Council of the European Union
General Secretariat

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

Brussels, 20 June 2025

WK 8383/2025 INIT

LIMITE

EF
ECOFIN
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Financial Services and the Banking Union (Payment Services/ PSR/PSD) Financial Services Attachés
Subject:	Consolidation PSR Art. 49-84 of the Questionnaire Ddl 02/05/25 Replies from 20 MS

From: BG, BE, AT, SI, SE, PT, NL, LV, LU, IT, IE, HU, HR, FR, FI, ES, EL, EC, DE, CZ **Updated: 15/05/2025 11:39**

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 recent Council Working Party meetings. Written contributions from Member States following these meetings are still being analysed. The new amendments (compared to the previous version of the consolidated table) are highlighted in yellow.

Commission proposal	Legacy text of previous presidiencies	PL PRES drafting suggestions	MS drafting suggestions and comments
CHAPTER 4			
Authorisation of payment transactions			
Article 49			
Authorisation			
		*[**PRES comment:** The below proposal was presented at the 4 April CWP meeting.]*	BE (MS drafting suggestions and comments): **BE: as a general comment, please note that BE is not able at this stage to express its agreement or refusal on the proposals on fraud-related issues insofar as several provisions are still under discussion. Our competent ministers will be able to take a position once final texts are available. See our written comments on the Discussion notes**

			provided at the meeting on 29 April.
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.		1. A payment transaction or a series of payment transactions shall be authorised only if the payer has given its consent ~~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.	SI (MS drafting suggestions and comments): SI: We would prefer to keep the 1a paragraph in Article 49 of the PSR rather than move it to the Recitals, as also indicated in the Presidency note for the CWP on 29 April: 1a. A payment transaction shall not be deemed as authorised where the transaction was cariied out by a third party who is acting without the consent of the payment service user. PT (MS drafting suggestions and comments): PT strongly supports maintaining Article 49(2) as proposed by the PL Presidency in the February CWP, which clearly highlighted that a payment transaction shall not be deemed as authorised where the transaction was initiated by a 3rd party using the personal security

			credentials of the PSU fraudulently obtained. In our view, the currently contemplated text for Article 49(1a) appears to merely reiterate the content of Article 49(1), which tends to diminish the clear focus previously given to the specific case highlighted with the February drafting, that also mirrored the EBA's conclusions presented in its Opinion on new types of payment fraud. We believe there is merit in having the general conditions presented in point 1) being followed by the described explanatory example in 1a), enhancing legal clarity and enforceability. **Drafting suggestion:** [New point 1a.] 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.

			FI (MS drafting suggestions and comments): FI: As a general remark, we are not commenting on the blue parts as we are expecting the next compromise from the PCY. EL (MS drafting suggestions and comments): **EL:** As the described mentioned Option 1 of the February paper wk02161 which 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		2. Access to a payment account for the purpose of account information services or payment initiation services by payment service	

account information services provider or, respectively, to the payment initiation service provider, to access the payment account and the relevant data in that account.		providers shall be authorised only if the payment service user has given its consent ~~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 an account information service provider or a payment initiation service provider shall be considered to be unauthorised.		3. In the absence of consent ~~permission~~, a payment transaction or access to a payment account by an account information service provider or a payment initiation service provider shall be considered to be unauthorised.	
4. Account servicing payment service providers shall not verify the permission given by the payment service user to the account information service		4. Account servicing payment service providers shall not verify the consent ~~permission~~ given by the payment service	

provider or payment initiation service provider.		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.		5. The consent ~~permission~~ referred to in paragraphs 1 and 2 shall be expressed in the form agreed between the payer and the relevant payment service provider. 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.		6. The procedure for giving consent ~~permission~~ shall be agreed between the payer and the relevant payment service provider.	
7. The payment service user may withdraw permission to execute a payment transaction or to access a payment account for the purpose of payment initiation services or account information services may be withdrawn		7. The payment service user may withdraw consent ~~permission~~ to execute a payment transaction or to access a payment account for the	

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.		purpose of payment initiation services or account information services may be withdrawn by the payment service user at any time. The payment service user may also withdraw consent ~~permission~~ to execute a series of payment transactions, in which case any future payment transaction shall be considered to be unauthorised.	
Article 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,		~~1. In case of credit transfers, the payment service provider of the payee shall, free of charge,~~	

verify whether or not the unique identifier and the name of the payee as provided by the payer 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.		~~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 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		~~2. The payment service providers shall provide the service referred to in paragraph 1 immediately after the payer provided to its payment service provider~~	

possibility to authorise the credit transfer.		~~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 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.		~~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 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		~~4. Payment service providers shall ensure that payment service users~~	

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.		~~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 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		~~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 paragraph 1 may lead to transferring the funds to a payment account not held~~	

service user opts out from receiving the service referred to in paragraph 1.		~~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.		~~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		~~7. The matching service referred to in paragraph 1 shall not be~~	HU (MS drafting suggestions and comments):

unique identifier and the name of the payee.		~~required where the payer did not input himself the unique identifier and the name of the payee.~~	We would suggest to add this subparagraph 7, as in some business models, in case of credit transfers as well, the payer does not input himself the unique identifier and the name of the payee. In case of these business models the service would unnecessary and would hinder the operation.
8. This Article shall not apply to instant credit transfers denominated in euro falling within the scope of Regulation XXX (IPR).		~~8. This Article shall not apply to instant credit transfers denominated in euro falling within the scope of Regulation XXX (IPR).~~	
		In the case of credit transfers, PSPs shall comply with provisions of Article 5c(1)-(7) and Article 5b(2) of Regulation (EU) 260/2012, that shall apply to all credit transfers, including those that fall outside the scope of Regulation (EU) 260/2012.	LV (MS drafting suggestions and comments): We support the amendments. LU (MS drafting suggestions and comments): LU: we support the proposed amendments. IT

			(MS drafting suggestions and comments): IT. We agreee. However, in our view the previously proposed wording was clearer ("*Payment service providers when offering credit transfers denominated in the currency of a Member State whose currency is not the euro shall comply with provisions of Article 5c (1)-(7) and Article 5b(2) of Regulation (EU) 260/2012*"). IE (MS drafting suggestions and comments): This should be "payment service providers" and not "PSPs". "In the case of all credit transfers, payment service providers shall comply with provisions of Article 5c(1)-(7) and Article 5b(2) of Regulation (EU) 260/2012, ~~that shall apply to all credit transfers~~, including those that fall outside the scope of Regulation (EU) 260/2012."

