Council of the European Union
General Secretariat

Brussels, 25 February 2025

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

WK 2589/2025 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 of the MS replies to the Presidency Questionnaires PCY questionnaire on fraud authorisation and liability . Deadline 17 December 2024. Replies from 20 MS

Presidency questionnaire on the PCY Discussion Note on authorisation of payment transactions and fraud in PSR
From: AT, ES, SK, SI, SE, RO, PT, NL, LV, LU, LT, IT, IE, HR, FI, DK, DE, CZ, CY, BG **Updated: 25/02/2025 12:50**

Questions	MS comments
Delineation between authorised / unauthorised payment transactions	

hich of the specific cases of payment transactions below should be treated in PSR as "authorised":	AT (MS comments): Please take into account, as a general remark, our stance on the delineation between authorised and unauthorised transactions: We do not support adding subjective elements to the concept of authorisation, since this would excessively broaden the liability of PSPs to fraud cases outside their sphere of responsibility. Deceptions and manipulations that affect the PSU's decision-making with respect to transaction amount, payee, or transaction purpose are outside the immediate responsibility of the PSP. Holding the PSP liable in cases of flawed decision-making, nonetheless, would present a significant shift in principle. We consider this approach immensely unbalanced and risky, most probably leading to increased consumer prices that would burden all consumers. Besides, it could also lead to an increase in moral hazard and, thus, even facilitate the successful execution of fraud. Moreover, under the current COM proposal, the burden of proof for authorization (=consent) would shift to the PSP (we oppose this due to the apparent difficulties PSPs would face in proving circumstances beyond their control). If the concept of authorization were further burdened with subjective criteria, it would effectively lead to an almost unavoidable liability for PSPs in cases of fraud, making them liable in all cases where a PSU denies having authorised a transaction. SE (MS comments): We advocate a principles-based liability model adaptable by case law. Therefore, we do not think it is a constructive approach to list specific cases where a transaction is to be classified as authorised or not. We think that the general principle for social engineering fraud should be that transactions which the PSU has been misled or forced to authenticate should be treated as unauthorised. This would mean that victims of social engineering fraud may have their case tried for **possible compensation**, given that they have not acted with gross negligence. This does however **not** mean that the significance of the PSU's own part in social manipulation fraud is ignored, as it is a key aspect of the gross negligence assessment, along with other relevant aspects.

	Furthermore, we are concerned about the phrasing 'where the payer gave consent to the execution of the payment transaction, **in the form and following the procedure agreed with its PSP'**. It could be understood as leaving the definition of consent to the PSP. PSPs should not be able to circumvent the consent by checking a box for a specific form and procedure specified in the framework contract. PT (MS comments): **Preliminary comments:** • As stated before, we favour a solution already envisioned by the EBA expressed in paragraph 31(a)(ii) of the 'EBA Opinion on new types of payment fraud and possible mitigants' (EBA-Op/2024/01), where it is specified that, in case of payer-initiated transactions (e.g., credit transfers), a transaction denied by the payer cannot be considered as authorized where the payment order was initiated by a fraudster, even if it was subsequently authenticated by the PSU. • Besides the solution above, we do not support adding more subjective elements to the concept of authorisation, since this would excessively broaden the liability of PSPs to fraud cases outside their sphere of responsibility. As such: - we supported the proposed drafting of article 49(2)(ii) that states that transactions initiated by a third party using the personal security credentials of the PSU shall not be considered authorized; but - we don't agree with the proposed drafting of article 49(2)(i) that includes the subjective notion of intent from which result scenarios difficult to evaluate by PSPs and NCAs. Also, this notion of intent is independent from technical security measures taken by the PSPs. Thus, in such cases, there is no basis for assigning responsibilities to the PSPs. Furthermore, the PSP is not able to assess the intention of the payer. **In short, we consider that for a transaction to be considered authorized, it needs to be both initiated and authenticated by the payer**. Other criteria, namely intent or other subjective indicators, and scenarios of manipulation should be left out of the equation. If we have a payment transaction, in the form and following the procedure agreed between PSP and PSU and if the PSU, itself, orders the payment transaction, this transaction should be deemed as authorised. PSP's do not have the means and are not in a position to acess the intention of the payer or to evaluate other subjective circumstances (this kind of evaluation should only be done by courts).

	NL (MS comments): We had some discussion on how to interpret this question. We interpret the question as: which cases of the ones listed below should be seen as authorised or not. In that case our answer is that all of them should be seen as authorised. We find it important that the concept of authorised is not altered and that once something is authorised, there will be no discussion on whether something was really authorised (with intent) or whether the person who authorised the payment was manipulated to do so. Therefore, we do not support adding subjective elements to the concept of authorisation. LU (MS comments): **LU:** We would like to stress out that it **is of utmost importance to ensure that a definition of authorization achieves legal certainty, irrevocability and predictability**. This approach should be retained for all type of payment transactions and all payment instruments used. In our view both PSPs and PSUs would highly benefit from a legally sound and predictable approach. Thus, we object to the introduction of subjectivity elements in the definition of the concept of authorised transaction. The following comments reflect our current assessment; we reserve our right to modify positions during the ongoing negotiations. IT (MS comments): **IT.** As a preliminary remark, we point out that, so far, the '*impersonation fraud*' has been treated in the discussion as if it should always have the same consequences in terms of qualifying a transaction as authorised or not. In our opinion, very different scenarios fall under the umbrella of "impersonation fraud", depending on the effect the fraud has on the victim's behaviour. For example, as a result of the fraud, the victim may be persuaded to: 1. surrender its credentials to the fraudster; 2. perform actions that results into a payment, without being aware of it (e.g. being persuaded to make a 'fake' payment for security reasons: see scenario 4 of the DE non-paper);

	3. knowingly make a payment, but with the erroneous belief, induced by the fraudster, that the IBAN entered corresponds to the intended payee; 4. knowingly make a payment, but for the wrong reasons. All these cases can result from 'impersonation fraud', but - in our opinion - only in the first two cases the "*consent to the execution of the payment transaction*" is missing (and the transaction unauthorised). In the other two cases, the transaction should be treated as authorised (although case 3 is debatable; see below). Also as a preliminary remark, we point out that qualifying a transaction as unauthorised does not mean that it must always (or even in most cases) be refunded, since "gross negligence" will still operate as a concrete filter. Indeed, in our experience, "gross negligence" is the most important element to allocate the liability between the PSP and the PSU (the PSPs, in order to avoid liability, most often attempt to prove the "gross negligence" of the PSU, rather than trying to prove that the PSU was lying when he denied the transaction). The distinction between "authorized" and "not authorized" is more important to define the scope of the liability than to regulate it. IE (MS comments): On the delineation between authorised/unauthorised payment transactions, we would support consideration being given to what is practical and workable with less emphasis on the subjective elements. The below examples contain circumstances that would be very difficult to determine e.g. option 3 requires the PSP to determine the payer's full awareness of all relevant circumstances – how would this be measured and documented? FI (MS comments): FI: All our comments are of preliminary nature and based on the presumption that there will two categories of transactions, namely "authorised" and "unauthorised". DE (MS comments):

	General remark: DE does **not support broadening** the liability of PSPs to all fraud cases as we consider this approach to be unbalanced. <u>Differentiation whether PSU is aware or unaware of a payment transaction</u> According to our understanding of the consent requirement under PSD2, a payment transaction is already considered **unauthorized**, if the user is **unaware that he/she is initiating such payment transaction**. If there is no awareness of issuing a declaration of intent to initiate a payment transaction, it cannot, in our view, be regarded as consent. In such cases, **liability therefore rests with the PSP**. To illustrate our position, we refer to fraud scenarios where the PSU is somehow deceived by false messages or notifications to hand over SCA elements to the fraudster and the fraudster uses these elements – without the payer knowing – to complete a payment transaction initiated by the fraudster. We have presented a set of such fraud scenarios in our non-paper on fraud in November 2023. In our understanding of the current legal framework under PSD2, all of these cases should be considered as unauthorised. The relevance of those fraud scenarios is particularly mentioned in the Commission's Impact Assessment for the payments package. In our understanding of the PSD2, the situation is different only in scenarios, where the PSU is **aware that he/she is initiating a payment** but is mistaken about specific details of the transaction, such as the payee's identity or the exact amount. The fraudster thus manipulates the PSU with regard to the **underlying circumstances of the payment**. However, such errors do not invalidate the PSU's consent to execute the payment transaction itself and hence, the transaction should be considered authorised under the current PSD2 regime. We do not support broadening the definition of authorisations towards those fraud cases, since the deceptions and manipulations applied that affect the PSU's perception of the broader circumstances of the payment do not regard the consent to the payment transaction itself and hence, are outside the immediate responsibility of the PSP. Holding the PSP liable in cases of flawed decision-making, nonetheless, would present a significant shift in principle. We consider this approach immensely unbalanced and risky, most probably leading to increased consumer prices that would burden all consumers. Besides, it could also lead to an increase in moral hazard and, thus, even facilitate the successful execution of fraud. <u>Burden of proof</u>

	This is particularly relevant given that, under the current COM proposal, the burden of proof for user authorization (=consent) would shift to the PSP. We oppose this due to the apparent difficulties PSPs would face in proving circumstances beyond their control. If the concept of authorization were further burdened with subjective criteria, it would effectively lead to an almost **unavoidable liability for PSPs** in cases of fraud, making them **liable in all cases where a PSU denies having authorised a transaction**. <u>Narrow regulation of impersonation fraud related to banks</u> As regards impersonation fraud, we see a need for a well-defined shift in principles of liability for bank employee impersonation fraud as proposed by the COM in Art. 59. If the PSU is aware that he/she is initiating a payment but has been misled into doing so by a fraudster impersonating a bank employee, the payment, in our understanding, should still be considered as authorized. However, given that the bank bears a certain level of responsibility for preventing fraudsters from impersonating bank employees or otherwise acting in its name, an exception should be made in such cases, establishing PSP liability even for authorized payments. In this context, we would even go further and suggest broadening the scope to fake websites and apps assigned to the PSP that are used by fraudsters in order to take new forms of digital fraud into account. For other types of impersonation fraud, we do not see a direct responsibility of PSPs and hence, would consider it highly unbalanced to extend the PSPs liability to those fraud cases as well. However, we believe that such patterns of impersonation fraud will effectively be tackled by the new **IBAN name check** (art. 50), that specifically address misconceptions about the recipients.
	BG (MS comments): We believe that the existing framework of authorised payment transactions should be maintained in the PSR. We are of the opinion that payment service providers should not be held liable in situations where the fraud is 'external' to the payment transaction but relates to the underlying reasons. Moreover, we do not think that payment service providers should be required to investigate the awareness/state of mind (subjective elements) of the payment service user regarding the reasons leading to the payment transaction. Considering the above, we believe that option 1 of the 3 below represents a regime, similar the existing framework. However, we would like to highlight that option 1 excludes any subjective elements, which is recognized by the court practice on the current legal framework on authorisation of payment transactions and should be maintained.

1. where the payer gave consent to the execution of the payment transaction, in the form and following the procedure agreed with its PSP, regardless of whether the consent was given based on manipulated premises (e.g., regardless of whether the payer fell victim of an impersonation fraud)	AT (MS comments): This case should be treated as authorised. ES (MS comments): Not authorized if consent was given based on manipulated premises. SK (MS comments): Seems to be the most suitable option. SI (MS comments): We do not support this option. RO (MS comments): No. PT (MS comments): We consider the transaction resulting from this scenario should be classified as **authorised**. Nevertheless, in the case of an impersonation of the PSU's PSP, the provisions foreseen in article 59 may apply. It should be noted that in our understanding, the cases covered by article 59 should be restricted to authorised transactions where a PSU was manipulated by a fraudster pretending to act in representation of his PSP, using its spoofed e-mail address or telephone number. NL (MS comments): This should be treated as "authorised", in line with the existing PSD2-regime. LV

	(MS comments): If the payer has performed typical actions and the agreed procedures were followed, but it was not possible to identify the payee (e.g. no notification to confirm the payment with SCA), then this example could be considered as unauthorised. It would be considered authorised if the payer was able to identify the payee and the PSP can prove that the customer was alerted to the amount due and the payee. LU (MS comments): Such transaction should be considered as authorized, it is beyond the control of the PSP to verify or to identify in advance a transaction concluded based on manipulated premises. PSUs should be given the possibility to dispute the transaction and the burden of proof should be shared between PSU and PSP. We support the current PSD2 approach where the PSP has to prove that the payment transaction was "authenticated". IT (MS comments): **IT.** It depends on how the manipulation affected the consent of the payer (see our answer just above). If "*manipulated premises*" means "*a mistake, induced by the fraudster, on the 'underlying reasons' of the payment*", then the transaction should be considered as "authorised". HR (MS comments): We support only this approach for the definition of an authorised payment transaction. FI (MS comments): FI: Not necessarily. Manipulation through impersonation fraud could entail that the payer has not given their consent necessary to deem a payment transaction authorised. DK (MS comments): No, this should not be treated as authorised.

