer, the payer's payment service provider shall, within ~~10~~ 15 business days after noting or being notified of the transaction, do either of the following:		
(a) refund the payer the amount of the unauthorised payment transaction if the payer's payment service provider has concluded, after further investigation, that no fraud has been committed by the payer;			
(b) provide a justification for refusing the refund and indicate the bodies to which the payer may refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the payer does not accept the reasons provided.			

PUBLIC

3. Where applicable, the payer's payment service provider shall restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. The payer's payment service provider shall also ensure that the credit value date for the payer's payment account shall be no later than the date the amount had been debited.			
4. Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund immediately, and in any event no later than by the end of the following business day, the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the			

PUBLIC

unauthorised payment transaction not taken place.			
5. If the payment initiation service provider is liable for the unauthorised payment transaction, the payment initiation service provider shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer, including the amount of the unauthorised payment transaction. In accordance with Article 55(1), the burden shall be on the payment initiation service provider to prove that, within its sphere of competence, the payment transaction was authorised, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.			
6. The payer may be entitled to further financial compensation			

PUBLIC

from the payment service provider in accordance with the law applicable to the contract concluded between the payer and the payment service provider or the contract concluded between the payer and the payment initiation service provider, where applicable.			
Article 57			
Payment service provider's liability for incorrect application of the matching verification service			
1. The payer shall not bear any financial losses for any authorised credit transfer where the payment service provider of the payer failed, in breach of Article 50(1), to notify the payer of a detected discrepancy between the unique identifier and the name of the payee provided by the payer.			

PUBLIC

2. Within 10 business days after noting or being notified of a credit transfer transaction executed in the circumstances referred to in paragraph 1, the payment service provider shall do either of the following:	2. Within ~~10~~ 15 business days after noting or being notified of a credit transfer transaction executed in the circumstances referred to in paragraph 1, the payment service provider shall do either of the following:		
(a) refund the payer the full amount of the authorised credit transfer;			
(b) provide a justification for refusing the refund and indicate the bodies to which the payer may refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the payer does not accept the reasons provided.			
3. Where the payment service provider of the payee is responsible for the breach of Article 50(1) committed by the payment service provider of the payer, the payment service			

PUBLIC

provider of the payee shall refund the financial damage incurred by the payment service provider of the payer.			
4. The burden shall be on the payment service provider of the payer or, in the case referred to in paragraph 3, of the payee to prove that there was no breach of Article 50(1).			
5. Paragraphs 1 to 4 shall not apply if the payer has acted fraudulently or if the payer opted out from receiving the verification service in accordance with Article 50(4).			
6. This Article shall not apply to instant credit transfers denominated in euro falling within the scope of by Regulation XXX (IPR).			
Article 58			
Liability of technical service providers and of operators of payment schemes for failure to			

PUBLIC

support the application of strong customer authentication			
Technical service providers and operators of payment schemes that either provide services to the payee, or to the payment service provider of the payee or of the payer, shall be liable for any financial damage caused to the payee, to the payment service provider of the payee or of the payer for their failure, within the remit of their contractual relationship, to provide the services that are necessary to enable the application of strong customer authentication.			
Article 59			
Payment service provider's liability for impersonation fraud			
			DK (MS drafting suggestions and comments):

			We see this as an important article for the finalisation of the fraud discussion now that the discussion on article 49 has been concluded. We would support a further expansion of PSPs liability than bank employee impersonation fraud.
1. Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer's payment service provider using the name or e-mail address or telephone number of that payment service provider unlawfully and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without any delay, reported the fraud to the police and notified its payment service provider.			PT (MS drafting suggestions and comments): X We believe that what is considered *impersonation fraud*" under PSR should include websites and apps (not limited to just phone and email contacts). In our view, this approach would be more appropriate and future-proof. "*Mirror pages*" should also be adressed particularly because (i) from the perspective of the abusive use of the PSP's name and image, these pages do not appear to differ from using the name and contact details, and also because (ii) mirror pages are the usual method for carrying out impersonation frauds. Therefore, we suggest the following: **Drafting suggestion**:

			«1. Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer's payment service provider using the name and or e-mail address or name and telephone number or website or mobile application, including mirror website or mobile application , of that payment service provider unlawfully and that manipulation gave rise to subsequent fraudulent authorised payment transactions (…)» MT (MS drafting suggestions and comments): Malta highlights a concern regarding the treatment of payer fraud manipulation, specifically in cases where the fraudster impersonates a third-party entity that is not a Payment Service Provider (PSP) [for instance: courier services, postal services, and the Police Force]. Malta believes it is essential for the Payment Services Regulation (PSR) to clarify that such cases should be considered as authorised fraud, provided the PSP can demonstrate that the payment was authorised by the payer. In such instances, the PSP should not bear any liability. EL

			(MS drafting suggestions and comments): **EL:** It is necessary to include reference to "website or mobile application" as suggested by the Presidency note wk2161 of Feb meeting in order to make clear that this type of fraud is related to PSP impersonation when the user is scammed ny means of spoofing.
2. Within 10 business days after noting or being notified of the fraudulent authorised payment transaction, the payment service provider shall do either of the following:			EL (MS drafting suggestions and comments): **EL:** We propose to align with the 15 days introduced above in 57.2
(a) refund the consumer the amount of the fraudulent authorised payment transaction;			
(b) where the payment service provider has reasonable grounds to suspect a fraud or a gross negligence by the consumer, provide a justification for refusing the refund and indicate to the consumer the bodies to which the consumer may refer the matter in accordance with Articles 90, 91,			

PUBLIC

93, 94 and 95 if the consumer does not accept the reasons provided.			
3. Paragraph 1 shall not apply if the consumer has acted fraudulently or with gross negligence.			
4. The burden shall be on the payment service provider of the consumer to prove that the consumer acted fraudulently or with gross negligence.			
5. Where informed by a payment service provider of the occurrence of the type of fraud as referred to in paragraph 1, electronic communications services providers shall cooperate closely with payment service providers and act swiftly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC, including with regard			EL (MS drafting suggestions and comments): **EL:** We believe that the role of Electronic Communication Service Providers (ECSPs) is crucial in the fight against fraud. Fraud types such as spoofing, SIM-swapping, or phishing sites - especially those presented as sponsored results in search engines - highlight the need for targeted preventive measures also from the part of ECSPs. We remain on the viea that issue should be addressed in the PSR now and not rely only in a future review.

PUBLIC

to calling line identification and electronic mail address.			
Article 60			
Payer's liability for unauthorised payment transactions			
1. By way of derogation from Article 56, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.			EL (MS drafting suggestions and comments): EL: We would like to indicate again that in the proposed Art. 60 (1) PSR the wording regarding possible reduction of liability in case the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations should be in line with the existing wording in Art. 74 (1) PSD2. It is the MS that should have the discretion to reduce liability, not competent authorities or PSPs.
The first subparagraph shall not apply where any of the following occurred:			
(a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment,			