			HR (MS drafting suggestions and comments): We agree with the proposed drafting. DE (MS drafting suggestions and comments): **Remark** We think the reference to Regulation (EU) 260/2012 is wrong here. Instead there should be a reference to Regulation (EU) 2024/886 amending Regulation (EU) 260/2012. Further, we remain cautious about extending the scope of payee verification beyond what is outlined in the instant payments regulation (Regulation (EU) 2024/886). In our view, the extension could also be moved to a future review of the

			PSR. Given that the implementation efforts are significant, this approach would provide time to 1) implement the service within the scope currently envisaged by the instant payments regulation, and 2) allow for more targeted adjustments based on the experience from the VoP in accordance with the SEPA regulation.
		For the purpose of the first subparagraph, where the payment account of the payee is not identified by the payment account identifier specified in point (1)(a) of the Annex of Regulation (EU) 260/2012, references in Article 5c of that Regulation to the payment account identifier shall be construed as referring to the unique identifier used to unambiguously identify	LV (MS drafting suggestions and comments): We support the amendments. HR (MS drafting suggestions and comments): We agree with the proposed drafting. DE (MS drafting suggestions and comments): **Remark**

		the payment account of the payee. ***[PRES comment:*** *The presented wording is built on the proposal presented by the PRES and comments of Member States in this regard.]*	As we understand it, this case could – if at all – only occur for non-euro credit transfers, as it is otherwise IBAN-only (as specified in the SEPA regulation). With regard to the extension of the scope, we refer to our remarks in the previous comment. This might also be an aspect better be addressed in a review.
Article 51			
Limits and blocking of the use of the payment instrument			
		[PRES comment: *The proposal for this Article will be part of the discussion at the CWP meeting on 29 April.]*	IE (MS drafting suggestions and comments): Care needs to be taken in the drafting here that any potential conflict between Article 51 and provisions introduced by the IPR in the SEPA Regulation is avoided in the interests of consistency and legal certainty.

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 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).	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 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	SI (MS drafting suggestions and comments): SI: We support the proposal prepared for the CWP meeting on 29 April. HU (MS drafting suggestions and comments): Some technical amendments: 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~~ ~~T~~the 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~~ set for each ~~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. It shall be possible for the payment service user to set

		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 require the application of strong customer authentication in accordance with Article 85 (1)(d). *[**PRES comment**: The proposal presented at the January CWP meeting.]*	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 require the application of strong customer authentication in accordance with Article 85 (1)(d). ES (MS drafting suggestions and comments): We agree with the changes proposed.
	1a. The payment service providers shall not unilaterally increase the spending limits agreed with their payment	1a. The payment service providers shall not unilaterally increase the	SI (MS drafting suggestions and comments):

	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, 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.	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 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.]*	SI: We support the proposal prepared for the CWP meeting on 29 April. 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. 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.*** 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.
		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.	HU (MS drafting suggestions and comments): It would be important to clarify the exact meaning of „leads to exceeding" as it may cause unclarity in practice, whether the non-execution provision is applicable and whether the exact amount qaulifies as „leads to exceed the maximum amount". ES (MS drafting suggestions and comments): We agree with the changes proposed
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	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	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	BG (MS drafting suggestions and comments): *We consider that in order to increase consumer protection PSPs should be obliged to block 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.	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.	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. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	*payment instrument for objectively justified reasons relating to the security by operation of the law and not **only** if it was agreed with the consumer. In practice payment service users are not in a position to negotiate the clauses of the framework contracts and it is up to the PSP to decide whether such blocking shall take place. In that regard, we suggest to delete any reference to the framework contract in that provision.* IE (MS drafting suggestions and comments): IE suggests that the blocking of the use of the payment instrument and refusal to execute a payment order should be mandatory in certain circumstances for example, objectively justified reasons relating to the security of the payment instrument, or the suspicion of unauthorised or fraudulent use of the payment instrument, and not only "if agreed in the framework contract".

			FR (MS drafting suggestions and comments): We are in favor of maintaining the possibility for the PI to refuse the execution (article 51 (2) PSR) in addition to the possibility of blocking the payment instrument. ES (MS drafting suggestions and comments): We agree with the changes proposed
3. In such cases the payment service provider shall inform the payer of the blocking of the payment instrument and the reasons for it in an agreed manner, where possible before the payment instrument is blocked and at the latest immediately thereafter, unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant Union or national law.		3. In such cases the payment service provider shall inform the payer of the blocking of the payment instrument and the reasons for it in an agreed manner, where possible before the payment instrument is blocked and at the latest immediately thereafter, unless providing such information ~~would compromise objectively justified security reasons~~	

		~~or~~ is prohibited by other relevant Union or national law. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
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.]*	IE (MS drafting suggestions and comments): IE is in favour of retaining the clause allowing the service user to confirm their consent. Confirmation of legitimacy should be adequate grounds for unblocking. ES (MS drafting suggestions and comments): We agree with the changes proposed
	~~5. By way of derogation from Article 65(2), the payment service provider may refuse to execute the payment transaction for objectively justified reasons relating to the suspicion of unauthorised or fraudulent payment~~		ES (MS drafting suggestions and comments): We oppose to the removal of this paragraph, since it is key to prevent fraud that the PSPs have clear

	~~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).~~		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			
The payment service user entitled to use a payment instrument shall:	1. The payment service user entitled to use a payment instrument shall:	~~1.~~ The payment service user entitled to use a payment instrument shall: *[**PRES comment**: The paragraphs 2 and 3 are deleted resulting in no need for numbering.]*	
(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.			
	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*	IT (MS drafting suggestions and comments): IT. We agree with the deletion. HU (MS drafting suggestions and comments): We do not agree with the deletion of paragraphs 2 and 3. Even if this provision may seem duplicative, it clarifies within the legal text, rather than in the Recital, that the PSU has the option to turn to the PSP for fraud and damage prevention and, as a victim of crime, msut report it to the police. These elements can