	DE (MS comments): DE supports this option. According to our understanding of the PSD2 regulation, **manipulated transactions** are considered **authorised** as long as the PSU **knows** that a payment transaction will take place and **gives consent** to that. This applies regardless of the way in which a manipulation takes place. The decisive factor is whether the **PSU initiates the payment transaction** himself/herself (authorised) or whether a third party obtains certain data and then initiates the payment transaction (unauthorised). According to our understanding of the consent requirement, a significant number of types of impersonation fraud should already be considered as unauthorised under the current PSD 2 regime (If, e.g. the PSU thought, the payment account would not be debited, because it was only a trial run /security check etc, a conscious consent to execute the payment transaction might be missing – thus making it unauthorised according to German case law.) If the PSU is instead **mistaken** about **any circumstances** underlying the payment, this **does not nullify the declaration of consent** to the payment transaction itself. CZ (MS comments): This payment transaction should be treated as **authorised.** For us, it is important that the consent is given by the payer in the agreed form and procedure. The crucial issue is who is giving the consent; if it is the payer, the transaction is authorized. The other result would be in case the PSP (or its employee acting on behalf of PSP) would mislead the PSU leading to unauthorised transaction. CY (MS comments): Such a payment transaction should be treated as “authorised”, unless the consent given by the payer was given based on manipulated premises.

2. where the payer gave consent, in the form and following the procedure agreed with its PSP, as regards the amount and the payee, provided that the payer was not manipulated as regards the identity of the payee by a fraudster impersonating the intended payee	AT (MS comments): This case should be treated as authorised. ES (MS comments): Authorized. SI (MS comments): We could support this option (BE PRE proposal - option C). However, we are concerned about the wording "as regards the amount and the payee", as it means that the PSP would need to verify information it is not otherwise obliged to, given the fundamental principle that the payment transaction is independent of the underlying obligations between the payer and the payee (please see the definition of the payment transaction). Additionally, if the clause "the payer was not manipulated…" remains, it should be limited to the fraudster impersonating the bank (bank employee impersonation fraud). RO (MS comments): Yes. We support this approach because it will help increase the payment service providers awareness to develop efficient transaction monitoring mechanisms and so contribute to fraud decreasing. Additionally, we believe that a payment transaction shall not be deemed as authorised if the payer was manipulated through complex fraud scenarios, as social engineering, into initiating the payment transaction in favour of a third party which was not the intended payee, or if the transaction was initiated by a third party using fraudulently obtained payment service user personal security credentials. PT (MS comments): As stated, if the payer initiated and authenticated the transaction following the procedure agreed with its PSP, the transaction should be considered authorised. Manipulation only plays a part in the case of impersonation of the PSU's PSP, where article 59 may apply.

	NL (MS comments): This should be treated as “authorised”. In case the question is whether this should be the definition of authorised, then ‘no’ as we do not support the inclusion of the subjective element that the payer was not manipulated. We do not want to make the concept of authorisation dependent upon the question whether the payer was manipulated. We see more merit in a separate reimbursement scheme for payment fraud (e.g. article 59 in the PSR-proposal), without altering the definition of ‘authorisation’. LV (MS comments): The consumer may be unaware of the fraudster's involvement, which cannot be detected during the process, given the methods used by fraudsters, which psychologically and technologically affect the consumer's ability to make an appropriate decision. Consequently, this offer may not work in practice. How and at what point does the payment service provider identify the fraudster, how long does it take? In any case, if there are SCA notificiations, the responsibility lies with the payer. An exception could be in the case of smishing, where card data attached to a digital wallet without SCA is stolen, resulting in the customer being unable to trace the payment. LU (MS comments): Such transaction should be considered as authorized, we have difficulties to identify the grounds for a dispute as long as the PSU gave consent to the transaction and was not manipulated. LT (MS comments):

	We opt for the second alternative – cases where the payer consented to a payment transaction but was misled about the purpose should be regarded as 'authorised push payments. Reimbursement of such fraudulent payment transactions should require a different set of rules. IT (MS comments): **IT.** The transaction should be treated as "authorised": the PSU was not manipulated a therefore the consent is genuine. HR (MS comments): We do not support this approach. FI (MS comments): FI: Mainly yes. If the payer has given their consent as regards the amount and the payee, the transaction should generally be deemed authorised. However, exceptions to this could exist. DK (MS comments): Yes, we agree that such a transaction should be deemed as authorised. It could also be considered to include "purpose" here along with amount and payee to ensure that also romance and investment fraud would be covered. DE (MS comments): No, DE firmly **opposes the inclusion of any subjective elements** in the context of user authorisation (Art. 49), as this would **significantly impact PSPs' liability**. Deceptions and manipulations that affect the PSU's decision-making are outside the immediate sphere of responsibility of the PSP. Holding the PSP liable in cases of flawed decision-making, nonetheless, would present a significant shift in principle. We consider this approach immensely unbalanced and risky, most probably leading to increased consumer prices that would burden all consumers. Besides, it could also lead to an increase in moral hazard and, thus, even facilitate the successful execution of fraud.

	This is particularly relevant given that, under the current COM proposal, the burden of proof for authorization (=consent) would shift to the PSP. We oppose this due to the apparent difficulties PSPs would face in proving circumstances beyond their control. If the concept of authorization were further burdened with subjective criteria, it would effectively lead to an **almost unavoidable liability for PSPs** in cases of fraud, making them **liable in all cases where a PSU denies having authorised a transaction**. CZ (MS comments): This payment transaction should be treated as **authorised.** For us, important is that the consent was given by the payer in agreed form and procedure. CY (MS comments): Such a payment transaction should be treated as “authorised”.

3. where the payer gave consent in the form and following the procedure agreed with its PSP, provided that the payer's consent was given in full awareness of all relevant circumstances (including amount, payee, and purpose of the transaction)	AT (MS comments): This case should be treated as authorised. ES (MS comments): Authorized. SK (MS comments): We do not support such a broad definition, could create confusion through unintended consequences. SI (MS comments): We do not support this option. RO (MS comments): No PT (MS comments): We reject any subjective requirements namely to evaluate awareness of all relevant circumstances, which would be difficult or completly dependent of subjective evaluations, that cannot be done by PSPs. NL (MS comments): This should be treated as "authorised". In case the question is whether this should be the definition of authorised, then 'no' as we do not support the inclusion of the subjective element that the payer was in full awareness of all relevant circumstances. LV

	(MS comments): This is probably supportable as an authorised transaction. LU (MS comments): Such transaction should be considered as authorized. IT (MS comments): **IT.** The transaction should be treated as "authorised". We point out that, in our view, any mistake regarding the "*purpose of the transaction*" (*i.e.* the "*underlying reason*" of the transaction) should be irrelevant. A fraud concerning the purpose of the transaction would be an APP fraud, which we believe should not lead to the liability of the PSP under the PSR. HR (MS comments): We do not support this approach. FI (MS comments): FI: Yes. If the payer has given their consent in full awareness of all relevant circumstances (including amount, payee, and purpose of the transaction), the transaction should be deemed authorised. DK (MS comments): It could be considered to include the purpose in the text above along with the amount and payee to ensure that also romance and investment fraud would be covered. However, the way it is written here in option 3 would seem to go too far considering that there could be more relevant circumstances than just the three listed here since the word "including" is used (which

	indicates that more circumstances could be relevant) instead of "as regards" (which would indicate that it should be limited to the circumstances mentioned). It also seems to go too far with the mention of full awareness. It would probably never be possible to have full awareness of all relevant circumstances (e.g. the PSP should not be liable if the PSU is sold a product under the impression that it was made with better quality of materials than it actually was. If the PSU has been seriously misled in this regard it could be reported to the police but it should not be the responsibility of the PSP). DE (MS comments): No, DE firmly **opposes the inclusion of any subjective elements** in the context of user authorisation (Art. 49), as this would **significantly impact PSPs' liability**. The discussions surrounding the liability regime focus on the handling of fraud cases. However, the proposal does not establish this nexus. Instead, it broadly refers to impaired consent that was given without full awareness of the relevant circumstances. Whether this lack of awareness stems from deception or, for example, simply from the PSU's inattentiveness when initiating the payment transaction no longer matters. Such an expansion goes entirely beyond the scope of the current discussions in the Council and is completely unwarranted for. CZ (MS comments): This payment transaction should be treated as **authorised.** However, the state of mind of the payee is not a decisive point for us. CY (MS comments): Such a payment transaction should be treated as "authorised".

Which of the specific cases of payment transactions below should be treated in PSR as "unauthorised"?	LU (MS comments): It is of utmost importance to create a sound legal framework that provides PSPs with the legal clarity and certainty on whether a transaction is to be considered as authorized or not. PSPs do not have the means to identify a transaction that was duly authorised by the PSU with its own credentials and from its own device as manipulated through social engineering. Only an enhanced vigilance from the PSUs can redeem this type of fraud; any other measures would rather increase fraud as users would become less vigilant and as they know that they would be reimbursed. IE (MS comments): Social engineering techniques are lies and deceptions. From our reading, options 1-3 are not distinct enough to be seen as separate cases. They are all examples of fraud executed through social engineering techniques. HR (MS comments): We do not support any of the suggested examples/cases as none of the cases where SCA was applied can a priori be considered an unauthorised transaction. In this context, gross negligence and prevention measures play a key role. It is necessary to emphasize the importance of fraud prevention and, in this sense, to strengthen the transaction monitoring mechanisms and the role of the ECSPs.

1. where the payer was manipulated into giving consent or initiating the payment transaction in favour of a third party impersonating the intended payee, regardless of the means of manipulation used, e.g. regardless of whether it used social engineering techniques or simple lies/deception	AT (MS comments): This case should be treated as authorised. ES (MS comments): Not authorized. Although we do consider that means of manipulation could be taken into consideration in terms of liability, these operations should be deemed not authorized. SK (MS comments): Do not support. SI (MS comments): We do not support this option. RO (MS comments): We are in favour of this option but, this should not be without taking into consideration the gross negligence of the PSU, since the payment should be treated as unauthorised only in complex fraud scenarios as social engineering. A different approach might ultimately result in a PSU moral hazard. PT (MS comments): If the payer initiated and authenticated the transaction following the procedure agreed with its PSP, it should be classified as authorised. Manipulation shall not play a part as a requirement to evaluate authorisation of transactions. NL (MS comments): This should not be treated as unauthorised. Instead, when a payer is manipulated into authorizing a transaction, an exception to the generally applicably liability scheme should be made for certain types of fraud (in any case

	bank help desk fraud). As in the Commision's proposal, liability arises in cases of a 'fraudulent authorised payment transaction'. Although it is fraudulent, it still is authorised (see article 59 PSR-proposal). In this cases, the payer should be reimbursed by the PSP. LV (MS comments): This should be treated as "unauthorised" transaction, provided that it was not possible to identify. LU (MS comments): No, such transaction cannot be considered as unauthorised; the PSU must remain vigilant and must be aware of the consequences of its actions when making a payment. Fraud elements such as social engineering techniques or lies/ deceptions are beyond the control of PSPs. IT (MS comments): **IT.** In principle, the transaction should be considered as unauthorized, because the PSU was mistaken about one of the identifying element of the payment transaction. However, we point out that in the case of credit transfers, by legislative choice (art. 88 PSD2; art. 57 PSR), only the IBAN, and not the name entered by the PSU, is relevant to identify the payee. Therefore, when the transaction is executed towards the IBAN entered by the PSU, then the PSU's consent covers all *legally relevant* information for the execution, hence the transaction should be regarded as "authorised" for PSD2/PSR purposes. Nevertheless, the IBAN check should help the PSU to become aware of the mismatching and consequently of the potential fraud. At any rate, in our opinion, the means of manipulation used are irrelevant to determine if the transaction is authorized or not (what matters is their effect on the PSU: see our first answer). The different means of manipulation can be relevant to assess "gross negligence". FI