PUBLIC

except where the payer has acted fraudulently; or			
(b) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.			
The payer shall bear all of the losses relating to any unauthorised payment transactions if those losses were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 52 with intent or gross negligence. In such cases, the maximum amount referred to in the first subparagraph shall not apply.			DE (MS drafting suggestions and comments): **Remark:** We would like to draw attention to the pending ECJ C- 665/23 Veracash SAS request for preliminatry ruling on the question whether Art. 74 (1) 3 PSD2 (identical with Art. 60 (1) b 2 PSR) should be interpreted as meaning that, in the event of losses relating to unauthorised transactions which the payer notified late with intent or gross negligence, the payer is deprived of the right to reimbursement in relation to all unauthorised transactions, as opposed to only those transactions which could have been prevented if the notification had not been late.
Where the payer has neither acted fraudulently nor intentionally		Where the payer has neither acted fraudulently	ES

failed to fulfil its obligations under Article 52, national competent authorities or payment service providers may reduce the liability referred to in this paragraph, taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated.		nor intentionally failed to fulfil its obligations under Article 52, national competent authorities, dispute resolution bodies or payment service providers may reduce the liability referred to in this paragraph, taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated. ***[PRES comment**: The proposal presented at the February CWP meeting.]*	(MS drafting suggestions and comments): We agree with the changes proposed. LV (MS drafting suggestions and comments): We support. FI (MS drafting suggestions and comments): FI: We support this addition. DE (MS drafting suggestions and comments): **Remark** Regarding Art. 60 (1): In our view, it is systematically wrong to designate ADR entities in Article 60(1) of the PSR. ADR entities are required to reach decisions that are based on the prevailing legal framework. ADR solutions are based on the factual situation as it has arisen in the procedure, should be aligned with the applicable law and in particular respect mandatory consumer protection laws. It is therefore misleading if, in the context of liability rules, as it is now expressly provided that ADR entities may accept a limitation of liability under

PUBLIC

			certain conditions. If the applicable substantive law provides for such a possibility of limitation, the ADR entity should base its solution on it anyway. The same applies for national competent authorities. It is suggested that the MS be granted the authority to establish exceptions in such circumstances, with the matter to be subject to general regulation.
2. Where the payer's payment service provider fails to fulfil the obligation to require strong customer authentication set out in Article 85, the payer shall not bear any financial losses unless the payer has acted fraudulently. The same shall apply where either the payment service provider of the payer or of the payee applies an exemption from the application of strong customer authentication. Where the payee or the payment service provider of the payee fails to develop or amend the systems, hardware and software that are necessary to apply strong customer			

PUBLIC

authentication, the payee or the payment service provider of the payee shall refund the financial damage caused to the payer's payment service provider.			
3. Where the payee's payment services provider applies an exemption from the application of strong customer authentication, the payee's payment services provider shall be liable towards the payer's payment services provider for any financial loss incurred by the latter.			
4. The payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with of Article 52, point (b), except where the payer has acted fraudulently.			
If the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or			

PUBLIC

misappropriated payment instrument, as required under of Article 53(1), point (c), the payer shall not be liable for the financial consequences resulting from use of that payment instrument, except where the payer has acted fraudulently.			
Article 61			
Payment transactions where the transaction amount is not known in advance			
1. Where a payment transaction is initiated by or through the payee in the context of a card-based payment transaction and the exact future amount is not known at the moment when the payer authorizes the execution of the payment transaction, the payer's payment service provider may only block funds on the payer's payment account if the payer has given his or her			ES (MS drafting suggestions and comments): We suggest replacing "card-based payment transaction" with payments initiated through a payment instrument".

PUBLIC

permission to that precise amount of funds to be blocked.			
2. The amount of the funds blocked by the payer's payment service provider shall be in proportion with the amount of the payment transaction which can reasonably be expected by the payer.			
3. The payee shall inform its payment service provider of the exact amount of the payment transaction immediately after delivery of the service or goods to the payer.			
4. The payer's payment service provider shall release the funds blocked on the payer's payment account immediately after receipt of the information about the exact amount of the payment transaction.			
Article 62			

PUBLIC

Refunds for payment transactions initiated by or through a payee			
1. A payer shall be entitled to a refund from the payment service provider of an authorised payment transaction which was initiated by the payer through a payee and which has already been executed, where both of the following conditions are met:		1. A payer shall be entitled to a refund from the payment service provider of an authorised payment transaction which was initiated by or ~~the payer~~ through a payee and which has already been executed, where both of the following conditions are met: *[**PRES comment**: The wording aligned to the wording of Article 76 PSD2, based on the comment of one of the Member States. Such deviation from the PSD2 has not been justified nor explained, thus creating an impression that this*	ES (MS drafting suggestions and comments): We propose to include an exemption to the unconditional refund right for direct debits in the case of tax authorities. The justification lies with the fact that tax law already includes a refund regime. However, the process would only include the tax authority and the tax payer, without obligations for the PSP. Particularly, we suggest including an additional paragraph 2a: *Direct debits where the tax authority is the payee are excluded from paragraph 1.* LV (MS drafting suggestions and comments): We support. IT (MS drafting suggestions and comments):

		deviation was not intentional.]	**IT:** We agree. CZ (MS drafting suggestions and comments): We agree with the change only to "throug a payee".
(a) the authorisation did not specify the exact amount of the payment transaction when the authorisation was made;			
(b) the amount of the payment transaction exceeded the amount the payer could reasonably have expected taking into account the previous spending pattern, the conditions in the framework contract and relevant circumstances of the case.			
At the payment service provider's request, the payer shall bear the burden of proving such conditions are met.			
The refund shall consist of the full amount of the executed payment transaction. The credit value date for the payer's payment account			

PUBLIC

PUBLIC

shall be no later than the date the amount was debited.			
Without prejudice to paragraph 3 of this Article, in addition to the right referred to in the first subparagraph of this paragraph, for authorised payment transactions which were initiated by a payee, including direct debits as referred to in Article 1 of Regulation (EU) No 260/2012, the payer shall have an unconditional right to a refund within the time limits laid down in Article 63 of this Regulation.			DE (MS drafting suggestions and comments): **Request for Change** We are sceptical to the extention of Art. 61(1) to all forms of Merchant Initiated Transactions. In fact, for other forms of Merchant Initiated Transactions besides direct debits there exist elaborate charge-back provisions already today determining the refund rights for PSUs. Overriding those provisions would generate uncertainties and potential forms of desrisking to the detriment of PSUs. Hence, we propose to keep the wording of Art. 76(1) subparagraph 4 PSD 2. CZ (MS drafting suggestions and comments): We suggest the following change in Article 62 (1) *Without prejudice to paragraph 3 of this Article, in addition to the right referred to in the first subparagraph of this paragraph, for ~~authorised payment transactions which were initiated by a payee, including~~ direct debits as*

PUBLIC

			referred to in Article 1 of Regulation (EU) No 260/2012, the payer shall have an unconditional right to a refund within the time limits laid down in Article 63 of this Regulation. The change fully corresponds with Article 76 (1) last subpara PSD2 and it allows national none-EUR debtor driven direct debits to be operated. As a consequence first subpara applies.
2. For the purposes of paragraph 1, first subparagraph, point (b), the payer shall not invoke reasons related to possible currency exchange costs if the reference exchange rate agreed with its payment service provider in accordance with Article 13(1), point (e), and Article 20, point (c)(iii), was applied.			
3. The payer and the payment service provider may agree in a framework contract that the payer has no right to a refund where:			
(a) the payer has authorised the execution of the payment transaction directly with the payment service provider;			

PUBLIC

(b) where applicable, information on the future payment transaction was provided or made available in an agreed manner to the payer for at least 4 weeks before the due date by the payment service provider or by the payee.			
4. For direct debits in currencies other than euro, payment service providers may offer more favourable refund rights in accordance with their direct debit schemes provided that they are more advantageous to the payer.			
Article 63			
Requests for refunds for payment transactions initiated by or through a payee			
1. The payer may request the refund referred to in Article 62 of an authorised payment transaction initiated by or through a payee for			