		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,* *iii) this Article relates to the obligations of the PSP, which seems not to be the case of this proposal.]*	potentially help recover funds (if the fraud has occurred) because the police can block entire accounts, not just specific transactions. Additionally, they can share information between PSPs without violating banking secrecy, thus preventing the occurrence of damage or further damages. Without this, all the burden remains on the PSPs, leaving out the police's tools or allowing their use only with significant delays. HR (MS drafting suggestions and comments): We agree with the deletion of this provision. ES (MS drafting suggestions and comments): We agree with the changes proposed.
	3. In case of suspicous fraudulent transaction the payment service user	~~3. In case of suspicous fraudulent transaction the~~	SE

	shall take all reasonable steps to report the incident to the police and fully inform the payment service provider.	~~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,* *ii) Article 52(b) already covers the scope of this proposal.]*	(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. 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. In our opinion, the provision in Article 52(1)(b) does not cover the scope of this proposal because the possibility of reporting the incident to the police depends on the decision of the individual PSP.

			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 is considered as 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 as a criteria for identifying of gross negligence.
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): With regard to the PSU, due consideration needs to be given in the drafting here 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 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	(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)	(c) ensure that appropriate means are available at all times to enable the payment service user to	

(b), or to request unblocking of the payment instrument pursuant to Article 51(4);	point (b), or to request unblocking of the payment instrument pursuant to Article 51(4);	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.]*	
(d) provide the payment service user with the possibility to make a notification pursuant to Article 52 point (b) free of charge and only charge any possible replacement costs directly attributed to the payment instrument;	(d) provide the payment service user with the possibility to make a notification pursuant to Article 52(1) point (b) free of charge and only charge any possible replacement costs directly attributed to the payment instrument;	(d) provide the payment service user with the possibility to make a notification pursuant to 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.]*	
(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 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:~~	IT (MS drafting suggestions and comments): IT. We agree with the deletion. HR (MS drafting suggestions and comments): We consider push notification a useful tool so we propose to keep it. Also, we would like to remind about BE non-paper containing useful proposals for improving the security

			of banking application that we support. 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 as to the new payment fraud methods occurring, no later than every 6 months in accordance with Article 84(1),	~~(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).~~	
	(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	PT (MS drafting suggestions and comments): PT would favour a minor adjustment in this regard, to enhance clarity and precision. **Drafting suggestion:**

		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.]*	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. HR (MS drafting suggestions and comments): We agree with the proposal. ES (MS drafting suggestions and comments): We agree with the changes proposed.
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 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 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 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.	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 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. […].	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 appropriate,~~ the fact that the payment transaction was authenticated, including where applicable, via strong customer authentication, 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	AT (MS drafting suggestions and comments): We strongly support the insertion of the term “necessarily”. In this regard, we also refer to our comments in the latest working group meeting. SI (MS drafting suggestions and comments): SI: In our view, the inclusion of the word “necessarily” softens the bank’s obligations. Nevertheless, we could accept it. LV (MS drafting suggestions and comments): We support the amendments. IT

		necessarily 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. *[**PRES comment:** The result of several discussions on fraud and fraud-relates issues.]*	(MS drafting suggestions and comments): IT. We agree. HU (MS drafting suggestions and comments): We do not support adding the word "necessarily". HR (MS drafting suggestions and comments): We support this drafting. ES (MS drafting suggestions and comments): We agree with the changes proposed. DE (MS drafting suggestions and comments): **Drafting Suggestion** Technical difference between "Authentication" vs. "Authorization" needs to be

			considered. Payment service users do authenticate themselves (if applicable via SCA). After being authenticated they can authorise a payment transaction, by using SCA processes. "…the fact that the payment transaction was ~~authenticated~~ **authorised**, including where applicable, ~~via~~ by means of strong customer authentication,…"
	3. For the purpose referred to in paragraph 1, the payment service user shall provide the payment service provider with all the relevant information available to him regarding the events leading to the disputed payment transaction.	3. For the purpose referred to in paragraph 1, the payment service user shall provide the payment service provider with all the relevant information requested by the payment service provider and that the payment service user can reasonably be expected to have ~~available to him~~ regarding the events leading to the disputed payment transaction.	AT (MS drafting suggestions and comments): We can accept this amendment. SE (MS drafting suggestions and comments): We support the amendment. LV (MS drafting suggestions and comments): We support the amendments. HR

		*[**PRES comment:** The result of several discussions on fraud and fraud-relates issues.]*	(MS drafting suggestions and comments): We agree with this drafting. FR (MS drafting suggestions and comments): The drafting is too unbalanced and difficult to fulfil for the PSU, we'd like to rephrase it : 3. For the purpose referred to in paragraph 1, the payment service user shall provide the payment service provider with all the relevant information ~~requested by the payment service provider and~~ that the payment service user can reasonably be expected to have regarding the events leading to the disputed payment transaction. ES (MS drafting suggestions and comments): We agree with the changes proposed.

	~~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].~~		
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			IT (MS drafting suggestions and comments): IT. We strongly reiterate the need to introduce **clearer procedural rules**

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.			for PSPs when assessing PSUs' refund request. Currently, Article 56 only addresses cases where the payer is suspected of fraud and does not cover other possible (and far more common) reasons for refusing reimbursement of an unauthorized transaction, such as "gross negligence". In other words, Article 56 does not talk with Article 60. For the sake of clarity, we underline that in our national experience (and thus not under a strictly "objective" approach), Art. 73 and Art. 74 PSD2 have led to a situation where the PSP refunds, within one business day, the full amount, but such refund is made "under reserve" ("salvo buon fine"). At a later stage (sometime after months) the PSP debits the PSU again, if it concludes (unilaterally) that there has been gross negligence on the part of the PSU. (After that, the PSU is free to bring the matter to the Courts or to an ADR scheme). This approach is consistent with the European Commission's response to Q&A No. 223 here (albeit in the context of PSD1).