	(MS comments): FI: Mainly yes. However, the way the payer was manipulated (i.e., e.g., the innovativeness and complexity of the fraud) should be taken into account when assessing the payer's (possible gross) negligence. In case the means of manipulation will be further distinguished, and this would be the decisive factor for whether a transaction will be deemed authorised or unauthorised, we note that the expression "social engineering" is not accurate enough for this. DK (MS comments): This should be considered as unauthorised. DE (MS comments): No, **manipulated** transactions should be treated as **authorised** as long as the PSU **knows** that a payment transaction will take place and gives consent to that. **This applies regardless of the way in which a manipulation takes place.** The decisive factor is whether the **PSU initiates** the payment transaction himself/herself (authorised) or whether a third party obtains certain data and then initiates the payment transaction (unauthorised). If the PSU is **mistaken** about the **payee** due to an impersonation fraud, this is merely an error about the underlying reasons for a payment transaction which **does not nullify the declaration of consent.** Deceptions and manipulations that affect the PSU's decision-making are outside the immediate sphere of responsibility of the PSP. Holding the PSP liable in such cases of flawed decision-making, nonetheless, would present a significant shift in principle. However, DE supports regulating impersonation fraud in a limited way as done in Art. 59 as regards bank employee impersonation fraud, since in those cases a certain responsibility of the PSP can be assumed. In this context, we would even go further and suggest broadening the scope to fake websites and apps assigned to the PSP that are used by fraudsters in order to take new forms of digital fraud into account. Apart from the cases regulated in Art. 59, we do **not** see the **need** to extend the PSPs liability to all impersonation frauds, including where social engineering techniques are used. The new **IBAN name check** will address misconceptions about the recipients and therefore also tackle patterns of impersonation fraud. The effects of the new IBAN name check should be awaited and assessed first. CZ

	(MS comments): This payment transaction should be treated as **authorised.** For us, it is important that the consent is given by the payer in the agreed form and procedure. The crucial issue is who is giving the consent; if it is the payer, the transaction is authorized. CY (MS comments): Such a payment transaction should not be treated as "unauthorised". Should the payment service provider have reasonable grounds to suspect that the payer acted fraudulently, the payment service provider may treat such payment transaction as authorised.

2. 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	AT (MS comments): This case should be treated as authorised. ES (MS comments): Not authorized. SK (MS comments): Do not support. SI (MS comments): We could support this option (BE PRE proposal - option C). We believe that this problem will be partially covered by IBAN check (Art. 50), that specifically address misconceptions about the recipients. Beyond that, we suggest limiting it to bank employee impersonation fraud, as this will increase the trust of payment service users in the system. RO (MS comments): We support this approach, as it will help decrease the number of frauds and does not limit fraud scenarios only to impersonation fraud. Moreover, it incentivises the PSP to invest and develop more efficient transaction monitoring mechanisms. PT (MS comments): If the payer initiated and authenticated the transaction following the procedure agreed with its PSP, it should be classified as authorised. Manipulation shall not play a part as a requirement to evaluate authorisation of transactions. Other social engineering based frauds could be envisioned to be included in article 59, on the basis of an impact assessment. NL

	(MS comments): See reply to 1. LV (MS comments): This is probably supportable as an authorised transaction, if there have been SCA notifications and the customer has been able to identify the payee. LU (MS comments): No, such transaction cannot be considered as unauthorised; the PSU must remain vigilant and must be aware of the consequences of its actions when making a payment. The new IBAN name check provisions could however become an effective prevention method. IT (MS comments): **IT.** See answer above. FI (MS comments): FI: Mainly yes. DK (MS comments): This should be considered as unauthorised. DE (MS comments): No, **manipulated** transaction should be treated as **authorised** as long as the PSU **knows** that a payment transaction will take place and gives consent to that. This applies **regardless** of the way in which a manipulation takes place, i.e. **irrespective** of whether **social engineering** was used. The decisive factor is whether the **PSU initiates** the payment transaction himself/herself (authorised) or whether a third party obtains certain data and then initiates the payment transaction (unauthorised). If the PSU is mistaken about the payee due to an impersonation fraud, this is merely an error about the underlying reasons for a payment transaction which **does**

	not nullify the declaration of consent. Deceptions and manipulations that affect the PSU's decision-making are outside the immediate sphere of responsibility of the PSP. Holding the PSP liable in such cases of flawed decision-making, nonetheless, would present a significant shift in principle. However, DE supports regulating impersonation fraud in a limited way as done in Art. 59 as regards bank employee impersonation fraud, since in those cases a certain responsibility of the PSP can be assumed. In this context, we would even go further and suggest broadening the scope to fake websites and apps assigned to the PSP that are used by fraudsters in order to take new forms of digital fraud into account. Apart from the cases regulated in Art. 59, we do **not** see the **need** to extend the PSPs liability to all impersonation frauds, including where social engineering techniques are used. The new **IBAN name check** will address misconceptions about the recipients and therefore also tackle patterns of impersonation fraud. The effects of the new IBAN name check should be awaited and assessed first. Finally, a **clear definition of social engineering techniques** is missing. The term could lead to delineation problems and legal uncertainty. We also wonder, if in the future the majority of frauds will be committed via social engineering, rendering the restriction meaningless. CZ (MS comments): This payment transaction should be treated as **authorised.** The crucial issue is who is giving the consent; in case it is the payer, the transaction is authorized. CY (MS comments): Such a payment transaction should be treated as "unauthorised".

3. same as in point 2 above, but limited to *consumers* falling victim of impersonation fraud using social engineering	AT (MS comments): This case should be treated as authorised. ES (MS comments): Not authorized, although we would not limit it to consumers. In line with article 2 of the Draft Law for the creation of the Independent Administrative Authority for the Defense of Financial Customers for the extrajudicial resolution of conflicts between financial entities and their customers, approved by the Council of Ministers and submitted to the Spanish Parliament for legislative processing, we favour the inclusion of businesses that fall under the definition of SMEs according to Annex I of Commission Regulation (EU) No 651/2014 of 17 June 2014. SK (MS comments): Do not support. SI (MS comments): We would not limit it to consumers only, as we have also identified the issue with small entrepreneurs. Although they are subject to a higher standard of care, they can still be victims of fraud. RO (MS comments): In our opinion the approach should be similar as in point 2 above and the payment should be treated as unauthorised. PT (MS comments): If the payer initiated and authenticated the transaction following the procedure agreed with its PSP, it should be classified as authorised. Manipulation shall not play a part as a requirement to evaluate authorisation of

	transactions. Other social engineering based frauds could be envisioned to be included in article 59, on the basis of an impact assessment. NL (MS comments): See reply to 1. LV (MS comments): This is seemingly no different from what is described in point 1. LU (MS comments): Idem 2 IT (MS comments): **IT.** In our opinion, the distinction between consumers/non-consumers should not be relevant. We remind that art. 27 PSR already provides that the PSP and the PSU who is not a consumer may agree that art. 55 ("*Evidence on authorisation and execution of payment transactions*") and art. 60 ("*Payer's liability for unauthorised payment transactions*") do not apply in whole or in part. FI (MS comments): FI: Although consumers are a group that should be especially protected, we would not, at least at this stage, consider the identity of the payer to be the decisive factor in determining whether a transaction is authorised or unauthorised. DK (MS comments): But is this not already the case cf. article 27(1) which reference that it can just be agreed between the PSP and the PSU (when the PSU is not a consumer or a microenterprise) that article 55 and 60 do not apply fully or in part? But yes, we can support that it only applies to consumers and microenterprises.

	CZ (MS comments): This payment transaction should be treated as **authorised**. CY (MS comments): Such a payment transaction should be treated as “unauthorised”.

4. where the transaction was initiated by a third party using the personal security credentials of the PSU fraudulently obtained, regardless of whether SCA was applied	AT (MS comments): This case should be treated as **un**authorised. ES (MS comments): Not authorized. However, we consider that the liability regime could differ in certain cases. SK (MS comments): We can support, should be applied without prejudice to the gross negligence. SI (MS comments): In our opinion, such a payment transaction is unauthorized, as the PSU did not give consent for its execution, being unaware that they were initiating such a transaction. If there is no awareness of issuing a declaration of intent to initiate a payment transaction, it cannot, in our view, be regarded as consent. We believe that this interpretation is already possible under the PSD2. RO (MS comments): We support this approach in this case, as it will help decrease the number of frauds and, in our opinion, this will incentivises the PSP to develop more efficient transaction monitoring mechanisms. PT (MS comments): We consider the transactions regarding this scenario as **unauthorised, because transactions to be considered authorised need to be initiated by the PSU.** NL (MS comments): Yes, this should be treated as unauthorised, as the payment was done by a third party.

	LV (MS comments): This is probably supportable as an authorised transaction only if there have been SCA notifications and the customer has been able to identify the payee. Otherwise it is considered unauthorised. LU (MS comments): In such case we could consider some flexibility, as long as the transaction was not performed by the PSU itself, except in cases of gross negligence or criminal behaviour of the PSU. When a transaction is duly authorized by the PSU using the appropriate credentials and its own device, the PSP has no reasonable grounds for suspicion. However, in cases where the user's credentials are obtained fraudulently and then subsequently used, the PSP might raise suspicion as the different devices or different IP addresses will be used for the transaction. In such cases, fraud can be detected and prevented by alerting the PSU about the use of a different device or a suspicious transaction. LT (MS comments): We opt for this alternative. However, with some amendments: "where the transaction was initiated and/or authenticated/the consent was given by a third party using the personal security credentials of the PSU fraudulently obtained, regardless of whether SCA was applied". Unauthorised (fraudulent) payment transactions can take place when the fraudster interrupts the procedure of initiating a payment transaction and/or authenticates it on the name of the payer – this interruption by the fraudster to manipulate the payer to falsely get its consent to a payment transaction can happen in any stage, not only in the initiation stage. IT (MS comments): **IT.** The transaction is unauthorised, because the PSU did not give its consent to it. How the credentials were obtained by the third party can be relevant to assess the PSU's gross negligence.

	(For completeness' sake: the transaction is also unauthorised if the payment order transmitted to the PSP differs from the one entered by the PSU, due to interference by the fraudster, such as through a fake website or a man-in-the-middle/browser attack). IE (MS comments): This represents a more distinct example: if SCA was not applied, the payment should not be considered as authorised. We would argue that if SCA was applied but the credentials were stolen that the payment should also not be considered as authorised. FI (MS comments): FI: Yes. DK (MS comments): This should be considered as unauthorised. DE (MS comments): This case should be treated as **unauthorised**. As explained above, the decisive factor is whether the PSU initiates the payment transaction himself/herself (authorised) or whether a third party obtains certain data and then this third party initiates the payment transaction (unauthorised). CZ (MS comments): This payment transaction should be treated as **unauthorised**. In this scenario it is not the payer giving consent. CY (MS comments):

	Such a payment transaction should be treated as “unauthorised”. Furthermore, if the personal security credentials of the payment service user were fraudulently obtained and as a result the payment instrument was recreated and SCA was not applied by the payment service provider of the payment service user, then such a payment transaction should also be treated as ‘’unauthorised”. BG (MS comments): We believe that this scenario depicts an unauthorised payment transaction as the use of personal security credentials of the payment service user, that are fraudulently obtained, should be accounted for when judging whether a transaction is authorised or not.

Allocation of liability	

Who should bear liability for authorised transactions?	AT (MS comments): The PSP should be liable in the case of an unauthorised payment transaction only. Furthermore, we do not see the need to extend the PSP's liability to all impersonation frauds, including where social engineering techniques are used. The new IBAN name check will address misconceptions about the recipients and therefore also tackle patterns of impersonation fraud. The effects of the new IBAN name check should be awaited and assessed first. ES (MS comments): If the order is considered authorized by the PSU, it should not be considered that fraud has occurred, so the PSP should not assume losses. SK (MS comments): Without prejudice to the exceptions it should be PSU. SI (MS comments): If the transaction is authorized, the responsibility lies with the PSU. However, an important question here is when a transaction is considered authorized – see above. SE (MS comments): With a sufficiently wide definition of unauthorised transactions, there should be no issue of liability for authorised transactions. RO (MS comments): In our opinion, the PSU should bear the liability for authorised transactions, but only taking in consideration the specific cases where a transaction should be considered authorised, i.e. excluding the complex fraud scenarios (e.g. spoofing, social engineering etc.).