PUBLIC

a period of 8 weeks from the date on which the funds were debited.			
2. Within 10 business days of receiving a request for a refund, the payment service provider shall do either of the following:	2. Within ~~10~~ 15 business days of receiving a request for a refund, the payment service provider shall do either of the following:		ES (MS drafting suggestions and comments): We agree with the changes proposed. DE (MS drafting suggestions and comments): **Remark** In Art. 97 (1) e PSR a sanction for the failure of the PSP to respect the period mentioned in Art. 63 (2) PSR appears to be missing.
(a) refund the full amount of the payment transaction;			
(b) provide a justification for refusing the refund and indicate the bodies to which the payer may refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the payer does not accept the reasons provided.			
The payment service provider's right under the first subparagraph of this paragraph to refuse the refund shall not apply in the case			

PUBLIC

set out in of Article 62(1), fourth subparagraph.			
CHAPTER 5			
Execution of payment transactions			
Section 1			
Payment orders and amounts transferred			
Article 64			
Receipt of payment orders			
1. The time of receipt of a payment order shall be when the payment order is received by the payer's payment service provider.			
The payer's account shall not be debited before receipt of the payment order. If the time of receipt is not on a business day for the payer's payment service provider, the payment order shall be deemed to have been received on the following business day. The payment service provider may establish a cut-off time near the			

PUBLIC

end of a business day beyond which any payment order received shall be deemed to have been received on the following business day.			
2. If the payment service user placing a payment order and the payment service provider agree that the execution of the payment order shall start on a specific day or at the end of a certain period or on the day on which the payer has put the funds at the payment service provider's disposal, the time of receipt for the purposes of Article 69 shall be deemed to be the agreed day. If the agreed day is not a business day for the payment service provider, the payment order received shall be deemed to have been received on the following business day.			
3. This Article shall not apply to instant credit transfers denominated in Euro as covered by Regulation XXX (IPR).			

PUBLIC

Article 65			
Refusal of payment orders	**Refusal ~~of payment orders~~ <u>to execute a payment order</u>**		
			IT (MS drafting suggestions and comments): **IT. Italy would suggest to redraft Art. 65, par. 1 and 1.a in order to provide that both provisions - i.e. the obligation to execute authorized payment transactions under para 1 and the possibility for the PSP to refuse a payment under para 1a - are without prejudice to the obligation to refrain from executing transactions under art. 71 AMLR or other relevant Union or national LAW. This would also ensure**

PUBLIC

			consistency with recital 69c.
		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. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	ES (MS drafting suggestions and comments): We do not fully agree with the changes proposed, since it could hinder the possiblities of the PSP to refuse to execute a payment order in case of fraud suspicion. We suggest to delete " if agreed in the framework contract" in the next paragraph to mitigate the risk. LV (MS drafting suggestions and comments): We support. IT (MS drafting suggestions and comments): IT. "1. Where all of the conditions set out in the payer's framework contract are met **and without prejudice to 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

PUBLIC

			through a payee, unless the execution of the payment transaction would be prohibited by other relevant Union or national law." BE (MS drafting suggestions and comments): BE: we support in general the Presidency's suggestion regarding Article 65. However, we are still analysing the latest drafting suggestions made by the Presidency during the meeting of 19th March. Therefore we do not have yet a strong position regarding the precies wording of this provision and we will provide more comments in our written answers to the questions asked by the Presidency following the meeting of 19th March.
		1a. By way of exception from the above, if agreed in the framework contract, the payer's payment service provider may refuse to execute an authorised payment transaction where, based on the transaction monitoring referred to in Article 83 and on any	ES (MS drafting suggestions and comments): We suggest to remove " if agreed in the framework contract" from this paragraph. For completeness, we would suggest to include that the **PSP of the payee should also be able to refuse the payment transaction if there is suspicion of fraud.** NL

		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. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	(MS drafting suggestions and comments): We suggest changing the word ‘’and’’ to ‘’or’’ ….’’based on the transaction monitoring referred to in Article 83 ~~and~~ or 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. LV (MS drafting suggestions and comments): We support. IT (MS drafting suggestions and comments): IT. in line with the previous comment, we suggest the following amendment: “1a. By way of exception from the above ***and without prejudice to article 71 AMLR,*** if agreed in the framework contract, the payer’s payment service provider may refuse to execute an 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." EL (MS drafting suggestions and comments): **EL:** We are concerned about derisking by PSPs and the potential incentives to reject large volumes of transactions out of fear of repercussions.
		For the purpose of this Regulation, the fact that a payment order is unusual shall not by itself constitute reasonable grounds to suspect fraud. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	ES (MS drafting suggestions and comments): We do not fully agree with the changes proposed, since it could hinder the possiblities of the PSP to refuse to execute a payment order in case of fraud suspicion. LV (MS drafting suggestions and comments): We support. LU (MS drafting suggestions and comments): LU: this provision is rather confusing as fraud detection mechanisms are largely based on

			transaction monitoring and profiling of the PSUs usual behavior.
		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	ES (MS drafting suggestions and comments): We agree with the changes proposed. PT (MS drafting suggestions and comments): This paragraph shall clarify what is meant by "*sufficient information*", namely, the elements that must necessarily be communicated (e.g. the identification of the payee, the payment instrument, the transaction's value, the channel used, the risks identified or any possible disclaimers to the PSU). LV (MS drafting suggestions and comments): We support. EL (MS drafting suggestions and comments): **EL:** We propose to ammend the last sentence as follows (in orange):

		suspect fraud. The notification shall give the payer sufficient information to enable the payer to understand the risks that the payment service provider has identified. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	"The notification by the payer PSP shall ~~give the payer~~ contain sufficient information to enable the payer to understand the risks that the payment service provider has identified.
		Where it is not possible for the payer's payment service provider to contact the payer within the timelines specified in Article 69(1), 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	ES (MS drafting suggestions and comments): The current drafting seems opposite to Article 71 of the AMLR, which prohibits executing any suspicious transaction until it has been reported to the Financial Intelligence Unit and complied with the instructions it has given. In other words, the PSP cannot decide by itself whether to execute a suspicious transaction or not. LV (MS drafting suggestions and comments): We support.

PUBLIC

		to execute the payment order. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
		The obligation in the third subparagraph shall not apply in the case of instant credit transfers. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	LV (MS drafting suggestions and comments): We support. BG (MS drafting suggestions and comments): The obligation in the third subparagraph shall not apply in the case of instant credit transfers or card-based payment transactions. *[We agree with the Presidency's drafting proposals however, we believe that the requirements should also not apply to card-based payment transactions, which, despite their deferred settlement, generate similar transaction monitoring problems as those faced during the monitoring of instant payments.]*
1. Where the payment service provider refuses to execute a payment order or to initiate a payment transaction, the payment service provider shall notify the		~~2~~1. Where the payment service provider refuses to execute a payment order or to initiate a payment	ES (MS drafting suggestions and comments): We agree with the changes proposed. IT

refusal and, if possible, the reasons for that refusal and the procedure for correcting any factual mistakes that led to the refusal to the payment service user, unless prohibited by other relevant Union or national law.		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 any factual mistakes that led to the refusal ~~to the payment service user~~, unless prohibited by other relevant Union or national law. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	(MS drafting suggestions and comments): **IT.** In line with the previous comment we suggest the following amendment: "2. 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 any factual mistakes that led to the refusal to the payment service user, unless prohibited **by Article 73 AMLR or 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 in any case within the periods specified in Article 69.		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	ES (MS drafting suggestions and comments): We agree with the changes proposed. LV (MS drafting suggestions and comments): We support.