			Due to this lack of clear rules, **a preliminary reference has been raised by a Polish Court (C-70/25 [Tukowiecka])** regarding the interpretation of Art. 73 and 74 PSD2. The key question is whether a PSP may refuse the reimbursement of an unauthorized transaction on the grounds that the PSU was grossly negligent or – as proposed by the national court – whether the PSP must first reimburse the PSU and then refer the matter to a court. If the national court's interpretation were to be upheld by the CJEU, it could have an extremely significant impact on the application of the PSD2 across multiple MSs, where the PSP can debit the PSU again if "gross negligence" is established at a later stage. **The existence of such widely divergent interpretations on an issue with significant implications for the implementation of PSD2 (a decade after its adoption) clearly highlights the need for a more detailed and coherent legal framework**. This need is even more pressing given the innovations that the PSR will introduce.

			In our view, **it is essential that the PSR clarifies that PSPs are able to independently assess whether the PSU was grossly negligent and, on that basis, deny the refund request**. If PSPs were required to refund the PSU at T+1 (except when there is a suspicion of fraud by the PSU, which is and should be a very rare occurrence) but were then unable to recover the funds in case of gross negligence, unless they initiated court proceedings (which would be economically unfeasible for low value transactions and on such a massive scale), the resulting framework would be quite dysfunctional. In practice, the substantive rules governing the PSU's liability would be unenforceable. To clarify the procedural rules, we believe there are two main approaches that could be considered: 1. **Proposal 1 - T+1 only for**

			non-compliance with SCA: one approach would be to recognize that the T+1 rule is better suited for a stricter application of "objective theory", which requires simpler and more automatable controls (roughly, compliance with SCA). Under a non-strictly objective approach, the PSP should have time to make a more complex assessments of the relevant circumstances. Accordingly, the T+1 rule could be limited to cases where SCA was not applied, , while in any other cases there would be a deadline by which the PSP should either refund the payer or justify the reasons for the refusal. 2. **Proposal 2 - T+1 plus reclaim by the PSP:** another approach would be to maintain the T+1 rule, in order to ensure that the reimbursement is prompt and to prevent PSPs from using the time needed to collect and assess

			information as a means to delay (or effectively deny) the refund. However, if the T+1 rule is retained, it should be made clear that the PSP has the right to debit the payer's account again in cases where it subsequently determines that the refund was unjustified. Find our proposals below, with the changes from the original EC proposal highlighted. We remain fully open to discussing alternative suggestions. ***PROPOSAL 1* - T+1 only for non-compliance with SCA** *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: ***(a) if payer's payment service***

			provider has failed to fulfil_the obligation to require strong customer authentication set out in Article 85 or an exemption from the application of strong customer authentication has been applied, 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; ***(b) unless it has refunded the payer according to point (a),_the payer's payment***

			service provider, within XX business days after noting or being notified of the unauthorised transaction, shall refund the payer the amount of the unauthorised payment transaction or 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 justification provided. 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:~~ ~~(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.~~ 3. **[NO CHANGE]** 4. Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund***, in accordance with paragraph 1,*** ~~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 unauthorised payment transaction not taken place. 5. **[NO CHANGE]**

			6. **[NO CHANGE]** ***PROPOSAL 2 -*** **T+1 plus reclaim by the PSP** *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.

			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 *XX* ~~*10*~~ 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. ***2a. If the payer's payment service provider has refunded the payer in accordance with paragraph 1, and***

			subsequently obtains evidence, pursuant to Article 55, that 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, or that any other reasons exist for the payer to be held liable for the payment transaction, the payer's payment service provider can recover from the payer the amount refunded and, where applicable, debit that amount directly from the payer's payment account, no later than XX business days after the refund took place. ***The payment service provider shall provide to the payer, on a durable medium, a justification for its decision 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. **[NO CHANGE]**

			4. Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund***, in accordance with paragraph 1 and without prejudice to paragraph 2a,*** ~~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 unauthorised payment transaction not taken place. 5. **[NO CHANGE]** 6. **[NO CHANGE]**
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.			
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 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 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			
		*[**PRES comment:** The presented wording is built on the proposal presented by the PRES and comments of Member States in this regard.]*	HR (MS drafting suggestions and comments): It is not clear why is almost entire Article 57 being deleted, so clarification is needed here.
		Where PSPs fail to comply with their obligations under Article 50, and where that failure results in a defectively executed payment transaction, the payer's PSP shall without delay refund the payer the	LV (MS drafting suggestions and comments): We support the amendments. IT (MS drafting suggestions and comments):

		amount transferred and, where applicable, restore the debited payment account to the state in which it would have been had the transaction not taken place.	IT. We agree. However, to fully align the PSR with the IPR, the following should be added (see Art. 5c(8) IPR): "*Where the failure to comply occurs because the payee's PSP, or the payment initiation service provider, failed to comply with its obligations under this Article, the payee's PSP or, where relevant, the payment initiation service provider, shall compensate the payer's PSP for the financial damage caused to the payer's PSP by that failure.* *Any further financial loss caused to the payer may be compensated in accordance with the law applicable to the contract concluded between the payer and the relevant PSP*". IE (MS drafting suggestions and comments): This should be a reference to "payment service providers" not "PSPs". HU

			(MS drafting suggestions and comments): In order to ensure consistency, we would consider referring to Article 5c (8) of Regulation (EU) 260/2012. HR (MS drafting suggestions and comments): When amending this Article, care should be taken to include all liability provisions relating to PSPs obligations in Article 50 PSR. It seems that the new proposal does not cover all the liabilities from IPR which were foreseen in the proposal for the January meeting where it was proposed that the PSPs shall comply with the provisions of Article 5c(8), subparagraphs 2-4 of Regulation (EU) 260/2012. ES (MS drafting suggestions and comments): We agree with the changes proposed.