	PT (MS comments): For authorised transactions, the principle remains that PSUs bear liability, but with a liability shift in certain cases, incl. for (authorised) bank-employee impersonation fraud (except where the consumer acted fraudulently or with gross negligence). For unauthorised transaction, same as in PSD2. This is same as saying that*, unless there is a disposition setting the liability of the PSP of the payer for specific types of authorised payment transactions (e.g. impersonation fraud),* we consider that PSPs should be liable only in cases of unauthorised payment transactions. NL (MS comments): In principle, PSUs should bear liability. LV (MS comments): Payers PSP, payees PSP, ECPSs that are liable for Processes that are the competence of each entity involved, i.e. the responsibility should lie with the person who refused or failed to provide authorisation for the customer's convenience, for example if there was no notification of the amount and beneficiary of the transaction. If the PSP of the payer has evidence of deliberate actions by the customer in the payment process, then the payer should also be held liable. LU (MS comments): Authorized transactions that are correctly performed by the PSP should not trigger any liability. LT (MS comments): We are of the view that, in general, PSUs should bear the losses for fraudulent authorised payment transactions. IT (MS comments):

	IT. Considering the distinction between authorised and unauthorised operations outlined above, there is no liability to speak of. The economic consequences of the transaction remain on the PSU. IE (MS comments): We could support assigning liability to PSPs for social engineering fraud where there are elements to this type of fraud that the PSP can control or impact and, therefore, steps that the PSP can take to combat the fraudster. HR (MS comments): Payment service users FI (MS comments): FI: In case authorised and unauthorised transactions will be clearly distinguished, the PSU should, as a general rule, bear the liability for authorised transactions. The same principle should, as a starting point, apply in case there would be a third group of transactions called “authenticated but unauthorised”. However, the abovementioned should not apply in case a group of transactions called “authorised but with a right to a refund” would be established. DK (MS comments): If a transaction is authorised the PSP would not be liable. DE (MS comments): PSU CZ (MS comments): In case the transaction is authorised and correctly executed (in line with the unique identifier) there is no liability issue. It is already set in PSD2. E.g. if the payment transaction is not correctly executed, the liable party is PSP. If

	the payment transaction is correctly executed on the side of PSP, but PSU e.g. provided incorrect unique identifier, the PSU bears the cost. However, is the question correct? CY (MS comments): The liability for authorised transactions should be borne by the payment service provider of the payer and of the payment service provider of the payee, depending on the specific circumstances under which the payment transaction was authorised, unless the payer acted fraudulently or with gross negligence. BG (MS comments): We believe that the payer should bear the responsibility for authorised payment transactions, provided that the personal security credentials, used to authorise the transaction, were not fraudulently obtained.

Do you envisage exceptions from the rule in the previous question? If yes, which exceptions?	AT (MS comments): Yes, if the PSP does not block a transaction despite reasonable grounds for suspecting fraud (see below). ES (MS comments): We propose to maintain the exceptions considered in article 89 of PSD2 (PSP liability for non-execution, defective or late execution of payment transactions). SK (MS comments): In a view of compromise we can live with Article 59 regarding bank-employee impersonation fraud, however we do not support any extensions of the scope as it could negligence on side of the PSUs which could lead to unintended client categorization and de-risking of PSPs. SI (MS comments): Bank employee impersonation fraud can be an exception. SE (MS comments): Exceptions add complexity. We would prefer a sufficiently wide definition of unauthorised transactions, covering most types of fraud. This would mean that there is no need for specific exceptions. RO (MS comments): Exceptions should apply whenever the particular (fraudulent) payment did not benefit from proper security measures (e.g. 2FA, transaction monitoring mechanism, payee verification etc.). In these cases, the PSP should bear the liability. PT (MS comments):

	As we mentioned before, the case where occurs an authorised bank-employee impersonation fraud (except where the consumer acted fraudulently or with gross negligence). In this situation, the PSP will be liable. Additionally, we envision a shift of liability from the PSU to the PSP in the case where the PSP grossly fails to apply the provisions and requirements regarding the transaction monitoring mechanism as foreseen in Article 83(2) of the proposed PSR, in particular by failing to detect and prevent fraud by not taking into account elements of data that could be instrumental to prevent fraudulent transactions. NL (MS comments): Yes, in the following situations: - Bank-impersonation fraud, through spoofing or through other means. - For other types of fraud of which it could be reasonably expected from the PSP that it would technically prevent the fraud (or at least warn PSU specifically therefore). - In case the PSP did not fulfil its obligations under Article 83 or 83a, insofar as these provisions are relevant for the forms of fraud covered by Article 59. LV (MS comments): Payees PSP, where the evidence at its disposal shows that the transaction was authorised properly and that there is no risk of fraud, i.e. the responsibility should lie with the person who refused or failed to provide authorisation for the customer's convenience, for example if there was no notification of the amount and beneficiary of the transaction. LU (MS comments): No LT (MS comments): However, although we believe it is also important to delineate APP fraud type transactions separately from unauthorised payment transactions, for the most part we would support those proposed by the Presidency in

	option D. Having said that, we would be in favour of reimbursing PSUs their losses for APP type payment transactions. IT (MS comments): **IT.** No, we don't. (Certain cases of authorised transactions may be refunded if the IBAN check was not properly carried out; but this kind of liability is based on different grounds than that those set out in art. 56 PSR). HR (MS comments): Yes, but only in the case of bank impersonation fraud. FI (MS comments): FI: Yes. The PSU should not bear any financial losses: 1) if the payer's PSP fails to require SCA; 2) after the PSU has notified its PSU of loss, theft, misappropriation or unauthorised use of a payment instrument; 3) if the PSP does not provide appropriate means for such notification at all times. The exceptions should not apply where the PSU has acted fraudulently. We further point out that Article 60(1), fourth subparagraph should be amended to mention also *dispute resolution bodies* (courts and ADR bodies) as entities with the power to reduce the payer's liability. DK (MS comments): No, not if a transaction is authorised. We believe that if a transaction has been authenticated but through the use of manipulation of the PSU, then the transaction should never be considered as authorised in the first place. It would just complicate the regulation further if PSPs could be liable for authorised transactions. All cases that could include liability for PSPs should be included in the definition of unauthorised payments. We would, however, suggest dividing unauthorised payments into two distinct categories: 1) Unauthorised but authenticated, and 2) Unauthorised and unauthenticated.

	This would make it easier to make distinctions between different kinds of unauthorised payments when it comes to caps on liability, claim excess etc., and at the same time ensure that the authorised category is only for actual, legitimate payments. DE (MS comments): Yes, DE **supports** regulating **impersonation fraud in a limited way** as done in Art. 59 as regards **bank employee impersonation fraud**. In this context, we would even go further and suggest **broadening the scope** to fake websites and apps assigned to the PSPs that are used by fraudsters in order to take new forms of digital fraud into account. CZ (MS comments): Probably the first questions should be “who should bear liability for **unauthorised** transactions”? CY (MS comments): Exceptions from the rule in the previous question shall apply when the payer acted fraudulently or with gross negligence. BG (MS comments): We believe that there should be no exceptions to the rule above.

Do you support Article 59 of the COM's proposal which introduces a refund right for consumers where they fall victim of bank-employee impersonation fraud via 'spoofing'?	AT (MS comments): No. ES (MS comments): Yes, since it incentivises banks to adopt preventive fraud measures. However, we would favour the inclusion of a broader range of operations that would need to covered, in line with previous answers (manipulation could arise from other cases beyond bank impersonation). Depending on drafting needs, it is possible that article 59 becomes redundant when all manipulation cases are considered. SK (MS comments): We see some merit in the proposal, banks are in the position to enhance the security of their communications to limit possibilities of bank-employee impersonation fraud. We deem it right to make banks liable for this type of fraud. It could incentivise banks to take new innovative measures minimising the risks of such frauds. SI (MS comments): Yes. SE (MS comments): We support the idea, but strongly prefer that such fraud cases are treated as unauthorised. RO (MS comments): Regarding Article 59 of the PSR we see merits in extending the cases of impersonation to all cases where a consumer was manipulated by a third party pretending to be an employee of the consumer's PSP "or any other relevant entity of a public or private nature, as proposed in option E. PT (MS comments):

	Yes, we support the provisions foreseen in Article 59 as proposed by the COM. We would like to highlight that the intended scope of this article is a subset of authorised transactions that shall be treated differently. If notions of intent are included in the evaluation to decide if a transaction shall be classified as authorised/unauthorised, this Article would be irrelevant. NL (MS comments): Yes. LV (MS comments): We support with a comment, if not limited to the bank, but applying a broader approach - any "fake" third party, police supervisory authorities, etc. LU (MS comments): No, we do not support this approach; the most appropriate manner to address and reduce fraud is by incentivizing the PSU to act in a responsible manner and through targeted awareness raising. It is important to address the problems by its roots. Thus, we would support following mitigation and prevention measures: • an extension to all credit transfers of IBAN/name matching verification services. These have been proposed by the Commission for instant payments in Euro. All consumers should benefit from them, for both regular and instant credit transfers; • A legal basis for PSPs to share fraud-related information between themselves in full respect of GDPR (via dedicated IT platforms); • The strengthening of transaction monitoring; • An obligation by PSPs to carry out education actions to increase awareness of payments fraud among their customers and staff; • Enhanced SCA application. Any regime that will overburden the liability of PSPs with some “default liability” combined with elements taken from the subjective theory like “intend” together with a loose approach to the concept of “gross negligence” will lead to undesired consequences in terms of fraud prevention (opposite incentives from

	PSUs) or financial inclusion (high probability of de-risking of clients by PSPs that do not have digitally responsible behaviour either intentionally or not). LT (MS comments): We believe that excluding only one certain type of APP/impersonation fraud as worthy of reimbursement would not be fair to PSUs who suffer from similar type of impersonation fraud. Although we agree that banks have more possibilities to protect their name and their own fraud protection processes, however, the same principals should apply to reimbursement of all type of APP frauds (if any). At the same time, PSPs should make every effort to organize their fraud preventions systems and processes in a way that equally protect their PSUs from all type of fraud. IT (MS comments): **IT.** In our opinion, art. 59, as proposed by the COM, blurs the distinction between authorised and unauthorised operations outlined above, as evidenced by the term "*fraudulent authorised payment transactions*" used therein. In our opinion, if the distinction outlined above is accepted, the transactions referred to in the proposed art. 59 would be either: (i) "unauthorised transactions" covered by the general rule; or (ii) APP fraud, which – in our view – should not be refundable under the PSR. Regarding the need to find a balanced approach that involves the cooperation of all actors in the payment chain (ECSPs included), please, see the following answer. IE (MS comments): Yes HR (MS comments): Yes

	FI (MS comments): FI: Yes. DK (MS comments): Yes, however, we believe it should be extended to cover more cases. DE (MS comments): Yes. In this context, we would even go further and suggest **broadening the scope** to fake websites and apps assigned to the PSP that are used by fraudsters in order to take new forms of digital fraud into account. CZ (MS comments): No. This provision should be deleted. However, the added value of EC proposal is in gross negligence corrective which is missing in Art. 49(2) PSR of BE PRES proposal. CY (MS comments): We are supportive of Article 59 of the COM's proposal, which introduces a refund right for consumers where they fall victim of bank-employee impersonation fraud via 'spoofing'. BG (MS comments): We agree with the COM's proposal outlined in Article 59.

Would you support that refund rights extend to other types of impersonation fraud as well?	AT (MS comments): No. ES (MS comments): Yes, in line with our previous answer. SK (MS comments): We see it difficult to define what types of impersonation fraud could occur in the future, in some cases banks capacity to limit such fraud might be non-existent, thus making it not right to extent the refund right universally on other types of impersonation fraud. We should wait for the effect of the IBAN check on the fraud prevention. SI (MS comments): Considering that a PSP can only influence the security of its services and its public image, it does not seem reasonable to include other forms (e.g., misuse of contact information of government authorities). For other types of impersonation fraud, we do not see a direct responsibility of PSPs and would suggest limiting it to bank employee impersonation fraud. SE (MS comments): We think that such fraud cases should be treated as unauthorised. RO (MS comments): We support the extensions of refund rights to all cases where a consumer was manipulated by a third party pretending to be an employee of the consumer's PSP "or any other relevant entity of a public or private nature. PT (MS comments):

	On the basis of an impact assessment, we would be open to explore the possibility of including other types of social engineering based frauds in article 59. NL (MS comments): We would support this for all ways through which bank-impersonation fraud occurs. For other types of fraud, we would support reimbursement if it could reasonably be expected from the PSP to prevent the fraud from occurring or to at least warn the PSU for the specific occurrence of fraud in question. LV (MS comments): We would certainly support a broader scope. LU (MS comments): No, such extension is not necessary. LT (MS comments): Yes, provided, additional conditions (e.g. listed in option D) are introduced. IT (MS comments): **IT.** Following the distinction between authorised and unauthorised transactions outlined above, any impersonation fraud could lead to a refund right (barring gross negligence) if it means that the PSU has unwittingly authorized a transaction, he/she didn't wish to authorize (see our first answer). On the other hand, if art. 59, *as proposed by the COM*, were to be extended to types of impersonation other than that of a bank employee, it would cover virtually all possible APP fraud (e.g. romance fraud, fake investment fraud, emergency scam, etc.); a result we would not agree with. HR (MS comments):

	No FI (MS comments): FI: Yes. However, in order for this to be justifiable, the PSPs should be given adequate tools for fraud prevention (e.g., refusing to execute suspicious transactions, delaying making funds available/freezing of received funds, fraud data sharing) explicitly in the PSR and regardless of provisions in other EU legislation (such as the IPR). DK (MS comments): Yes. DE (MS comments): No. We do **not** see the **need** to extend the PSPs' liability to all impersonation frauds (beyond Art. 59), including where social engineering techniques are used. The new **IBAN name check** will address misconceptions about the recipients and therefore also tackle patterns of impersonation fraud. The effects of the new IBAN name check should be awaited and assessed first. CZ (MS comments): No. CY (MS comments): We are supportive of the extension of refund rights to other types of impersonation fraud.