PUBLIC

		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 within 10 seconds of the time of receipt of the payment order by the payer's payment service provider. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
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.		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.	ES (MS drafting suggestions and comments): We agree with the changes proposed. PT (MS drafting suggestions and comments): We support the proposed wording, namely the segment: "*but not in the case of a refusal due to a suspected fraudulent transaction*", suggested by the PL Presidency. LV

		*[**PRES comment**: The proposal presented at the January CWP meeting.]*	(MS drafting suggestions and comments): We support.
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 or through a payee, unless prohibited by other relevant Union or national law.		~~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 or through a payee, unless prohibited by other relevant Union or national law.~~ *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
	3. Where the conditions laid down in Article 71(1) of Regulation (EU)	~~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.	~~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.~~ *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
	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	~~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~~	

PUBLIC

	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 reasons or is prohibited by other relevant Union law. Where the refusal of a payment order is due to factual mistakes, the notification shall also include the procedure for correcting any factual	~~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 reasons or is prohibited by other relevant Union law. Where the refusal of a payment order is due to factual mistakes, the notification shall also include the procedure for correcting any factual~~	

	mistakes that led to the refusal the payment order.	~~mistakes that led to the refusal the payment order.~~ *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
3. For the purposes of Articles 69 and 75 a payment order whose execution has been refused shall be deemed not to have been received.			
Article 66			
Irrevocability of a payment order			
1. The payment service user shall not revoke a payment order once it has been received by the payer's payment service provider, unless otherwise specified in this Article.			
2. Where the payment transaction is initiated by a payment initiation service provider or by or through the payee, the payer shall not revoke the payment			

PUBLIC

order after giving permission to the payment initiation service provider to initiate the payment transaction or after giving permission to execute the payment transaction to the payee.			
3. In the case of a direct debit, and without prejudice to refund rights, the payer may revoke the payment order at the latest by the end of the business day preceding the day agreed for debiting the funds.			
4. In the case referred to in Article 64(2), the payment service user may revoke a payment order at the latest by the end of the business day preceding the agreed day.			
5. After the time limits laid down in paragraphs 1 to 4, the payment order may be revoked only if agreed between the payment service user and the relevant payment service providers. In the case referred to in			IT (MS drafting suggestions and comments): **IT**: The paragraph should clarify the conditions that must be met to revoke a payment order when a PISP is involved, so as to ensure legal clarity. In particular:

PUBLIC

paragraphs 2 and 3, the payee's agreement shall also be required. If agreed in the framework contract, the relevant payment service provider may charge for revocation.			1) which are the relevant PSPs (e.g.: only the ASPSP or also the PISP) whose agreement is required to revoke the payment order? Is a joint-agreement required (e.g.: ASPSP and PISP at the same time) or is the agreement between the PSU and the ASPSP sufficient (which appears preferable; see EBA Q&A 4496)? 2) in case of PISP transactions initiated by the payee, is the consent of the PISP, in addition to those of the payee, also required to revoke the payment order?
Article 67			
Amounts transferred and amounts received			
1. The payment service provider of the payer, the payment service provider(s) of the payee and any intermediaries of the payment service providers shall			

PUBLIC

transfer the full amount of the payment transaction and shall refrain from deducting charges from the amount transferred.			
2. The payee and the payment service provider may agree that the relevant payment service provider deduct its charges from the amount transferred before crediting it to the payee. In such a case, the full amount of the payment transaction and charges shall be separated in the information given to the payee.			
3. If any charges other than those referred to in paragraph 2 are deducted from the amount transferred, the payment service provider of the payer shall ensure that the payee receives the full amount of the payment transaction initiated by the payer. Where the payment transaction is initiated by or through the payee, the payment service provider of the payee shall ensure that the full amount of the			

PUBLIC

payment transaction is received by the payee.			
Section 2			
Execution time and value date			
Article 68			
Scope			
1. This Section applies to:			
(a) payment transactions in euro;			
(b) national payment transactions in the currency of the Member State outside the euro area;			
(c) payment transactions involving only one currency conversion between the euro and the currency of a Member State outside the euro area, provided that the required currency conversion is carried out in the Member State outside the euro area concerned and, in the case of cross-border payment transactions, the cross-border transfer takes place in euro.			

PUBLIC

2. This Section applies to payment transactions not referred to in paragraph 1, unless otherwise agreed between the payment service user and the payment service provider, with the exception of Article 73, which is not at the disposal of the parties. However, if the payment service user and the payment service provider agree on a longer period than that set in Article 69, for intra-Union payment transactions, that longer period shall not exceed 4 business days following the time of receipt as referred to in Article 64.			
Article 69			
Payment transactions to a payment account			
1. Without prejudice to Article 2(1), point (c) of Regulation (EU) No 260/2012, the payer's payment service provider			

PUBLIC

shall ensure that after the time of receipt as referred to in Article 64, the amount of the payment transaction will be credited to the payee's payment service provider's account by the end of the following business day. That time limit may be extended by a further business day for paper-initiated payment transactions.			
	The first subparagraph is without prejudice of the obligations of payment service providers pursuant to Article 71 of Regulation (EU) 2024/1624.	The first subparagraph is without prejudice of the obligations of payment service providers pursuant to ~~Article 71 of Regulation (EU) 2024/1624~~ other relevant Union or national legislation in the field of anti-money laundering and anti-terrorism financing. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	ES (MS drafting suggestions and comments): We agree with the changes proposed. LV (MS drafting suggestions and comments): We support.

2. The payment service provider of the payee shall value date and make available the amount of the payment transaction to the payee's payment account after the payment service provider has received the funds in accordance with Article 73.			DK (MS drafting suggestions and comments): We have earlier suggested the possibility to postpone making funds available in a new article 69(2a). It is our understanding from the last WPs that the drafting is being worked on but is expected to be included in the text, which we support.
		The first subparagraph is without prejudice to the obligations of payment service providers under other relevant Union or national legislation in the field of anti-money laundering and anti-terrorism financing. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	ES (MS drafting suggestions and comments): We agree with the changes proposed. LV (MS drafting suggestions and comments): We support.
3. The payee's payment service provider shall transmit a payment order placed by or through the payee to the payer's payment service provider within the time limits agreed between the			

PUBLIC

payee and the payment service provider, enabling settlement, as far as direct debit is concerned, on the agreed due date.			
Article 70			
Absence of payee's payment account with the payment service provider			
Where the payee does not have a payment account with the payment service provider, the payment service provider who receives the funds for the payee shall make the funds available to the payee within the time limit laid down in Article 69(1).		Where the payee does not have a payment account with the payment service provider, the payment service provider who receives the funds for the payee shall make the funds available to the payee within the time limit laid down in Article 69(1). For payment transactions with electronic money tokens from a custodial wallet to a self-hosted	ES (MS drafting suggestions and comments): We have no objections to the presidency´s proposal LV (MS drafting suggestions and comments): We support.

PUBLIC

		address, the payment service provider of the payer shall transfer the funds to the self-hosted address of the payee within the time limit laid down in Article 69(1). *[**PRES comment**: The proposal presented at the February CWP meeting.]*	
Article 71			
Cash placed on a payment account			
Where a consumer places cash on a payment account with that payment service provider in the currency of that payment account, the payment service provider shall ensure that the amount is made available and value dated immediately after receipt of the funds. Where the payment service user is not a consumer, the amount shall be made available and value			

PUBLIC

dated at the latest on the following business day after receipt of the funds.			
Article 72			
National payment transactions			
For national payment transactions, Member States may provide for shorter maximum execution times than those provided for in this Section.			
Article 73			
Value date and availability of funds			
1. The credit value date for the payee's payment account shall be no later than the business day on which the amount of the payment transaction is credited to the payee's payment service provider's account.			
2. The payment service provider of the payee shall ensure			

PUBLIC

that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account where, on the part of the payee's payment service provider, there is either of the following:			
(a) no currency conversion;			
(b) a currency conversion between the euro and a Member State currency or between two Member State currencies.			
The obligation laid down in this paragraph shall also apply to payments within one payment service provider.			
3. The debit value date for the payer's payment account shall be no earlier than the time at which the amount of the payment transaction is debited to that payment account.			
Article 74			
Incorrect unique identifiers			

PUBLIC

1. If a payment transaction is executed in accordance with the unique identifier, the payment transaction shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier.			
2. If the unique identifier provided by the payment service user is incorrect, the payment service provider shall not be liable under Article 75 for non-execution or defective execution of the payment transaction.			
3. The payer's payment service provider shall make reasonable efforts to recover the funds involved in the payment transaction. The payee's payment service provider shall cooperate in those efforts also by communicating to the payer's payment service provider all relevant information for the collection of funds.			