			DE (MS drafting suggestions and comments): **Change Request** While we do see the merits in harmonizing the provision with the wording from the IPR, **we prefer the previous drafting of Art. 57**. In partiuclar: - the current wording does not deal with cases where there has been fraud or gross negligence on the part of the payer when authorising the transaction. Under the current wording, PSPs will be liable irrespective of whether there has also been fault on the part of the payer - the current wording leads to a PSP's liability irrespective of whether the PSP is responsible for the lack of compliance with its duties under Art. 50. We believe that the liability should be fault-based; e.g. a PSP should not be

			liable where the lack of compliance with Art. 50 is due to circumstances beyond the PSPs control / outside it`s sphere (i.e. due to a power cut etc.) - the current wording only stipulates a claim of the payer against its PSP. It remains unclear whether the payer's PSP should also be held liable where failure to perform transaction monitoring was due to a lack of compliance on the part of the payee's PSP. If so, we would consider this an unbalanced liability. Hence, we propose to retain Article 57 and clarify that the provision of Article 57 prevails over the respective provisions of the SEPA regulation.
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		~~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~~	

identifier and the name of the payee provided by the payer.		~~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.~~	
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:	~~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;		~~(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.		~~(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 provider of the payee shall refund the financial damage incurred by the payment service provider of the payer.		~~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 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).		~~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).		~~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).		~~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 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			IE (MS drafting suggestions and comments): Could this result in TSPs and schemes being disproportionately liable for matters outside their control, bearing in mind some TSPs only have a peripheral role in payment services?

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			
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.		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 or website or mobile application of that payment service provider unlawfully and that manipulation gave rise to subsequent fraudulent authorised payment	SI (MS drafting suggestions and comments): SI: We would prefer that the term "consumer" is replaced with a broader term "payment service user" to offer equal protection to both natural and legal persons. Our concern are in particular natural persons performing business activities (enterpreuners) as well as small enterprises, as we have seen from practical experience that also these are vulnerable to bank impersonation fraud. Furthermore, any legal entity can fall victim to bank impersonation fraud.

		transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without undue ~~any~~ delay, reported the fraud to the police and notified its payment service provider when becoming aware of the fraud, providing the payment service provider with all the relevant information requested by the payment service provider and that the payment service user can reasonably be expected to have regarding the events leading to the disputed payment transaction.	NL (MS drafting suggestions and comments): 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 email address, name and telephone number, name and website, or name and mobile application of the 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 **payment service user, when becoming aware of the fraud, reports the fraud without undue delay to the police and its payent service provider and provides** the payment service provider with all the relevant information requested

			by the payment service provider **insofar as** the payment service user can reasonably be expected to have **such information** regarding the events leading to the disputed payment transaction. LU (MS drafting suggestions and comments): LU: we support the use of cummulative criteria, according to the wording proposed by the PRES during the working party on 29.04 IE (MS drafting suggestions and comments): IE suggests some examples of "all the relevant information" could be provided within a Recital. HR (MS drafting suggestions and comments): We do not agree with the proposal for Article 59(1) to revert to only one of the given elements in the fraud to be considered as bank

			employee impersonation fraud. In our opinion, it is not sufficient to hold the PSP liable for the fraud where fraudster uses only the PSP's name because we believe that there is no possibility for the PSP to take any preventive measure in such a case. In practice it is possible that the fraudster calls a PSU saying that he or she is a bank employee, so using just PSP's name without combining it with the other element should not be sufficient. FR (MS drafting suggestions and comments): We are stongly opposed to this pre-requisite condition, that add more complexity. We suggest removing the requirement to report the fraud to the police, which could be difficult for consumers (notably vulnerable group of persons like persons with disabilities, older persons, people with low digital skills and those who do not have access to digital channels) to comply with.

			We would suggest to list the information needed by the PSP, enabling the PSU to be aware of the expectations in case of payment transaction dispute. ES (MS drafting suggestions and comments): In order to prevent moral hazard cases, we propose the following adjusting to the wording: *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~~ and e-mail address or the name and telephone number or website or mobile application of that payment service provider unlawfully (…). EL (MS drafting suggestions and comments): **EL:** We are satisfied for taking into consideration our suggestions. CZ (MS drafting suggestions and comments): We still suggest deleting Article 59 and stick to PSD2 approach to liability for unauthorised payment transaction.
2. Within 10 business days after noting or being notified of the fraudulent			EL

authorised payment transaction, the payment service provider shall do either of the following:			(MS drafting suggestions and comments): **EL:** We propose to align with the 15 days introduced above in 57.2. This is a recurring comment not having been taken into account.
(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, 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 to calling line identification and electronic mail address.			
		Article 59a	
		Cross-sectoral cooperation for the purpose of fraud prevention and detection	EL (MS drafting suggestions and comments): **EL:** We welcome the introduction of this article. However, we continue to believe that it would be beneficial if obligations for ECSPs could also directly arise in connection with liability, rather than relying solely on national law. We

			would also prefer direct requirements in relation "verification of the advertisers of financial products" as Ireland had suggested in its non-paper, including involved actors in the scope of PSR (article 2).
		*[**PRES comment:** The below proposal was presented at the April CWP meeting.]*	IE (MS drafting suggestions and comments): It is important the definition of 'electronic communication service providers' captures firms regulated under the DSA in its scope. HU (MS drafting suggestions and comments): We welcome the provisions set out in this Article, specifically in the paragraphs on Cross-sectoral cooperation for the purpose of fraud prevention and detection, which represent progress compared to previous measures. However, we miss the extension of liability rules to ECSPs, especially in situations where they didn't apply protective

			measures, or where they didn't remove fraudulent content or communication channels used to commit ause that they detected or brought to their attention, or where they didn't comply with notification obligations. HR (MS drafting suggestions and comments): We accept the proposed approach for this cooperation.
		1. For the purpose of preventing and detecting fraud, including that referred to in Article 59(1), providers of 'electronic communications services' as defined in Article 2(4), points (a) and (b), of Directive (EU) 2018/1972 shall have in place measures to ensure effective cooperation with payment service providers, having regard to the	LV (MS drafting suggestions and comments): We support the amendments. LU (MS drafting suggestions and comments): LU: we prefer limmiting the scope of the ECPS requirements introduced in the PSR only to providers of interpersonal communications services as defined in Article 2(4)b) of the directive 2018/1972.

		technical characteristics of each of their services.	ES (MS drafting suggestions and comments): We support the inclusion of more specific cooperation requirements for ECSP. Moreover, we support the broad definition of ECSPs as it is stated in this paragraph (article 2(4) points (a) and (b). CZ (MS drafting suggestions and comments): We strongly prefer to apply the definition of ECSPs only to Article 2(4) letter (b) of the Code. Overall, we believe that PSR should not impose additional obligations on SMEs, as most related fraud issues occur on very large online platforms and search engines.
		For the purpose of the first subparagraph, without prejudice to Directive (EU) 2022/2555, Directive 2002/58/EC or Article 91 of this Regulation, electronic	LV (MS drafting suggestions and comments): We support the amendments.