Option D in the Presidency note lists some possible safeguards that could be introduced if cases of impersonation fraud using social engineering were be treated as unauthorised transactions. What is your position on such possible safeguards: 1. a cap on the PSP's liability for the impersonation fraud	AT (MS comments): Yes. ES (MS comments): As indicated above; cases of social engineering fraud should not be considered authorized. Regarding quantity caps, we would like to highlight the risk of the upper limit of the cap becoming a benchmark for reimbursements, thus reducing the thoroughness of case-by-case analyses. Therefore, we would favour the design of caps expressed as a percentage of the fraud, and PSP responsibility linked to certain factors. For instance, this percentage could be reduced if the customer has recurrently suffered the same type of fraud. SK (MS comments): If the bank is liable, we do not see a justification for capping the bank liability. SI (MS comments): We support the cap on the PSP's liability. SE (MS comments): The purpose of the safeguards is to balance the burden of liability to the PSPs advantage. **We cannot discuss the safeguards independently of the definition of unauthorised transactions.** We do not see a need for a compensation cap that would weaken consumer protection, especially as it would be difficult to calibrate in a relevant way. RO

	(MS comments): We don't see merit in imposing a cap on the PSP's liability for the impersonation fraud. PT (MS comments): Previous point: We are against considering such transactions as unauthorised. Regarding the possible safeguards: Although we understand the rational underlying this possible safeguard (balancing the position of the parties, not leaving the PSPs completely at the mercy of situations in which they have no control), if these situations are classified as unauthorised transactions, we do not see reasons to establish different rules to their reimbursement, since we understand that such caps could be deterrent of the implementation of mitigation measures by the PSP. Even in the case these situations are classified as authorised transactions, we believe that the cases of social engineering laid down in article 59 should have a consistent approach with the approach followed for unauthorised transactions (in particular regarding PSP liability with PSU liability in case of gross negligence). NL (MS comments): We do not support the introduction of a cap on the PSP's liability for the impersonation fraud. In the Netherlands banks currently reimburse victims of bank-impersonation fraud under certain conditions, but there is no cap installed. As a result, banks have improved their transaction monitoring systems and have taken other measures to prevent this type of fraud from happening. Transactions with very high amounts are generally noticed by the transaction monitoring system and are less frequent nowadays. Including a cap might reduce the incentive for PSPs to take preventive measures. LV (MS comments): We support inclusion of a cap, however, this should allow the MS to define the criteria to be taken into account. LU

	(MS comments): We are open to discuss the options described in option D and the appropriate method to frame these measures. However, it must remain clear that PSPs should not bear the whole liability for fraudulent transactions. We can support the cap on the PSP's liability for impersonalisation fraud LT (MS comments): We support – it might balance the burden of liability. IT (MS comments): **IT.** We do not agree to introduce a cap on the PSP's liability, *if* the liability of the PSP is not extended beyond "unauthorised transaction" (with the *caveats* outlined above). A hard cap could be considered more appropriate, for example, in the context of the UK liability regime for APP fraud, where it might well be seen as a counterbalance for the (virtually unlimited) scope of the PSP's liability. IE (MS comments): We can see the use in exploring the systemic benefits of financial caps but it needs further exploration and would need to be carefully calibrated, particularly to ensure that it is not detrimental to the PSU. HR (MS comments): We do not agree that cases of impersonation fraud using social engineering should be treated as unauthorised transactions.

	We do not support the proposal to introduce caps on the PSP's liability. FI (MS comments): FI: Preliminarily, we remain hesitant to introduce caps. However, if introduced, they should, at a minimum, be at an appropriate level taking into account the national specificities of different MSs. DK (MS comments): We can support a cap if it would be possible to set nationally. This would also cater for MS who might be a bit more sceptical towards extending the liability for PSPs to cases of impersonation fraud since they could set a lower cap if that is what they would prefer. However, we would not support a more general cap (e.g. if a payment has not been authenticated even though it should have been, or if the PSP fails to notify the PSU of discrepancies in the IBAN-name check – then the PSP should be fully liable). DE (MS comments): As already laid out, we oppose shifting the liability for fraud cases towards the PSP. **Manipulated transactions** should be treated as **authorised** (see above). CZ (MS comments):

	Acceptable (only in case that Article 59 or similar provision maintains); however, it is connected with many disadvantages – e.g. risk of increase in frauds in limit if PSU will be reimbursed automatically. CY (MS comments): We are supportive of a cap, at a level to be agreed among the member states, which should be made known to consumers. In this way, consumers would know in advance that any payments over the cap would not be covered, therefore it would make consumers more cautious before making payments in excess of the cap. BG (MS comments): We would like to reiterate that we support the existing liability regime that provides balanced and fair approach to the refund of fraudulent payment transactions. Introduction of new complex rules with exceptions, caps, sharing or shift in liability etc. would be difficult and costly to implement and administer by the PSPs (especially in cross-border aspect), challenging to supervise, and would not succeed to foster consumer protection.

2. possibility for the payer's PSP to apply a claim excess	AT (MS comments): No. ES (MS comments): Since we consider social engineering frauds as unauthorized, we do not see a good fit. SK (MS comments): We support to set a claim excess which would set liability for payments under certain level on the PSUs as it can motivate their prudence. Setting of a specific amount or the percentage could be further explored. SI (MS comments): We cannot take a position because it is not clear what this means. SE (MS comments): We do not see a need for a claim excess that would weaken consumer protection, especially as it would be difficult to calibrate a claim excess relevant in all MS. RO (MS comments): - PT (MS comments): Please consider the same reasons explained in the previous answer. NL

	(MS comments): We are not in principle opposed to this, as this is currently already part of PSD2, but it should be a reasonably small amount. LV (MS comments): We support. LU (MS comments): yes LT (MS comments): We support – it might balance the burden of liability for PSPs. It would ensure that fraudsters would not be encouraged to exploit the possibility to defraud small amounts of money as SCA requirement may not apply for such payment transactions. PSUs, on the other hand, would know they have to demonstrate a right amount of duty of care regardless of the payment transaction they authorise. IT (MS comments): IT. If considered important in order to achieve an appropriate balancing of the interests at stake, we are not necessarily opposed to generalise the rule of art. 60 PSR (art. 74 PSD2), *i.e.* that the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50. However, we think that the same goal could be best achieved, and in a more flexible way, by introducing a rule on “contributory negligence” (see “Additional remarks”). HR (MS comments): We do not support this proposal. FI

	(MS comments): FI: Could be further discussed. DK (MS comments): We can support a small claim excess for impersonation fraud (but again with the exceptions listed above. If it is clearly the PSPs fault, the PSU should not have to pay a claim excess. CZ (MS comments): Acceptable (only in case that Article 59 or similar provision maintains). CY (MS comments): We are supportive.

3. duty for the PSU and the PSP to cooperate (as described in the note)	AT (MS comments): Yes. ES (MS comments): We agree with the duty to cooperate, although it is important to keep in mind that PSPs and PSUs have different means and abilities, and hence this needs to be taken into account. SK (MS comments): We see the merit, however the exact rules have to be set, to avoid circumvention of the liability by PSPs. SI (MS comments): We support the duty for PSU and the PSP to cooperate. SE (MS comments): We do not see a need to regulate this. If they do not cooperate, this is already taken into account in the claim assessment. RO (MS comments): We support the collaboration perspective of PSU with PSP given that PSU might have evidence that could help in the fraud investigation process. Additionally, this should be done under certain conditions by excluding the possibility in which the PSP is burdening the PSU with excessive requests that may cause the PSU to abandon their initial dispute. PT (MS comments):

	A duty to cooperate, within reasonable limits, shall be independent of the classification of transactions as authoritsed or unauthorised. We understand the inclusion of provisions that support the inclusion of a general duty of collaboration, but, in that case, it must be concretely foreseen how PSU must collaborate, the deadlines within which it must do so, as well as the consequences of its non-collaboration. We believe that negotiation of the PSR could represent an opportunity to consider whether the PSU's communication of unauthorised operations (or authorised operations where PSP may bear liability) should clearly identify the said operations. This requirement would allow the PSP to ensure an accurate identification of the disputed transactions. NL (MS comments): Based on the discussion note it is not clear to us what the duty to cooperate exactly entails. The note merely states that there should be a duty to cooperate, but it does not mention what the duty should consist of. In any event, we believe that not too much burden should be placed on the PSU. We can imagine that the PSP informs the PSU which information may be of use for its investigation and that the PSU then provides the information which is in his possession. LV (MS comments): We support amendments in articles related to duty to cooperate, but it should be harmonised with consumer protection regulations and should remain open to Member States to regulate in more detail or more specifically at national level. LU (MS comments): Open to discuss LT (MS comments): We definitely support. IT

	(MS comments): **IT.** We are in favour of a duty for the PSU and the PSP to cooperate in good faith. In our understanding, such a duty crucial to enable the PSP to gather all the necessary elements to determine, in each specific case, whether the PSU was "grossly negligent". Indeed, such assessment is often carried out on the basis of the factual elements provided by the PSU himself (in the complaint and, often, in the report filed with the police) and therefore, when the PSU remains silent, the PSP may often in practice be unable to prove 'gross negligence'. Having said that, we have the following observations on the proposal under option D. First of all, we do not understand why it is proposed to limit such a duty to two specific cases: (i) impersonation fraud and (ii) when the PSU denies having authorised a transaction for which SCA was applied. Indeed, the second point already covers all cases where the "gross negligence" is relevant and therefore the cooperation of the PSU is important (if SCA was not applied, "gross negligence" is irrelevant, as per art. 60(2) PSR). In the second place, we agree that the failure by the PSU to comply should not constitute *in itself* a ground for rejection of the refund. In the proposal, such failure should only give more time to the PSP to conduct an investigation. However, as we have said, in our opinion the PSP is often unable, in practice, to know the relevant facts (e.g. the messages sent by the fraudster) without the PSU's collaboration. In this scenario, additional time for the investigation might be of little or no use. We propose instead that the silence of the PSU may be an element to be considered, *always together* with the other circumstances, to assess the client's gross negligence, although *it cannot, by itself, constitute a ground for rejection* of the refund request. Alternatively, the consequences of the non-cooperation by the PSU may be left to the prudent assessment of Courts/ADR, which may take into account all the circumstances of the individual case. IE (MS comments): While we support this in principle, what does the 'duty to cooperate' mean in practice for the PSU? What are the consequences of non-cooperation? HR (MS comments):

	We agree with the duty for the PSU and the PSP to cooperate. FI (MS comments): FI: Could be further discussed. However, excessive requirements for the PSUs should not be introduced. DK (MS comments): We agree with the description of the duty to cooperate as described in the note. CZ (MS comments): Yes. CY (MS comments): We are supportive.