PUBLIC

Where the collection of funds under the first subparagraph is not possible, the payer's payment service provider shall provide to the payer, upon written request, all information available to the payer's payment service provider and relevant to the payer in order for the payer to file a legal claim to recover the funds.			
4. Where agreed in the framework contract, the payment service provider may charge the payment service user for recovery.			
5. If the payment service user provides information in addition to the information referred to in Article 13(1), point (a), or Article 20 point (b) (ii), the payment service provider shall be liable only for the execution of payment transactions in accordance with the unique identifier provided by the payment service user.			
6. Where the unique identifier provided by the payment initiation			

PUBLIC

service provider is incorrect, payment service providers shall be liable in accordance with Article 76.			
Article 75			
Payment service providers' liability for non-execution, defective or late execution of payment transactions			
1. Where a payment order is placed directly by the payer, the payer's payment service provider shall, without prejudice to Article 54, Article 74(2) and (3), and Article 79, be liable to the payer for correct execution of the payment transaction, unless it can prove to the payer and, where relevant, to the payee's payment service provider that the payee's payment service provider received the amount of the payment transaction in accordance with Article 69(1). In that case, the			

PUBLIC

payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction.			
Where the payer's payment service provider is liable under the first subparagraph, it shall immediately refund to the payer the amount of the non-executed or defective payment transaction, and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.			
The credit value date for the payer's payment account shall be no later than the date on which the amount was debited.			
Where the payee's payment service provider is liable under the first subparagraph, it shall immediately place the amount of the payment transaction at the payee's disposal and, where applicable, credit the			

PUBLIC

corresponding amount to the payee's payment account.			
The credit value date for the payee's payment account shall be no later than the date on which the amount would have been value dated, had the transaction been correctly executed in accordance with Article 73.			
Where a payment transaction is executed late, the payee's payment service provider shall ensure, upon the request of the payer's payment service provider acting on behalf of the payer, that the credit value date for the payee's payment account is no later than the date the amount would have been value dated had the transaction been correctly executed.			
In the case of a non-executed or defectively executed payment transaction where the payment order is placed by the payer, the payer's payment service provider shall, regardless of liability under			

PUBLIC

this paragraph, on request and without charging the payer, make immediate efforts to trace the payment transaction and notify the payer of the outcome.			
2. Where a payment order is placed by or through the payee, the payee's payment service provider shall, without prejudice to Article 54, Article 74(2) and (3), and Article 79, be liable to the payee for correct transmission of the payment order to the payment service provider of the payer in accordance with Article 69(3). Where the payee's payment service provider is liable under this subparagraph, it shall immediately re-transmit the payment order in question to the payment service provider of the payer.			
In the case of a late transmission of the payment order, the amount shall be value dated on the payee's payment account no later than the date the amount would have been			

PUBLIC

value dated had the transaction been correctly executed.			
Without prejudice to Article 54, Article 74(2) and (3), and Article 79, the payment service provider of the payee shall be liable to the payee for handling the payment transaction in accordance with its obligations under Article 73. Where the payee's payment service provider is liable under this subparagraph, it shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account. The amount shall be value dated on the payee's payment account no later than the date the amount would have been value dated had the transaction been correctly executed.			
In the case of a non-executed or defectively executed payment transaction for which the payee's			

PUBLIC

payment service provider is not liable under the first and third subparagraphs, the payer's payment service provider shall be liable to the payer. Where the payer's payment service provider is so liable it shall, as appropriate and without undue delay, refund to the payer the amount of the non-executed or defective payment transaction and restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place. The credit value date for the payer's payment account shall be no later than the date the amount was debited.			
The obligation under the fourth subparagraph shall not apply to the payer's payment service provider where the payer's payment service provider proves that the payee's payment service provider has received the amount of the payment transaction, even if			

PUBLIC

execution of payment transaction is merely delayed. If so, the payee's payment service provider shall value date the amount on the payee's payment account no later than the date the amount would have been value dated had it been executed correctly.			
In the case of a non-executed or defectively executed payment transaction where the payment order is placed by or through the payee, the payee's payment service provider shall, regardless of liability under this paragraph, on request and without charging the payer, make immediate efforts to trace the payment transaction and notify the payee of the outcome.			
3. Payment service providers shall be liable to their respective payment service users for any charges for which they are responsible, and for any interest to which the payment service user is			

PUBLIC

subject as a consequence of non-execution or defective, including late, execution of the payment transaction.			
Article 76			
Liability in the case of payment initiation services for non-execution, defective or late execution of payment transactions			
1. Where a payment order is placed by the payer or by the payee through a payment initiation service provider, the account servicing payment service provider shall, without prejudice to Article 54 and Article 74(2) and (3), refund to the payer the amount of the non-executed or defective payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the			

PUBLIC

defective payment transaction not taken place.			
The burden shall be on the payment initiation service provider to prove that the payment order was received by the payer's account servicing payment service provider in accordance with Article 64 and that within its sphere of competence the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the non-execution, defective or late execution of the transaction.			
2. If the payment initiation service provider is liable for the non-execution, defective or late execution of the payment transaction, it shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer.			

PUBLIC

Article 77			
Additional financial compensation			
Any financial compensation additional to that provided for under this Section may be determined in accordance with the law applicable to the contract concluded between the payment service user and the payment service provider.			
Article 78			
Right of recourse			
1. Where the liability of a payment service provider under Articles 56, 57, 59, 75 and 76 is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary shall compensate the first payment service provider for any losses			

PUBLIC

incurred or sums paid under Articles 56, 57, 59, 75 and 76. That shall include compensation where any of the payment service providers fail to apply strong customer authentication.			
2. Further financial compensation may be determined in accordance with agreements between payment service providers or intermediaries and the law applicable to the agreement concluded between them.			
Article 79			
Abnormal and unforeseeable circumstances			
No liability shall arise under Chapter 4 or 5 in cases of abnormal and unforeseeable circumstances beyond the control of the party pleading for the application of those circumstances, the consequences of which would have been unavoidable despite all			

PUBLIC

efforts to the contrary, or where a payment service provider is bound by other legal obligations covered by Union or national law.			
CHAPTER 6			
Data protection			
Article 80			
Data protection			
Payment systems and payment service providers shall be allowed to process special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 to the extent necessary for the provision of payment services and for compliance with obligations under this Regulation, in the public interest of the well-functioning of the internal market for payment services, subject to appropriate safeguards for the fundamental			LT (MS drafting suggestions and comments): In the processing of payment transactions, other parties, such as technical services providers, are also involved. They also transmit data, which contain personal data, including special categories of personal data. Therefore, they should be also included into the scope of this article. DE (MS drafting suggestions and comments): **Important Remark** We see a considerable need for discussion regarding this provison. In order to further

PUBLIC

rights and freedoms of natural persons, including the following:			assess GDPR-conformity, we ask for further clarification with regard to the following questions: - Is this provision intended to provide an exception within the meaning of Article 9 (2) g GDPR – and if so, which of the exceptions in Article 9 (2) GDPR shall apply? - Is this provision (also) intended to provide a legal basis within the meaning of Article 6 (1) GDPR? - Which categories of special categories of personal data need to be processed for which specific purposes (under this regulation) and by whom? Are "payment systems" a suitable subject of this provision, as its definition (Art. 3 (9)) describes a system, but not an entity that could be bearer of rights and duties? Which entity shall be adressed by this provision? As Art. 80 (1) adresses payment service providers (and "payment systems"): why is Regulation (EU) 2018/1725, which applies only to the procession of personal data by Union institutions and bodies, mentioned in this context?