		communications services providers shall establish dedicated communication channels with payment service providers to allow for faster and more effective sharing of any information that could be useful in the prevention and detection of fraud within the meaning of this Regulation and in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC.	
		2. Payment service providers may make use of the notification mechanisms referred to in Article 16 of Regulation (EU) 2022/2065 to notify providers of hosting services of the presence on their service of specific items of information that they consider, including based on notifications	LV (MS drafting suggestions and comments): We support the amendments.

		received from payment service users, illegal content within the meaning of this Regulation. Payment service providers may also apply to be awarded trusted flagger status pursuant to Article 22 of Regulation (EU) 2022/2065.	
		3. The Commission and the European Board of Digital Services shall encourage and facilitate the drawing up of a voluntary code of conduct at Union level to foster prevention, enhance security and combat payment fraud and financial scams, under the conditions set out in Article 45 of Regulation 2022/2065.	LV (MS drafting suggestions and comments): We support the amendments.
Article 60			
Payer's liability for unauthorised payment transactions			

1. By way of derogation from Article 56, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.			
The first subparagraph shall not apply where any of the following occurred:			
(a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or			
(b) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.			
The payer shall bear all of the losses relating to any unauthorised payment transactions if those losses were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 52 with			HU (MS drafting suggestions and comments): In our view, currently that is not clear whether on this subparagraph

intent or gross negligence. In such cases, the maximum amount referred to in the first subparagraph shall not apply.			the PSP may refuse the refund under article 56 if the payer acted with intent or gross negligence. Based on our understanding Section 1 of Article 56 of the PSR imposes an obligation for the PSP to refund the transaction within one business day, except for that the PSP has reasonable grounds for suspecting fraud committed by the payer. In the latter case the PSP communicates it to the NCA. It has to be considered, that based on Section 1 of Article 56 the PSP has to refund within one business day the amount of the unauthorised transaction, even if the PSP suspected fraud committed by other person than the payer and the payer was grossly negligent (as the PSP only be exempted from the one business day refund obligation if it suspects fraud committed by the payer). Therefore, it shall be specified that if the PSP has

			refunded the amount under Section 2 (as it did not suspect fraud by the payer, but suspected fraud by an other person), but after an investigation by the PSP it has concluded that the payer was grossly negligent, can the PSP then claim the amount back from the PSU and how? 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. In the light of the EJC preliminary ruling it could be considered to introduce a clarification in the PSR.
Where the payer has neither acted fraudulently nor intentionally 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.		Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 52, national competent authorities or dispute resolution bodies, in accordance with their requisite powers or payment service providers may reduce the liability referred to in this paragraph, taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment	HU (MS drafting suggestions and comments): It would be very important to clarify the meaning of ”requisite power”, as currently it may give rise to misinterpretation, how this process will work in practice. HR (MS drafting suggestions and comments): We accept the proposed wording. ES (MS drafting suggestions and comments): We agree with the changes proposed.

		instrument was lost, stolen or misappropriated. *[**PRES comment**: The proposal presented at the April CWP meeting.]*	DE (MS drafting suggestions and comments): **Remark** In our view, it is systematically wrong to refer to the bodies that may reduce the aforementioned liability. Dispute resolution bodies, be it courts or ADR entities, base their decisions on the applicable law. If, therefore, the substantive law provides for a reduction in liability, courts and ADR entities will apply such a provision without a need for it being expressly stated within the substantive law. The same applies for national competent authorities. We would therefore suggest the following wording: "Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 52, national competent authorities or dispute resolution bodies, in accordance with their requisite

			powers, or payment service providers may reduce the liability referred to in this paragraph may be reduced, thereby 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.”
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 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 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 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			
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:	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

		*[**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 deviation was not intentional.]*	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.*
(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 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. 62(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): **As we have pointed out many times. The refund for direct debits should be maintained as follows:** **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~~ **for 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. In the CZ, direct debits are debtor-driven, which provides the payer with sufficient guarantees. It is noteworthy that in the Czech Republic, there are almost 0% requests for direct debit refunds. The PSD2 approach constitutes a well-balanced approach in this respect and gives debtor-driven direct debits a high level of reliability for PSUs (consumers and businesses).
2. For the purposes of paragraph 1, first subparagraph, point (b), the payer			ES

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.			(MS drafting suggestions and comments): Particularly, we suggest including an additional paragraph 2a: *Direct debits where the tax authority is the payee are excluded from paragraph 1.*
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;			
(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 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:		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 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 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).			
Article 65			
Refusal of payment orders	**Refusal ~~of payment orders~~ to execute a payment order**		
		*[**PRES comment:** The new proposal for this Article will be part of the discussion at the CWP meeting on 29 April.]*	
		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	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.

		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.]*	We suggest to delete " if agreed in the framework contract" in the next paragraph to mitigate the risk.
		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 other relevant information available to the payment service provider, the payment service provider has duly justified and	BG (MS drafting suggestions and comments): *We consider that in order to increase consumer protection PSPs should be obliged to refuse the execution of suspected fraudulent payment transaction by operation of the law and not **only** if it was agreed with the consumer. In practice payment service users are not in a position to negotiate the clauses of the framework contracts and it is up to the PSP to decide whether such blocking shall take place. In that regard, we suggest to delete any*

		reasonable grounds to suspect fraud against the payment service user. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	*reference to the framework contract in this paragraph.* 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 block the acceptance of the payment transaction if there is suspicion of fraud.** With that purpose, we suggest to adjust the wording: *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 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. *In the same vein, the payee's payment service provider may reject the reception of the funds when it has duly justified and reasonable grounds to suspect fraud against the payment service user.*
		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.]*	
		Without prejudice to Article 69(1), where based on the transaction monitoring referred to in	PT (MS drafting suggestions and comments):