4. requirement to report the fraud to the police as a condition for the consumer's right of refund	AT (MS comments): Yes. ES (MS comments): We agree. SK (MS comments): Do not support. SI (MS comments): In principle, yes. We expect that the PSU will have at least some information to provide to the police. However, caution is needed here, as the provision could be too strict for the PSU. SE (MS comments): We oppose an obligation to report fraud incidents to the police. This is not a single market issue and goes beyond the mandate of this legal file. If needed, some guidance could be provided in a recital clarifying that PSPs could take this into account when PSUs seek compensation. RO (MS comments): Currently, at MS level, this is an usual practice, in which victims often report to the police frauds that fall under impersonation and investments scam. However, we don't support the approach that the refund right of the customer to be enforced only if the fraud is reported to the police. PT (MS comments):

	We agree and consider that PSP should require the same formality from PSU in other cases. PSP's often mention that this requirement would be relevant, namely, to attest the client's serious conduct. NL (MS comments): We are not principally opposed to this requirement, but it could also be reframed as the PSP encouraging the PSU to file a report at the police. LV (MS comments): Regarding the requirement for consumers to report the fraud to the police, we suggest making it as a recommendation rather than an obligation, or leave it to national legislation. LU (MS comments): yes LT (MS comments): We support. IT (MS comments): **IT**. We are unsure about introducing an express duty to report all frauds to the police. It could be overly burdensome for both the PSU and the police, without creating any added value in most cases. IE (MS comments): While we would support the requirement for consumers falling victim to fraud to report the fraud to the police and we support the notion of duty to cooperate, we would like to seek clarity around what the 'duty to cooperate' means

	in practice for the PSU together with any consequences of non-cooperation. As above, we would want to ensure that it is not detrimental to the PSU HR (MS comments): We agree with this requirement. FI (MS comments): FI: Yes, subject to a reasonable deadline. DK (MS comments): Yes, but this requirement could be on the PSP instead. CZ (MS comments): Yes. CY (MS comments): We are supportive.

5. further obligations on fraud prevention for ECPSs (in addition to the duty to cooperate in the COM's proposal)	AT (MS comments): Yes. ES (MS comments): We would like to highlight the relevance of declaring the obligations of all actors in the payment chain under the PSR, so that they arise at the same time, with a specific mandate to Member States to develop such provisions under the specific sectorial regulation and amend if needed the national telecommunication regime. For instance, in Spain, national legislation is currently being updated in order to allow ECS the possibility to block calls and/ or SMS where fraudulent elements are identified). Furthermore, we would like to highlight the fact that article 9 of the ePrivacy Directive (not included in the mapping exercise of EU regulation) prevents the use of location data to fight against fraud, which might be key to blocking certain fraudulent communications. Therefore, it needs to be considered if measures implemented in order to prevent fraud shall not be considered in breach of articles 5, 6 and 9 of Directive 2002/58/EC. This will serve in order to mitigate the risk that fraudsters move to those countries with a lax regulation. Regarding the possible additional obligations on fraud preventions, it should be also noted the need for ECPS to proactively adopt measures for fraud prevention. SK (MS comments): Obligations in alignment with the DCA directive. SI (MS comments): It is worth investigating further this option. In particular, it is necessary to check whether information can be obtained based on a court order. What is also very important is the exchange/access to data when fraud has already occurred. In practice, there have been cases where the recipient's bank did not provide information about its client, into whose account the fraudulently transferred funds were deposited. We suggest exploring this possibility, as it can also reduce the extent of fraud. This is especially true for the exchange/access to data that enables criminal and civil prosecution.

	SE (MS comments): We are open to explore this. We generally support the proposal from the Irish delegation. RO (MS comments): We also support the obligation under option E (EP's proposal) for ECSPs to refund the payer's PSP where the ECSP "does not remove the fraudulent or illegal content, after being informed of its occurrence" (Article 59(5))14, as well as other fraud prevention requirements for ECSPs that includes the perspective under Article 49(5b): that All providers involved in the fraud chain shall act swiftly to ensure that the appropriate organisational and technical measures are in place to safeguard the security of payments users when making transactions. PT (MS comments): In our view, seeking the cooperation of electronic communications service providers (ECSPs) in the level 1 text can improve outcomes in this area (for example, setting user education and awareness obligations and the obligation to share critical information about fraudulent activities with financial institutions and payment service providers). Furthermore, regarding liability in cases of impersonation fraud, we support the inclusion in the PSR of consequences for non-compliance by ECSPs with the requirement to cooperate with PSPs. With this in mind, we believe it would be essential to specify what actions and specific timings should be considered in the notions of 'cooperate closely' and 'act swiftly', under Article 59(5) of PSR. For this reason and considering the inherent specificities and technical challenges at a cross sectorial level, we believe that the EBA should be mandated to, in cooperation with BEREC, develop RTS to further specify what should be considered as 'cooperate closely' and 'act swiftly'." Nonetheless this poses some difficulties as ECSPs are not supervised by the same NCAs as PSPs. In view of the above, we believe that a broader articulation between ECSPs, PSPs and NCAs should be envisioned with the aim of fighting payment fraud not limited to impersonation fraud cases. Having this in mind, we consider that the consequences to ECSPs when they fail to comply with articulation requirements should be further discussed (penalties, liability or both). To ensure adequate legal certainty and clarity on this matter, it is essential, consistent with our previous comment, to further delineate the specific situations that

	could trigger such consequences. More specifically, we wonder whether a more proactive approach by ECSPs could be foreseen. NL (MS comments): Yes, we believe that the obligations for ECPSs should be further fleshed out and refer to our prior written comments in this respect. LV (MS comments): The direction of providing for a certain cooperation mechanism is welcome, but it is not clear whether this regulation imposes additional requirements on the mechanisms already regulating this segment. LU (MS comments): In our view the PSD/ PSR is not the right regulatory environment to address the rules applicable to ECPSs; the rules, regulations and provisions applicable to electronic communication service providers under the DSA and the Electronic Communication Code are already very complex, mixing up further elements or adding a new layer would create confusion in terms of which rules apply to whom under which circumstance and who is in charge of enforcing such rules. LT (MS comments): We support. IT (MS comments): **IT**. In principle, we believe that the discussion about ECSPs can be conducted independently from the discussion on "unauthorised transaction". In particular, we believe in the PSR we should realistically aim at two goals: ▪ A short-term goal should be strengthening the cooperation obligation that the Commission has already enshrined in its original proposal and require ECSPs to cooperate with PSPs [and PSUs]

	and by devising additional obligation, including being active in detecting abnormal patterns. In this regard, we are open to consider further obligation on fraud prevention for ECSPs. At the same time, we should avoid being too prescriptive, to ensure such provision is future-proof and leave national legislators and courts sufficient room for maneuver, to protect customers and define the exact boundaries of such a responsibility regime. ▪ The second goal should be medium-term and should be enshrined in a specific review clause, which, on the one hand, would require the Commission to carry out a holistic review of all relevant EU regulatory frameworks to verify if any amendments are needed to prevent frictions and facilitate fraud prevention and, on the other, would create a mechanism for monitoring fraud episodes and emerging techniques, participated by institutions, PSPs, ECSPs, and possibly customers' associations, to keep track and analyze the evolutions undergoing in the fraud environment. The ultimate goal should be substantiating the cooperation obligation imposed on the ECSPs and proposing adaptations and improvements (either at EU or national level) capable of ensuring a high and long-lasting level of customer protection. IE (MS comments): As noted in our non-paper, we support further obligations on fraud prevention for ECPSs HR (MS comments): We agree with further obligations for ECSPs. FI (MS comments): FI: No. A general cooperation duty would be appropriate. DK (MS comments): Yes. For telcos, this could be done by requiring them to apply SMS spam filters and by requiring better protection against spoofing. For digital platforms this could be as suggested in the Irish non-paper, and by requiring platforms to take down fraudulent ads when notified about them.

	They could also be required to take down websites with obvious fraudulent content, if they are flagged about this cf. the trusted flaggers. ECSPs should be obligated to act and to assist with information if they have any. It might then be necessary for the PSR to explicitly specify what they are allowed to share to protect them from GDPR violations. We have scrutiny reservation regarding potential liability for ECSPs. If liability is extended to ECSPs it is important that it would only be for something where they would have a realistic chance of preventing the fraud. However, if more actors are included in the definition (as suggested in the PCY discussion note from November 15) but with different requirements, we believe it would be better to have separate definitions for them. CZ (MS comments): Not acceptable. CY (MS comments): We are supportive.

6. a shared liability between the payer's and the payee's PSP	AT (MS comments): Yes. ES (MS comments): Perhaps the possibility that the payer's PSP claims against the payee's PSP if the latter has not fulfilled its obligations regarding the payee's KYC. SK (MS comments): Could be further explored if broader support of the MSs is indicated. SI (MS comments): The idea is interesting, but there are many open questions regarding its practical implementation, including the division of responsibility between PSPs (unless it is determined at the EU level that in such cases the responsibility is always divided, for example, 50-50). SE (MS comments): We are open to explore this. RO (MS comments): We are open to support a shared liability between payer's and payee's PSP as to it would motivate PSP's to develop better monitoring mechanism to prevent fraudulent transactions, including from the perspective of blocking a suspected/reported fraudulent transaction at payee's PSP level. We also support the obligation under option E for ECSPs to refund the payer's PSP where the ECSP "does not remove the fraudulent or illegal content, after being informed of its occurrence" (Article 59(5))14, as well as other fraud prevention requirements for ECSPs that includes the perspective under article Article 49(5b): that All providers involved in the fraud chain shall act swiftly to ensure that the appropriate organisational and technical measures are in place to safeguard the security of payments users when making transactions.

	PT (MS comments): Notwithstanding the duty of PSPs to enact adequate measures in order to prevent the use of their accounts as payees in fraudulent transactions, we believe it to be advantageous to keep the payer's PSP as the sole bearer of liability for unauthorised payments. Whereas under PSD2, the identity of the liable party is obvious to all involved (and, most importantly, to the client), introducing a system of shared liability would inevitably introduce uncertainty, as well as an added layer of procedural complexity, which would, in practice, result in less protection for the client in the event of a fraudulent transaction. As such, when applicable, the obligation to reimburse the consumer should be borne exclusively by the payer's PSP. NL (MS comments): We do not think this is necessary, but do not oppose this either. It should be clear what the shared liability exactly entails and most important, it should be clear for the PSU where to go and who to contact in case of being a victim of fraud, being the payer's PSP. LV (MS comments): We support. LU (MS comments): Open to discuss LT (MS comments):

	In general, we support the idea. However, its fulfilment needs to be clearly defined, having in mind that a significant if not the majority of fraudulent payments are cross-border payment transactions as well as the fact that fraudsters use a chain of payment transactions to launder and cash out the money (so, how this would work for Euro leg, One leg out transactions, etc.). IT (MS comments): **IT**. In our view, under the PSD3/PSR framework, the payer's PSP is liable because it controls the authentication process and is in the best position to intercept unauthorized transactions. It is also the one providing the payment service to the PSU (and is compensated accordingly). By contrast, the payee's PSP plays a more passive role, simply receiving the payment. Therefore, a blanket shared liability would be unwarranted, particularly when the payer's PSP may not have fully complied with its obligations (e.g. SCA; TMM; spending limits, etc.). Of course, the payee's PSP may sometimes be liable toward the payer's PSP, e.g. if it fails to comply with KYC/AML obligations, by crediting funds to an account without proper verification, or it does not cooperate with the payer's PSP to recover the funds. For such cases, we believe that the general rules on civil liability are sufficient. On the other hand, a shared liability between the payer's and the payee's PSP seems to us more appropriate, for example, in the context of the UK liability regime for APP fraud, where the main goal is to protect the PSU, even from fraud ''external'' to the payment service, on which the PSP has less control. In such cases, distributing liability among the various actors within the payment system appears more reasonable. IE (MS comments): We would support a full exploration of this topic HR (MS comments): We do not support this proposal.

	FI (MS comments): FI: Could be further discussed. However, for this, the payee's PSP should also be given necessary tools (such as possibility to freeze received funds where there is a suspicion of fraud) in order for this to be justifiable. DK (MS comments): Yes, generally we support this. If the payee is a fraudster, then the payee´s PSP should be responsible for allowing a fraudster to have an account with them. However, this also means that we need to give the payee's PSP the appropriate tools to use transaction monitoring and to freeze received transfers of funds if their transaction monitoring gives rise to suspicions of fraud or if they are contacted by the payer's PSP (which for instance could also have suspicions due to their own transaction monitoring or due to being contacted by the payer). We have provided drafting for the freezing of funds in the 4CT after the WP on November 26th. We have included the suggestion in article 69. However, there could be some exceptions where only the PSP of the payer should be liable. This could be if the PSP does not correctly use IBAN name check or if a transaction is not even authenticated in cases where it would need to be authenticated. This could be considered to be a kind of gross negligence on the part of the payers PSP, and consequently the payee's PSP should not be liable. **<u>One point of entry for PSU for refund claims:</u>** to make the refund process as easy as possible there should only be one "point of entry" for the PSU, the PSU should only need to contact their own PSP which should cover the entire refund to the PSU. Then afterwards the payers PSP could seek for refund from the payee's PSP. CZ (MS comments): It depends on the procedure and specific rules of potential shared liability. CY (MS comments):

	We are supportive of a shared liability between the payer's and the payee's PSP. The matter of the PSP of the payer being outside the EEA should also be addressed.