PUBLIC

(a) technical measures to ensure compliance with the principles of purpose limitation, data minimisation and storage limitation, as laid down in Regulation (EU) 2016/679, including technical limitations on the re-use of data and use of state-of-the-art security and privacy-preserving measures, including pseudonymisation, or encryption;			DE (MS drafting suggestions and comments): **Important Remark** Insofar as this regulation (points a and b) is intended to provide for 'appropriate safeguards for the rights and freedoms of data subjects' within the meaning of Article 9(2) g GDPR, we have doubts that it fulfils the requirements of the aforementioned articles. In particular, it does not provide for any specific safeguards, but merely refers to or repeats the requirements already applicable under the GDPR.
(b) organizational measures, including training on processing special categories of data, limiting access to special categories of data and recording such access.			DE (MS drafting suggestions and comments): See above
CHAPTER 7			
Operational and security risks and authentication			
Article 81			
Management of operational and security risks			

PUBLIC

1. Payment service providers shall establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide. As part of that framework, payment service providers shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.			EL (MS drafting suggestions and comments): **EL:** All these provisions under article 81 prexisted in PSD2 and are now covered under DORA. We prospose a simple reference to DORA.
The first subparagraph shall be without prejudice to the application of Chapter II of Regulation (EU) 2022/2554 of the European Parliament and of the Council[1] to:			
(a) payment service providers referred to in Article 2(1), points (a), (b) and (d) of this Regulation;			

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

PUBLIC

(b) account information service providers referred to in Article 36(1) of Directive (EU) (PSD3); and			
(c) payment institutions exempted pursuant to Article 34(1) of Directive (EU) (PSD3).			
Payment service providers shall provide to the competent authority designated under Directive (EU) XXX (PSD3) on an annual basis, or at shorter intervals as determined by the competent authority, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.			IT (MS drafting suggestions and comments): **IT:** Regarding subparagraph 3 of the article 81(1), we confirm that we agree on the proposal to remove the obligation of the annual reporting related to the comprehensive assessment of the operational and security risks relating to the payment services. Reducing the quantity of assessment reporting about risks required to all PSPs is also in line with the objective to contain the burden of additional reporting requirements also pursued in the SSM. We reiterate our preference to delete this subparagraph. DE (MS drafting suggestions and comments): **Request for change** **(important point)**

PUBLIC

			We have motivated our proposal to delete the reporting obligations of Art. 81(1) subpara. 3 PSR in our Non Paper "Proposals for Simplification in PSR / PSD 3 regarding reporting and notifications" (WK 2068/2025 INIT) as well as in our written comments to the working party on the 21st of February. In the written comments to our Non Paper a vast majority of MS supports the deletion of Art. 81(1) subpara. 3 PSR from the text. In fact, from those 22 MS responding in the written comments, only 1 MS explicitly opposes the deletion of this subparagraph, while 16 MS support the deletion and 2 MS do not object the deletion. Hence, we propose to delete Art. 81(1) subpara. 3 PSR from the compromise text. CZ (MS drafting suggestions and comments): We would propose deleting this subparagraph.
2. The EBA shall promote cooperation, including the sharing of information, in the area of			

PUBLIC

operational and security risks associated with payment services among the competent authorities, between the competent authorities and the ECB and, where relevant, the European Union Agency for Network and Information Security.			
Article 82			
Fraud reporting			
1. Payment service providers shall provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities shall provide the EBA and the ECB with such data in an aggregated form.	1. Payment service providers shall provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities shall provide the EBA and the ECB with such data in an aggregated form. The EBA and the ECB shall publish an annual report	1. Payment service providers shall provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities shall provide the EBA and the ECB with such data in an aggregated form. The EBA and the ECB shall publish an annual joint	ES (MS drafting suggestions and comments): We agree with the changes proposed. LV (MS drafting suggestions and comments): We support. LT (MS drafting suggestions and comments): Currently all the data is reported to the ECB according to its regulation. The methodology was prepared having also in mind EBAs guidelines available at that time. Data is reported to the ECB, an the ECB shares it with the EBA.

	analysing the trends observed on the basis of these data.	report analysing the trends observed on the basis of these data. ***[PRES comment:*** *The amdendment follows the Member State's doubts as to wheteher each of these institutions would be obliged to publish a separate report. In the view of the PRES these doubts could be solved by the above amendment.]*	Current wording sounds as requiring double reporting by NCAs to both ECB and EBA. It should be updated to match the current situation.
	1a. Competent authorities may allow payment service providers to fulfill the obligation in paragraph 1 by reporting fraud data to their competent authority under another data reporting requirement, if that requirement is not less extensive than the reporting requirement under this Article and if	1a. Competent authorities may allow payment service providers to fulfill the obligation in paragraph 1 by reporting fraud data ~~to their competent authority~~ under another data reporting requirement, if that requirement is not less extensive than the reporting requirement under this Article and if	ES (MS drafting suggestions and comments): We agree with the changes proposed. LV (MS drafting suggestions and comments): We support the deletion.

PUBLIC

	arrangements have been made under which the EBA will receive the data that is due under this Article.	arrangements have been made under which the EBA will receive the data that is due under this Article. ***[PRES comment**: Fragment seems to be redundant.]*	
2. The EBA shall, in close cooperation with the ECB, develop draft regulatory technical standards on statistical data to be provided in accordance with paragraph 1 on the fraud reporting requirements referred to in paragraph 1.			
The EBA shall submit the regulatory technical standards referred to in first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated on the Commission to adopt the regulatory technical standards referred to in the first			

PUBLIC

subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.			
3. The EBA shall develop draft implementing technical standards establishing the standard forms and templates for the submission of the payment fraud data by competent authorities to the EBA, as referred to in paragraph 1.	3. The EBA shall develop draft implementing technical standards establishing the standard forms and templates for the submission of the payment fraud data by competent authorities to the EBA, as referred to in paragraph 1. <u>These implementing technical standards shall not be applicable if the competent authority makes use of the option referred to in paragraph 1a.</u>		ES (MS drafting suggestions and comments): We agree with the changes proposed.
The EBA shall submit the implementing technical standards referred to in first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this	The EBA shall submit the implementing technical standards referred to in first subparagraph to the Commission by [OP please insert the date=		ES (MS drafting suggestions and comments): We agree with the changes proposed.

PUBLIC

Regulation]. Power is delegated on the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Article 15 of Regulation (EU) No 1093/2010.	one year after the date of entry into force of this Regulation]. Power is delegated on the Commission to adopt the implementing ~~regulatory~~ technical standards referred to in the first subparagraph in accordance with Article 15 of Regulation (EU) No 1093/2010.		
Article 83			
Transaction monitoring mechanisms and fraud data sharing	**Transaction monitoring mechanisms ~~and fraud data sharing~~**		
			DK (MS drafting suggestions and comments): Generally, we would support a non-exhaustive list for the transaction monitoring. We have taken note of the CLS comment on the last WP, and if it is assessed that a non-exhaustive list is not possible to have, then we believe the list should be placed in level 2 to allow for more flexibility.