		Article 83 and on any other relevant information available to the payment service provider, the payer's payment service provider suspects that the payer may be a victim of fraud, the payer's payment service provider shall, without undue delay, notify the payer, in an agreed manner, of any information or action needed from the payer to enable the payment service provider to decide whether there are reasonable grounds to suspect fraud. The notification shall give the payer sufficient information to enable the payer to understand the risks that the payment service provider has identified.	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). **Dafting suggestions:** "The notification shall give the payer sufficient information to enable the payer to understand the risks that the payment service provider has identified. **The information shall include elements such as the identification of the payee, the payment instrument, the transaction's value, the channel used, the risks identified or any possible disclaimers to the payer**." HU (MS drafting suggestions and comments):

		*[**PRES comment**: The proposal presented at the January CWP meeting.]*	Subparagraph 3 and 4 of Article 65(1a) refers to the timelines specified in Aricle 65(1). Please note that Member States might determined shorter executions times for domestic payments denominited in the national currency of the Member State. This shorter execution time might not be enough for the payment service provider to contact the payer, thus we suggest determining an exact timeframe whithin which the payment service provider can to contact with the payer. ES (MS drafting suggestions and comments): We agree with the changes proposed.
		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	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

		assess, based on the transaction monitoring referred to in paragraph 1, and on any other relevant information available to the payment service provider, whether or not to execute the payment order. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	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.**
		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.]*	BG (MS drafting suggestions and comments): *We would like to once again reiterate that this exemption shall also apply to card payment transactions. Card payment transaction usually happens in two stages- first the authorisation takes place- at the moment the payer interacts with the POS, regardless if online or at the store, the payer inputs the security credentials and the issuer verifies that there are sufficient funds available on the account. The second stage is the actual settlement when the authorised amount is transferred*

			from the issuer to the acquirer. At the moment of the authorisation (this happens in a matter of seconds) the payee hands over the goods or services to the payer and the payer can no longer revoke the transaction even though the actual settlement is differed in time. Thus, the issuing PSP faces the issues to contact the payer in real time with card payment transaction authorisations as with instant payments and the same legal requirements should apply in both cases.
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 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.		2~~1~~. Where the payment service provider refuses to execute a payment order or to initiate a payment transaction, the payer's payment service provider shall notify the payer and, where applicable, the payment initiation service provider, of the refusal and~~, if possible,~~ the reasons for that refusal and the procedure for correcting 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.]*	
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 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	HU (MS drafting suggestions and comments): In this case it would be important to exactly give Member States the possibility to determine shorter notification time in case of national payment transactions which has shorter maximum execution time based on Article 72 as well.

		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. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	
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		~~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~~	

payee, unless prohibited by other relevant Union or national law.		~~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) 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.	~~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.~~ *[**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 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	~~4. Before refusing to execute a payment order, or in the case of an instant credit transfer, immediately after the refusal of the payment order, the payment service provider shall notify the payer of the refusal and the reasons for it, in an agreed manner at the earliest opportunity, and in any case within the periods specified in Article 69, or, in case of instant credit transfers in euro, within 10 seconds of the time of receipt of the payment order by the payer's payment service provider. Information about the reasons for refusal may not~~	

	mistakes that led to the refusal the payment order.	~~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.~~ *[**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 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 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.			
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 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 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.			
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 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.]*	
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.			
		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.]*	

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 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).	ES (MS drafting suggestions and comments): We do not have objections to the proposal.

		For payment transactions with electronic money tokens from a custodial wallet to a self-hosted 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 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 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			

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.			
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 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 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 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 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 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			

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 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 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 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.			
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 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 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			NL (MS drafting suggestions and comments): Payment systems and payment service providers shall be allowed to process special categories of personal data as referred to in

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 rights and freedoms of natural persons, including the following:			Article 9(1) of Regulation (EU) 2016/679 **and Article 10(1) of Regulation (EU) 2018/1725) and when it concerns fraud prevention and detection payment systems and payment sevice providers shall be allowed to process data as referred to** Article 10~~(1)~~ of Regulation (EU) 2018/1725 **and article 11 (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 rights and freedoms of natural persons **and subject to the rights for the data subject enshrined in Regulation (EU) 2018/1725**, including the following DE (MS drafting suggestions and comments): **Important Remark**

			We see a considerable need for discussion regarding this provison. In order to further 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?
(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
			NL (MS drafting suggestions and comments): **(c) measures to prevent de-risking and disproportionate measures a a result of transaction monitoring and fraud data exchange.**
CHAPTER 7			
Operational and security risks and authentication			
Article 81			
Management of operational and security risks			
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.			
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;			
(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		~~Payment service providers shall provide to the competent authority~~	HU (MS drafting suggestions and comments):

[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).

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.		~~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.~~ *[**PRES comment:** Part of simplification approach agreed upon by Member States.]*	We would suggest reconsidering this provision as it can be a useful information for competent authorities. ES (MS drafting suggestions and comments): We agree with the changes proposed. DE (MS drafting suggestions and comments): **Remark** We support this deletion.
2. The EBA shall promote cooperation, including the sharing of information, in the area of 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 analysing the trends observed on the basis of these data.	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 report analysing the trends observed on the basis of these data. ***[PRES comment:*** *The amdendment follows the*	ES (MS drafting suggestions and comments): We agree with the changes proposed.

		Member State's doubts as to whetеher 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.]	
	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 arrangements have been made under which the EBA will receive the data that is due under this Article.	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 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 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	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		

authorities to the EBA, as referred to in paragraph 1.	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>		
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 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.	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 Regulation]. Power is delegated on the Commission to adopt the <u>implementing</u> ~~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~~**		
		*[**PRES comment:** The proposal for this Article will be part of the discussion at the CWP meeting on 29 April.]*	

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.			BG (MS drafting suggestions and comments): (c) enable payment service providers to prevent and detect in real time potentially fraudulent payment transactions, including transactions involving payment initiation services. *(based on our imput for recital 100)* NL (MS drafting suggestions and comments):