Do you consider that all or some of the safeguards mentioned above could be introduced also if a different approach on the concept of authorisation were taken (e.g. if impersonation fraud were treated as 'authorised' transactions but with a right of refund)? If yes, please explain which safeguards you would support and in which cases.	AT (MS comments): Yes; in that case, we would also support the same safeguards. ES (MS comments): We agree with the safeguards mentioned above, but, as previously stated, we consider that impersonation fraud operations should be not authorized. SI (MS comments): / SE (MS comments): The purpose of the safeguards is to balance the burden of liability to the PSPs advantage. To introduce a narrower definition of unauthorised transactions compared to the current one in PSD2, **while at the same time** introducing safeguards to the PSPs advantage would mean an unacceptable deterioration of consumer protection. Furthermore, the main purpose of the definition of unauthorised transaction is its function as gatekeeper to the refund rights. It would only add complexity to set a narrow definition of unauthorised transactions while introducing different types of exemptions. RO (MS comments): We do not support the approach for considering impersonation fraud as authorised, but if, we believe that for other fraudulent payments the following safeguards are still relevant: (i) the possibility for the payer's PSP to apply a claim excess, (ii) duty for the PSU and PSP to cooperate, (iii) requirement to report the fraud to the police as a condition for the consumer's right of refund and (iv) further obligations on fraud prevention for ECPSs. PT

	(MS comments): As we referred above, we consider that bank-employee impersonation fraud should have a consistent approach with the one followed for unauthorised transactions (in particular regarding PSP liability with PSU liability in case of gross negligence). Therefore, and for the reasons we already mentioned, there are some safeguards that should be implemented in general, regarding these transactions and unauthorised transactions, namely: (i) The duty for the PSU and PSP to cooperate. (ii) The duty for the PSU reports the fraud to the police. Additionally, we would propose to impose a shift of liability from the PSU to the PSP in the case where the PSP grossly fails to apply the provisions and requirements regarding the transaction monitoring mechanism (TMM) as foreseen in Article 83(2) of the proposed PSR, in particular by failing to detect and prevent fraud by not taking into account elements of data that could be instrumental to prevent fraudulent transactions. On this topic of fraud prevention we fail to understand the constant lack of support in encouraging PSPs to invest in advanced and flexible Transaction Monitoring Mechanisms (TMM). We believe this possible shift of liability will encourage PSPs to invest in having better TMMs. This liability shift provision could be set in article 60 of the proposed PSR and be further detailed by means of recitals to be included in the Regulation, comprising the following key factors: • The PSP grossly disregarded the environmental and behavioural characteristics which are typical of the payment service user in the circumstances of a normal use of the personalized security credentials; • The PSP grossly disregarded the payment transaction history of the payment service user and normal amounts of payment transactions; • The PSP grossly disregarded lists of compromised or stolen authentication elements, signs of malware infection in any sessions of the authentication procedure and, in case the access device or the software is provided by the payment service provider, the 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. NL (MS comments): Our position regarding the different safeguards above remains the same. So we do not support 1, but could envision that measures 2-6 would be applied, but only in the form as outlined in our comments.

	LV (MS comments): SCA notification before "moving" or adding card data, same with payments. LT (MS comments): Even if impersonation fraud or other APP frauds would be defined in PSR as 'authorised' payment transactions, reimbursement rules for such fraudulent payment transactions would have to, nonetheless, entail the aforementioned additional conditions as they should not be treated equally 'unauthorised' payment transactions *by nature*, since the latter ones require and signify a different level of PSU involvement and its awareness. IT (MS comments): **IT.** We do not think it would be appropriate to break the symmetry between unauthorized → refund (except for payer's fraud or gross negligence) and authorized → no refund. We believe it would be better to properly define the concept of "unauthorized transaction" rather than to introduce an exception to the no-refund rule for authorized transaction (an exception that would in turn have to be properly defined). HR (MS comments): In any case, we have the same position regarding authorised transactions as we stated above in relation to impersonation fraud and Article 59 in the Commission's proposal. FI (MS comments): FI: Yes. We would not, at least at this stage, deem it necessary to limit the application of the safeguards based on what a refundable transaction is called. DK (MS comments):

	We believe that this would be creating too much confusion. If a transaction is authorised, it would be legitimate. However, we would support adding a new category for impersonation fraud so instead of just having two categories (authorised and unauthorised), we would have three categories: • 1) authorised and authenticated, • 2) unauthorised but authenticated, and • 3) unauthorised and unauthenticated. In category 1 there would be no question of liability since the payment was authorised and authenticated. In the second category we would have the impersonation fraud. Here, the PSP would be liable but e.g. claim excess and caps could apply but generally the PSP would be liable. The liability could also be shared by the PSPs. However, in category 3 the payer's PSP would be fully liable – no caps, no claim excess, and no shared liability. CZ (MS comments): We can imagine no 3 – duty for PSP and PSU to cooperate and no 6 – shared liability between the payer's and the payee's PSP (especially in cross border situations). We would be hesitant to set strict thresholds as "payer's PSP is liable on XX% if … and payee's PSP is liable YY% if…". This should be based on the civil law. CY (MS comments): We consider that all of the safeguards referred to above could be introduced should impersonation fraud be treated as ''authorised transactions with a right of refund''.

Would you support the shift of liability on the PSP in the EP's proposal (option E), e.g. where the PSP does not block a transaction in case of reasonable grounds for suspecting fraud?	AT (MS comments): While we are, in general, open to this idea, it is important to consider the different effects that may result from such a shift of liability; on the one hand, it could provide for incentives to improve the transaction monitoring/fraud prevention mechanisms of PSPs; on the other hand, PSPs could react to this obligation with excessive de-risking, seriously harming the smooth flow of payments. Furthermore, a certain extent of liability in such cases should also rest with the PSU, so instead of a total shift of liability, some kind of "co-liability" between the PSU and the PSP may be more appropriate. All in all, it would be important to have an in-depth discussion on this topic to strike a delicate balance here. ES (MS comments): We would favour introducing clear, robust, and actionable preventive measures for PSPs, such as access to information, sharing of data or transaction profiling. For the sake of compromise, only in those cases where requirements to these entities are clear and limited it would be reasonable to accept liability to arise, and it should be linked to the failure to implement any of those preventive measures. SK (MS comments): See the merit, open to consider. SI (MS comments): In principle, yes, but caution is needed in interpreting the block – if the PSU explicitly wants to execute this transaction despite the PSP's warning and the conditions for executing the payment order are met, we do not see how the PSP can avoid the transaction. SE (MS comments):

	This should be part of the broader liability assessment made by courts. There is no need to decide on this ex ante. The interpretation of 'reasonable grounds' needs to be assessed in any case, so there is no gain from reduced complexity in the liability assessments. RO (MS comments): We support the EP's proposal as it shifts the liability on the PSP in the situation of other fraud cases as well – e.g, where a PSP does not block a payment instrument "despite reasonable grounds for suspecting fraud". This extended liability seems to apply in the EP's proposal regardless of whether the transaction is "authorised" or "unauthorised", and regardless of whether the PSU acted or not with gross negligence. However, we think the article 51 (2) should also clearly include the possibility for the payer's PSP to not execute a payment transaction based on the results obtained from the application of the transaction monitoring mechanism (TMM) of fraud data sharing mechanism. PT (MS comments): Yes, please consider the previous answer considering our proposal on a shift of liability from the PSU to the PSP in the case where the PSP grossly fails to apply the provisions and requirements regarding the TMM as foreseen in Article 83(2) of the proposed PSR. NL (MS comments): No. LV (MS comments): We support. LU (MS comments): Open to further assessment; PSPs should have a sound risk management and transaction monitoring in place in order to prevent and reduce fraud cases as much as possible.

	LT (MS comments): We would restrain from this proposal as it might create a moral hazard of abuse on the side of PSUs (not to take a reasonable amount of duty of care). Fraud typologies or ways fraud is executed may change very quickly so it would very hard to define what are 'reasonable grounds' to suspect fraud, especially if it actually happens. We believe that reimbursement of clearly defined unauthorised and APP fraud payment transactions (followed by certain conditions) would constitute a rather balanced liability regime that ensures a high level of consumer protection. IT (MS comments): **IT.** We think that such a case would be best addressed by a rule on "contributory negligence". Indeed, if the PSU was "grossly negligent" it would be improper to shift all the liability because, for example, the transaction monitoring was not properly performed. If both parties are "at fault" a shared liability would the most flexible and equitable solution (see "Additional remarks"). HR (MS comments): We would support the shift of liability on the PSP where the PSP does not block a transaction in case of reasonable grounds for suspecting fraud. We do not support option E. FI (MS comments): FI: At least to some extent, yes. Ideally, this would incentivize the PSPs to examine suspicious transactions more thoroughly. DK (MS comments): We support this. However, this would be redundant if we decide to include impersonation fraud within the sphere of liability for PSPs. DE

	(MS comments): No, we do not support this proposal. The EP approach bears the risk that PSPs will on a large scale just block "unusual" payment transactions in order to avoid liability (e.g. PSU wants to make a payment transaction during vacation abroad). This would in the end impair PSUs who cannot fulfil their payment obligations. Besides, it would also open new liability questions, i.e. who would be liable for any damage caused by an undue blocking of a payment transaction. CZ (MS comments): Only in case Art. 59 and Art. 49 (2) [BE PRES proposal] are deleted. CY (MS comments): We are supportive of the shift of liability on the PSP, where the PSP does not block a transaction in case of reasonable grounds for suspecting fraud, as per the EP's proposal (option E).

Would you suggest a shift of liability on the PSP in other cases as well? If yes, please explain.	AT (MS comments): No. ES (MS comments): No. SI (MS comments): / SE (MS comments): We do not understand the question, a shift compared to what? RO (MS comments): Yes. This might include also payments that haven't been authenticated under current SCA regime, but also transactions that haven't been subject to other mandatory security measures such as payee verification (in line with the Instant Payment Regulation) or any other security measure recommendation issued by the competent authority. By shifting the liability to the PSP that are in violation of any additional security measure imposed or recommended by the competent authority. This approach will allow the PSPs to adapt faster in order to prevent fraudulent transactions, especially based on complex and innovative fraud scenarios. PT (MS comments): N.A. NL (MS comments): No.

	LV (MS comments): Only if there has been gross negligence on the part of the client. LU (MS comments): No LT (MS comments): No. IT (MS comments): **IT**. See our previous answer. HR (MS comments): No DK (MS comments): The examples mentioned below would be redundant if impersonation fraud is considered unauthorised. However: If the payer's PSP fails to notify the PSU of a discrepancy in the IBAN name check. If the payee's PSP does not freeze funds even if they have reasonable grounds for suspecting fraud (by their own transaction monitoring or by being contacted by the payer's PSP. DE (MS comments): No

	CZ (MS comments): Only in cases when PSP does not fulfil its obligation – e.g. when the transaction monitoring is insufficient or when IBAN verification is not provided as in the EC proposal. CY (MS comments): We have no further comments.

How wide range of cases should the reimbursement regime cover? (only if not covered by the responses to the Qs below)	ES (MS comments): Already covered in previous responses. SI (MS comments): / SE (MS comments): The payment landscape is changing fast, including the fraud methods. At the same time, the refund claims are very complex, with dozens of different circumstances to be taken into account – including the actions of PSUs and PSPs. Therefore, there is a strong case for a **less prescriptive liability model adaptable by case law**, with a scope sufficiently wide to cover today's fraud methods as well as the future's. Therefore, we think that **social engineering fraud** should be included in the scope of the liability regime as **unauthorised transactions**. This is crucial to give both PSPs and PSUs balanced incentives to actively develop capabilities to mitigate all types of fraud risk. In our experience, PSPs **can** take measures to prevent social engineering fraud – if they are incentivised to do so. This would mean that victims of social engineering fraud may have their case tried for **possible compensation**, given that they have not acted with gross negligence. This does however **not** mean that the significance of the PSU's own part in social manipulation fraud is ignored, as it is a key aspect of the gross negligence assessment, along with other relevant aspects. We would also like to emphasise that we are **not** saying that the PSPs should be liable in all social engineering fraud. We are just saying that **PSPs' liability should not be 0%.** We should not disqualify PSUs' claims solely based on the fraud methods used. RO (MS comments): -

	NL (MS comments): - LV (MS comments): All of the above are subject to the reimbursement regime. The minimum threshold could be €50, the maximum - AML thresholds, e.g. €10,000, would apply if the customer has not knowingly made payments. LT (MS comments): Covered in the answers above. IT (MS comments): **IT**. See our previous answers. HR (MS comments): We consider this question already covered by our responses to the questions above. CZ (MS comments): The range currently stated by PSD2 – unauthorised transactions. CY (MS comments): We have no further comments.
Burden of proof & "Gross negligence"	PT (MS comments): • **The burden of proof**

	We favour the cases that support that the PSP remains responsible to prove that the transaction was “authorised”, namely by proving it was initiated and authenticated by the payer. We note that in cases the PSU denies having authorised a payment, SCA is not sufficient to prove authorization.