Public

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.			
	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		PT (MS drafting suggestions and comments): As this Article was discussed in the 19th of March CWP, PT will consider sending subsequent written comments on the newly

	transaction. Without prejudice to Article 69(2), the payment service provider of the payee shall also carry out transaction monitoring of received payment transactions.		proposed draft put forward by the PRES PL, which differs from the one presented here. EL (MS drafting suggestions and comments): **EL:** We welcome the clarifications made on whether the payee's PSPs shall also carry out transaction monitoring. However we would like to raise our concerns on potential challenges that the payee's PSPs will have to perform transaction monitoring on received transactions and at the same time meet the requirement of the Instant Payment Regulation (IPR), which mandates that the payee's PSP make funds available within 10 seconds of receipt (Article 5a(4)c).
	1b. 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	~~1b. 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~~	PT (MS drafting suggestions and comments): As this Article was discussed in the 19th of March CWP, PT will consider sending subsequent written comments on the newly proposed draft put forward by the PRES PL, which differs from the one presented here. LV (MS drafting suggestions and comments): We support.

PUBLIC

	consolidate the following data with a view to identifying the payment service user's usual transactions in order to prevent and detect potentionally fraudulent transaction, support the application of strong customer authenthication:	~~consolidate the following data with a view to identifying the payment service user's usual transactions in order to prevent and detect potentionally fraudulent transaction, support the application of strong customer authenthication:~~ *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
	a) the amount of the payment transactions,	~~a) the amount of the payment transactions,~~	LV (MS drafting suggestions and comments): We support.
	b) the payment instruments used by the payment service user,	~~b) the payment instruments used by the payment service user,~~	LV (MS drafting suggestions and comments): We support.
	c) the types of transactions carried out by the payment service user,	~~c) the types of transactions carried out by the payment service user,~~	LV (MS drafting suggestions and comments): We support.
	d) the dates of the transactions executed,	~~d) the dates of the transactions executed,~~	LV (MS drafting suggestions and comments):

			We support.
	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.	~~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.~~ *[**PRES comment**: The proposal presented at the January CWP meeting.]*	LV (MS drafting suggestions and comments): We support.
	The data referred to in points a) to e) shall be aggregated in order to identify the usual	~~The data referred to in points a) to e) shall be aggregated in order to identify the usual~~	LV (MS drafting suggestions and comments): We support.

PUBLIC

	behaviour of the payment service user.	~~behaviour of the payment service user.~~ *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
2. Transaction monitoring mechanisms shall be based on the analysis of previous payment transactions and access to payment accounts online. Processing shall be limited to the following data required for the purposes referred to in paragraph 1:		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: *[**PRES comment**: The proposal presented at the January CWP meeting.]*	LV (MS drafting suggestions and comments): We support.
(a) information on the payment service user, including the environmental and behavioural characteristics which are typical of the payment service user in the	(a) information on the payment service user, including the environmental and behavioural	(a) information on the ~~payment service user~~ payer, including the environmental and behavioural	NL (MS drafting suggestions and comments): We find the specification of information in point (a) here rather vague. Which "environmental

circumstances of a normal use of the personalised security credentials;	characteristics which are ~~typical~~ usual of the payment service user in the circumstances of a normal use of the personalised security credentials;	characteristics which are typical of the ~~payment service user~~ payer in the circumstances of a normal use of the personalised security credentials; *[**PRES comment**: The proposal presented at the January CWP meeting.]*	and behavioural characteristics" are referred to here? What is "a normal use"? We would be in favor of making the provisions here, and possibly also provisions for other elements of the transaction monitoring mechanism, as specific as possible.
(b) information on the payment account, including the payment transaction history;			
(c) transaction information, including the transaction amount and unique identifier of the payee;			
(d) session data, including the device internet protocol address-range from which the payment account has been accessed.			
	(e) device data, including device identifiers.		
		Processing by the payment service provider of the payee shall be limited to the following	NL (MS drafting suggestions and comments): We strongly support an exhausitve list of data LV

PUBLIC

		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, the name of the payer and of the beneficiary. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	(MS drafting suggestions and comments): We support.
Payment service providers shall not store data referred to in this paragraph longer than necessary for the purposes set out in paragraph 1, and not after the termination of the customer relationship. Payment service			

PUBLIC

providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:			
(a) lists of compromised or stolen authentication elements;			
(b) the amount of each payment transaction;			
(c) known fraud scenarios in the provision of payment services;			
(d) signs of malware infection in any sessions of the authentication procedure;			
(e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.			
	3. Without prejudice to Article 69 and 71 of the Regulation (EU) 2024/1624 of the	~~3. Without prejudice to Article 69 and 71 of the Regulation (EU) 2024/1624 of the~~	LV (MS drafting suggestions and comments): We support.

	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.	~~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.~~ *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
3. To the extent necessary to comply with paragraph 1, point (c), payment service providers may exchange the unique identifier of a payee with other payment service providers who are subject to information sharing arrangements as referred to in paragraph 5, when the payment service provider has sufficient evidence to assume that there was a fraudulent payment transaction. Sufficient evidence for sharing	~~3. To the extent necessary to comply with paragraph 1, point (c), payment service providers may exchange the unique identifier of a payee with other payment service providers who are subject to information sharing arrangements as referred to in paragraph 5, when the payment service provider has sufficient~~		

PUBLIC

unique identifiers shall be assumed when at least two different payment services users who are customers of the same payment service provider have informed that a unique identifier of a payee was used to make a fraudulent credit transfer. Payment service providers shall not keep unique identifiers obtained following the information exchange referred to in this paragraph and paragraph 5 for longer than it is necessary for the purposes laid down in paragraph 1, point (c).	~~evidence to assume that there was a fraudulent payment transaction. Sufficient evidence for sharing unique identifiers shall be assumed when at least two different payment services users who are customers of the same payment service provider have informed that a unique identifier of a payee was used to make a fraudulent credit transfer. Payment service providers shall not keep unique identifiers obtained following the information exchange referred to in this paragraph and paragraph 5 for longer than it is necessary for the purposes laid down in paragraph 1, point (c).~~		

PUBLIC

4. The information sharing arrangements shall define details for participation and shall set out the details on operational elements, including the use of dedicated IT platforms. Before concluding such arrangements, payment service providers shall conduct jointly a data protection impact assessment as referred to in Article 35 of the Regulation (EU) 2016/679 and, where applicable, carry out prior consultation of the supervisory authority as referred to in Article 36 of that Regulation.	~~4. The information sharing arrangements shall define details for participation and shall set out the details on operational elements, including the use of dedicated IT platforms. Before concluding such arrangements, payment service providers shall conduct jointly a data protection impact assessment as referred to in Article 35 of the Regulation (EU) 2016/679 and, where applicable, carry out prior consultation of the supervisory authority as referred to in Article 36 of that Regulation.~~		
5. Payment service providers shall notify competent authorities of their participation in the information sharing arrangements	~~5. Payment service providers shall notify competent authorities of their participation in the~~		

PUBLIC

referred to in paragraph 5, upon validation of their membership by participants of the information sharing arrangement or, as applicable, of the cessation of their membership, once that cessation takes effect.	~~information sharing arrangements referred to in paragraph 5, upon validation of their membership by participants of the information sharing arrangement or, as applicable, of the cessation of their membership, once that cessation takes effect.~~		
6. The processing of personal data in accordance with paragraph 4 shall not lead to termination of the contractual relationship with the customer by the payment service provider or affect their future on-boarding by another payment service provider.	~~6. The processing of personal data in accordance with paragraph 4 shall not lead to termination of the contractual relationship with the customer by the payment service provider or affect their future on-boarding by another payment service provider.~~		
	Article 83a		
	Fraud data sharing		