			After c, we would like to add paragraph d. Especially data exchange with the police is crucial for us: **'(d) enable payment service providers to establish accountability towards supervisors, to inform decision about liability towards the customer and to inform the police for purposes of criminal investigation'.**
	1a. The payment service provider of the payer shall carry out the transaction monitoring referred to in paragraph 1 prior to the execution of a payment transaction. Without prejudice to Article 69(2), the payment service provider of the payee shall also carry out transaction monitoring of received payment transactions.		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 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:	~~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 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,~~	
	b) the payment instruments used by the payment service user,	~~b) the payment instruments used by the payment service user,~~	
	c) the types of transactions carried out by the payment service user,	~~c) the types of transactions carried out by the payment service user,~~	
	d) the dates of the transactions executed,	~~d) the dates of the transactions executed,~~	
	e) based on the process/execution arrangements and policy/principles/ of payment service providers the electronic transactions executed by the payment service user, including the environmental and behavioural characteristics which are usual of the payment service user in the circumstances of a normal use of the personalised security credentials.	~~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.]*	
	The data referred to in points a) to e) shall be aggregated in order to identify the usual behaviour of the payment service user.	~~The data referred to in points a) to e) shall be aggregated in order to identify the usual 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.]*	

(a) information on the payment service user, including the environmental and behavioural characteristics which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials;	(a) information on the payment service user, including the environmental and behavioural characteristics which are ~~typical~~ usual of the payment service user in the circumstances of a normal use of the personalised security credentials;	(a) information on the ~~payment service user~~ payer, including the environmental and behavioural 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.]*	IE (MS drafting suggestions and comments): IE notes that the concept of environmental and behavioural characteristics has not been defined in PSR. We would suggest that further clarity on what constitutes environmental and behavioural characteristics should be provided either in the PSR itself or in the proposed EBA Guidelines.
(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 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.]*	FR (MS drafting suggestions and comments): We would suggest adding some explanatory elements relating to the information expected, such as the collection of data on the environmental and behavioural characteristics typical of the payee in the circumstances of a normal use of his account.
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.			NL (MS drafting suggestions and comments): Payment service providers shall not store data referred to in this

Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:			paragraph longer than necessary for the purposes set out in paragraph 1, and not after **three years after** the termination of the customer relationship. Payment service 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	~~3. Without prejudice to Article 69 and 71 of the~~	

	the European Parliament and of the Council, the payment service provider of the payer and the payee shall monitor payment transactions before the execution of the transaction in order to identify unusual transactions.	~~Regulation (EU) 2024/1624 of the European Parliament and of the Council, the payment service provider of the payer and the payee shall monitor payment transactions before the execution of the transaction in order to identify unusual transactions.~~ *[**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 unique identifiers shall be	~~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 unique~~		

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).	~~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).~~		
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 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.	~~5. Payment service providers shall notify competent authorities of their participation in the 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		
		*[**PRES comment:** The new proposal for this Article will be part of the discussion at the CWP meeting on 29 April.]*	IE (MS drafting suggestions and comments): Commission's Legal staff responsible for AML/CFT need to

			be satisfied that these provisions as drafted do not conflict with any information sharing provisions in the AMLR.
	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.]*	IE (MS drafting suggestions and comments): There appears to be a slight anomaly in the text of Article 83a in terms of the circumstances in which information relating to fraud can be shared. Pursuant to Article 83a, it is proposed that PSPs can exchange information to the extent it is strictly necessary to comply with 83(1)(c). However, in Article 83a(1a), the text provides that the information shall only be exchanged when necessary to comply with Article 83(1)(c). If it is the case that information can only be shared where strictly necessary to comply with Article 83(1)(c) obligation, we would suggest that guidance is provided either in the primary text or in the

			proposed EBA Guidelines as to what firms should understand strictly necessary to mean. ES (MS drafting suggestions and comments): We agree with the changes proposed
	(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, 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.]*	NL (MS drafting suggestions and comments): (i) contact details, including e-mail address and telephone number **of the payee**. IE (MS drafting suggestions and comments): The drafting doesn't confirm who this information relates to i.e. is it the payer or payee or both. The text could provide more clarity. ES (MS drafting suggestions and comments): We agree with the changes proposed
	1a. A payment service provider may exchange such data with other payment service providers who are subject to an information sharing arrangement as referred to in paragraph 3 where: the payment service provider has reasonable and objective grounds to		DE (MS drafting suggestions and comments): **Remark** We still see the need for further clarification as to what constitutes

	suspect a fraudulent behaviour by a payment service user.		"reasonable and objective 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).		NL (MS drafting suggestions and comments): 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**s** (c) **and (d)**.
	1b. Payment service providers shall implement appropriate technical and organisational measures, including		

	measures to 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 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.		DE (MS drafting suggestions and comments): **Remark** 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 participants in the information sharing arrangement or, where applicable, as soon as their membership ceases.	~~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 participants in the information sharing arrangement or, where applicable, as soon as their membership ceases.~~ *[**PRES comment**: Part of simplification approach agreed upon by Member States.]*	DE (MS drafting suggestions and comments): **Remark** We support this deletion.
	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		NL (MS drafting suggestions and comments): 5. Payment service providers shall not rely solely on the information

	shall 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.		received in the context of the data sharing referred to in para. 1 to comply with the requirements of this Regulation and shall 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. **Datasharing 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** 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. We propose to add the

			following sentence at the end of the paragraph: *"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. *[**PRES comment**: The proposal presented at the January CWP meeting.]*	NL (MS drafting suggestions and comments): **For the purposes of this Article, payment service providers shall share the data as referred to in pargraph 1 with the relevant competent national authorities to the extent strictly necessary to comply with their obligations in article 83(1), point (d).a** ES (MS drafting suggestions and comments): We agree with the changes proposed
		Article 83aa	
		Platform on combatting fraud	

		*[**PRES comment:** The proposal for this Article will be part of the discussion at the CWP meeting on 29 April.]*	ES (MS drafting suggestions and comments): We propose to specify the mandate and draw clearly the functions of this platform in terms of cooperation, exchange of information/best practices.
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 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 1093/2010 with regard to the programmes on payment fraud risks referred to in paragraphs 1 and 2 of this Article.	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 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.		ES (MS drafting suggestions and comments): We agree with the changes proposed.
	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	4. Member States shall have in place adequate measures to raise awareness among the	CZ (MS drafting suggestions and comments):

	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 reaching out to the most vulnerable consumer groups, including older persons or those with low digital skills.	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 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 (...)")]*	The provision should not be part of a binding legal text. It is a text that should be in the recital. It is not a regulation of the provision of payment services, but an appeal to the Member States. How will the provision be enforced? Will this provision not endanger the fiscal balance of the Member States in the event of liability?