	1. Payment service providers 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):	1. Payment service providers 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: *[**PRES comment**: The proposal presented at the January CWP meeting.]*	NL (MS drafting suggestions and comments): 1. Payment service providers ~~may~~ shall 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: Furthermore, data sharing should not only be possible to comply with Article 83(1)(c), but also to exchange data with national authorities and with supervisory authorities. We proposed the following subparagraphs for Article 83(1): • enable payment service providers to inform competent national authorities for the purpose of a possible criminal investigation. • enabling payment service providers to establish accountability towards supervisory authorities LV (MS drafting suggestions and comments):

			We support. DK (MS drafting suggestions and comments): We support that the catalogue of data that may be shared should be a non-exhaustive list. It should probably be checked when the lists are finalised that the list for transaction monitoring also includes all of the datapoint which can also be shared.
	(a) the unique identifier of a payee;		
	(b) the name of the payee;		
	(c) the personal identification number or organisation number of the 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,		

PUBLIC

	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. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	ES (MS drafting suggestions and comments): We agree with the changes proposed. LV (MS drafting suggestions and comments): We support.
	1a. A payment service provider may exchange such data with other payment service providers who are subject to an information sharing		DE (MS drafting suggestions and comments): **Remark** We still see the need for further clarification as to what constitutes "reasonable and objective

	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.		grounds to suspect a fraudulent behaviour" – if not here at least in the recitals. In addition, in order to ensure data accuracy (incl. with regards to Article 5 (1) point d GDPR) we suggest the following addition to this paragraph: 'If a suspicion later proves to be unfounded, the payment service provider shall inform the other payment service providers who are subject to the information sharing arrangement of this fact.'
	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. Payment service providers shall implement appropriate technical and organisational measures, including measures to		

PUBLIC

	allow pseudonymisation, to ensure a level of security and confidentiality proportionate to the nature and extent of the information exchanged.		
	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 3 years after the suspected fraudulent transaction has taken place].		
	3. The information sharing arrangements shall specify the details of participation and the details of operational		DE (MS drafting suggestions and comments): **Remark**

	elements, including the use of dedicated IT platforms. Before concluding such arrangements, payment service providers shall jointly carry out a data protection impact assessment in accordance with Article 35 of Regulation (EU) 2016/679 and, where applicable, prior consultation of the supervisory authority in accordance with Article 36 of that Regulation.		It seems likely that different payment service providers participating in an information sharing arrangement would be considered joint controllers when processing shared data. Has this assessment already been considered? Which supervisory authority would consequently be considered lead supervisory authority in the case of transnational information sharing arrangements?
	4. Payment service providers shall notify the competent authorities of their participation in the information sharing arrangements referred to in paragraph 3 as soon as their membership is confirmed by the		DE (MS drafting suggestions and comments): **Request for change** **(important point)** We have motivated our proposal to delete the notification obligation of Art. 83a(4) PSR in our Non Paper "Proposals for Simplification in PSR / PSD 3 regarding reporting and notifications"

	participants in the information sharing arrangement or, where applicable, as soon as their membership ceases.		(WK 2068/2025 INIT) as well as in our written comments to the working party on the 21st of February. In the written comments to our Non Paper a vast majority of MS supports the deletion of Art. 83a(4) from the text. In fact, from those 22 MS responding in the written comments, only 2 MS explicitly oppose the deletion of this subparagraph, while 14 MS support the deletion and 2 MS do not object the deletion. Hence, we propose to delete Art. 83a(4) from the compromise text. CZ (MS drafting suggestions and comments): We ask if this provision is really needed. We would not oppose to delete this para.
	5. Payment service providers shall not rely solely on the information received in the context of the data sharing referred to in para. 1 to comply with the requirements of this Regulation and shall		ES (MS drafting suggestions and comments): It could be clarified in the last sentence that there needs to be an assessment of the information by the institution.

PUBLIC

	not draw conclusions or take decisions that have an impact on the business relationship with the payment service user or on the execution of a payment transaction on the basis of information received from other payment service providers who are subject to an information sharing arrangement without having assessed that information.		"without having assessed that information by their own means or procedures".
		6. For the purposes of this Article, Member States shall ensure that appropriate measures are in place so that the payment service providers are also able to share the data referred to in paragraph 1 with the relevant national authorities.	ES (MS drafting suggestions and comments): We agree with the changes proposed. NL (MS drafting suggestions and comments): We cannot agree to paragraph 6. It is very important for us that the PSR provides a legal basis for PSPs to share data with national authorities. While the newly proposed paragraph 6 is a step in the right direction, it is

		*[**PRES comment**: The proposal presented at the January CWP meeting.]*	not sufficiently prescriptive, which means that it could not serve as a legal basis. For this reason, we propose the following wording: 6. Payment service providers shall share the data as referred to in paragraph 1 with the relevant competent national authorities to the extent strictly necessary to comply with their obligations in Article 83(1), point (d). LV (MS drafting suggestions and comments): We support.
Article 84			
Payment fraud risks and trends			
1. Payment service providers shall alert their customers via all appropriate means and media when new forms of payment fraud emerge, taking into account the needs of their most vulnerable groups of customers. Payment service providers shall give their customers clear indications on how to identify fraudulent			

PUBLIC

attempts and warn them as to the necessary actions and precautions to be taken to avoid falling victim of fraudulent actions targeting them. Payment service providers shall inform their customers of where they can report fraudulent actions and rapidly obtain fraud-related information.			
2. Payment service providers shall organize at least annually training programmes on payment fraud risks and trends for their employees and shall ensure that their employees are adequately trained to carry out their tasks and responsibilities in accordance with the relevant security policies and procedures to mitigate and manage payment fraud risks.			
3. By [OP please insert the date= 18 months after the date of entry into force of this Regulation], the EBA shall issue guidelines in accordance with Article 16 of Regulation (EU) No	3. By [OP please insert the date= 18 months after the date of entry into force of this Regulation], the EBA shall issue guidelines in accordance		

PUBLIC

1093/2010 with regard to the programmes on payment fraud risks referred to in paragraphs 1 and 2 of this Article.	with Article 16 of Regulation (EU) No 1093/2010 with regard to the customer alerts and the training programmes on payment fraud risks referred to in paragraphs 1 and 2 of this Article.		
	4. Member States shall have in place adequate measures to raise awareness among the public about the trends and new forms of payment fraud, the procedures to be followed in order to identify fraudulent attempts and the rights and obligations conferred by this Regulation in what regards fraud. Member States shall ensure that communication measures are sufficient and well-targeted, in particular	4. Member States shall have in place adequate measures to raise awareness among the public about the trends and new forms of payment fraud, the procedures to be followed in order to identify fraudulent attempts and the rights and obligations conferred by this Regulation in what regards fraud. Member States shall ensure that communication measures are sufficient and well-targeted, in particular	ES (MS drafting suggestions and comments): We agree with the changes proposed. LV (MS drafting suggestions and comments): We support. IT (MS drafting suggestions and comments): **IT:** We agree. CZ (MS drafting suggestions and comments): We think that this text should be deleted. It is not appropriate for a regulation.

PUBLIC

	reaching out to the most vulnerable consumer groups, including older persons or those with low digital skills.	reaching out to the most vulnerable consumer groups, including older persons ~~or~~ and those with low digital skills. ***[PRES comment**: In the view of PRES conjunction "and" would fit better here, since the formulation is not exhaustive ("including (...)")]*	