Where the PSU denies having authorised an executed payment transaction, do you agree that the PSP should prove that the transaction was "authorised"?	AT (MS comments): No. We support the present PSD2 approach where the PSP has to prove that the payment transaction was "authenticated". We fear that the PSP cannot prove the authorisation (= PSU's consent to execute the payment transaction) as such, as the expression of consent through the initiation of the payment transaction by the PSU is outside the sphere of the PSP. The PSP cannot provide evidence based on its own resources and thus relies on the cooperation of the PSU. However, since the PSU has interests contrary to those of the PSP, conflicts of interest are to be expected. Therefore, it is appropriate to assign the burden of proof for circumstances within the PSU's sphere, which may only be known to them, to the PSU. Authentication, on the other hand, is the technical procedure for verifying authorisation, which takes place in the sphere of the PSP. In this regard, the burden of proof rightly lies with the PSPs. ES (MS comments): We believe that both the PSP should prove that the operation was 'authorized,' and the PSU should prove that it was not. We do not believe that the burden of proof should rest exclusively on one party. The decision on whether the operation was truly 'authorized' or not should be the result of an analysis of the evidence provided by both parties. However, it should be noted that responsibility in this sense needs to be assigned taking into consideration the asymmetric means and resources of PSPs and PSUs. SK (MS comments): We support. SI (MS comments): If the PSP can prove that SCA was performed, it is necessary to investigate whether the PSP could have suspected, based on other circumstances, that the transaction was not authorized (e.g., unusual time, transaction amount, different IP address, foreign IP address, etc.). If so, the PSP could timely identify the transaction as potentially unauthorized. Beyond this, the PSP likely will not have all the information needed to conclude whether the transaction was authorized or not.

	SE (MS comments): According to Swedish civil law praxis, the PSU should prove that there is reasonable doubt that he/she did not consent to the payment transaction. This seems like a reasonable approach – PSUs should be able to show some indication of fraud in support of their refund claim. RO (MS comments): Yes, we support this approach that the burden of proof lies on the PSP. PT (MS comments): The burden of proof is on the PSP. NL (MS comments): Yes. The PSP should prove that the transaction was correctly authenticated, and if this is the case, the transaction was authorised. The PSU should provide otherwise. LV (MS comments): Yes, the PSP should try to prove otherwise. LU (MS comments): We continue to support the current approach under PSD2, whereas the burden of proof lies on the PSP. Where the PSU claims that a payment was unauthorised, the burden lies on the PSP to demonstrate that the transaction was authenticated, accurately recorded, entered in the accounts, and not affected by a technical breakdown or some other deficiency of the service provided by the PSP. LT (MS comments):

	Yes. IT (MS comments): **IT**. Yes. As said, in our experience, the PSPs, in order to avoid liability, most often attempt to prove the "gross negligence" of the PSU, without even trying to prove that the transaction was authorized. IE (MS comments): We could agree that the PSP should prove that the transaction was authorised where the PSU denies having authorised the transaction HR (MS comments): The burden should be on the PSP, but specifically PSPs have to prove that the transaction was **authenticated**. We support keeping the current wording from PSD2 in this context. FI (MS comments): FI: Yes. DK (MS comments): Yes. But it should include a burden of proof and duty to cooperate for the PSU. DE (MS comments): We prefer keeping the present PSD2 approach where the PSP has to prove that the payment transaction was "authenticated". We fear that the PSP **cannot prove the authorisation** (= PSU's consent to execute the payment transaction) as such, as the intent/will of the PSU is an inherent fact outside the sphere of the PSP. Practically speaking, the PSP lacks knowledge of the specific circumstances surrounding the initiation of the payment

	transaction. The PSP cannot provide evidence based on its own resources and thus relies on the cooperation of the PSU. However, since the PSU has interests contrary to those of the PSP, conflicts of interest are to be expected. Therefore, it is appropriate to assign the burden of proof for circumstances within the PSU's sphere, which may only be known to them, to the PSU. Authentication, on the other hand, is the technical procedure for verifying authorisation, which takes place in the sphere of the PSP. In this regard, the burden of proof rightly lies with the PSPs. **Open questions:** -What is concretely the **difference** between the current rule (evidence on authentication) and the new rule (evidence on authorisation) in terms of the evidence to be presented? - How can the PSP prove the PSU's consent to execute the payment transaction? - What kind of evidence must the PSP present? CZ (MS comments): Yes – but the cooperation with PSU is necessary. CY (MS comments): We are supportive of requiring the PSP of proving that the transaction was ''authorised''. BG (MS comments): We agree with the Presidency's proposal.

Would you support to add that where a PSU denies having authorised a transaction, the use of SCA in itself is not sufficient to prove authorisation by the payer?	AT (MS comments): Yes, in accordance with the Art. 72 para 2 PSD2. ES (MS comments): Except in cases of manipulation (e.g., social engineering) or in those cases where the credentials are used without consent by the customer, SCA should be considered sufficient. In the case of manipulation or unauthorized use of credentials, strong customer authentication would not be sufficient. Gross negligence needs to be considered only for the sake of liability and reimbursement, not for the definition of authorized or unauthorized transactions. SK (MS comments): We see merit. SI (MS comments): Yes. SE (MS comments): Yes. RO (MS comments): We support this approach since the authentication or the use of the SCA shall not be sufficient to prove that the payment transaction was authorised by the payer. PT (MS comments): The performance of the SCA by the PSU must be proven by the PSP. SCA is not sufficient to prove authorization.

	NL (MS comments): No, we do think that SCA is sufficient. As indicated earlier we do not want to change the concept of authorized payments. We do think an article should be added (article 59) that bank impersonation fraud should be reimbursed even though the payment was authorised. LV (MS comments): Yes, given the use of social engineering techniques and psychological methods, the SCA itself does not prove conscious decision-making. LU (MS comments): Such addition would create a high degree of legal uncertainty and would question the application of SCA. LT (MS comments): We strongly support to include this in the regulation. IT (MS comments): **IT**. Yes. HR (MS comments): No FI (MS comments): FI: Yes. DK (MS comments):

	Yes. We strongly agree with this. DE (MS comments): We could agree to the proposal, if the word "necessarily" is reinserted as contained in the current PSD2 (Art. 72(2)), i.e.: "Where a PSU denies having authorised a transaction, the use of SCA shall in itself not **necessarily** be sufficient to prove authorisation by the PSU". Deleting the word "necessarily" (as proposed in Art. 55(2)) adds to the PSP's difficulty to prove that the transaction was authorised. It restricts the possibility of courts to be able to decide on a case-by-case basis that in exceptional circumstances the proof of the use of SCA might be sufficient to prove authorisation. That is why the word "necessarily" should be reinserted. Under this condition, we can agree to the above-mentioned addition on SCA. CZ (MS comments): Basically it the regime of PSD2 as well (there is a reference to a payment instrument - SCA.) CY (MS comments): We are supportive of adding the text ''where a PSU denies having authorised a transaction, the use of SCA in itself is not sufficient to prove authorisation by the payer''. BG (MS comments): We agree with the Presidency's proposal.

Would you support a "duty to cooperate" between the PSU and the PSP as described in Option D? If no, please explain which elements of such duty to cooperate outlined in Option D you do not agree with and explain why.	AT (MS comments): Yes. ES (MS comments): Yes, we support a duty to cooperate that takes into account the asymmetric means and resources available to PSPs and PSUs. SK (MS comments): See our comments above. SI (MS comments): It depends on the consequences if the PSU does not cooperate – if this does not affect its ability to be repaid (i.e., cooperation is not a condition for repayment), then in principle, we do not see any obstacles. SE (MS comments): We do not see a need to regulate this. RO (MS comments): We support the duty to cooperate between the PSU and the PSP, however we don't envisage to limit this collaboration only for the two scenarios included under option D: (*1*- where a consumer claims to have been a victim of impersonation fraud covered by Article 49(2) and *2*- where the PSU denies having authorised a transaction for which SCA procedure was applied), but rather the duty to cooperate between the PSU and the PSP should be applicable in all cases where the PSU disputes a payment transaction. PT (MS comments):

	We are in favour of establishing the referred collaboration duty to PSUs, namely setting out that PSUs shall provide supporting documentation, whenever possible. Nevertheless, the requirements to evaluate this duty to cooperate should be detailed to prevent the risk that the PSP unilaterally decides that the PSU did not "sufficiently" cooperate. NL (MS comments): See our previous comment. LV (MS comments): We support a duty for the cooperation between PSU and PSP, but it should be harmonised with consumer protection regulations and should remain open to Member States to regulate in more detail or more specifically at national level. There should also be a solution for cases where the MPL fails to communicate or lies, which is quite typical. LU (MS comments): Cooperation between PSU and PSP as outlined in option D constitutes an important element towards addressing fraudulent transactions. LT (MS comments): We support strongly as well the inclusion of 'duty of care' in the regulation. IT (MS comments): **IT**. Yes. (See our observations above). HR (MS comments): We support a duty to cooperate. FI (MS comments):

	FI: Yes. We find it important that excessive obligations are not imposed on the PSU. To this end, we support the limitation to "all the relevant information […] that the PSU can reasonably be expected to have regarding the events leading to the disputed payment transaction." Furthermore, the consequence for the breach of this duty should not constitute a ground for rejection of the refund. However, it could constitute a ground for the PSP to not refund the PSU immediately and conduct, within a reasonable time, an investigation for determining whether or not the transaction was authorised. DK (MS comments): We support. DE (MS comments): A "duty to cooperate" would be particularly relevant under a regime, where the PSP is not able to generate evidence based on its own resources and thus has to prove authentication solely on the basis of evidence presented by the PSU. In those situations, however, the interests of the PSU would be contrary to those of the PSP. In consequence, the system would be highly impracticable given the arising conflicts of interests, most likely leading to disputes regarding the quality and quantity of evidence produced by the PSU. Hence, we are in favour of keeping the current, clear PSD 2 regime, where both the PSU and the PSP have to prove different aspects of authorisation that are within their sphere of responsibility. CZ (MS comments): Yes. CY (MS comments): We are supportive of the "duty to cooperate" between the PSU and the PSP as described in Option D. BG (MS comments): We would like to see a more detailed framework for the duty to cooperate. Moreover, we are of the opinion that the consequences, stemming from a failure to comply with this obligation, should be outlined after the framework has been defined.

Do you consider that more clarifications in PSR as regards the duty to cooperate would be needed beyond the aspects outlined in Option D? If yes, please elaborate.	AT (MS comments): We think that the proposal by HU PCY provides for an appropriate cooperation framework between the PSP and the PSU under Option D. However, it must be clarified that there are no "unrealistic" expectations regarding the cooperation obligations of the PSU, who, in most cases, will be a consumer without any deeper understanding of the legal situation. ES (MS comments): No. SK (MS comments): Could be further explored. SI (MS comments): It depends on the consequences if the PSU does not cooperate – if this does not affect its ability to be repaid (i.e., cooperation is not a condition for repayment), then in principle, we do not see any obstacles. RO (MS comments): No. PT (MS comments): The aspects outlined in option D appear to provide some detail on the contents of the duty to cooperate. However, issues such as the obligation to the payer's PSP to assist the PSU in the fulfilment of their cooperation duty, or the consequences of non-cooperation by the PSU, should not be merely mentioned in the recitals, as suggested in the Discussion Note, but rather be inserted into the articles. NL

	(MS comments): Yes, as indicated earlier we do not think that this is clear enough. LV (MS comments): It may not be necessary to oversaturate the text. LT (MS comments): We believe that PSPs should bear the responsibility and be active in collecting evidence regarding the disputed transaction and the PSUs will. PSUs, upon the request of the PSPs, have to provide information and evidence, yet, they should not bear the responsibility to know what information might be needed to prove their case. However, we also think that obligation for PSUs to cooperate with their PSPs as well as the consequences for failing to do that, should be incorporated in the regulation. E.g. 'In cases where there is no objective evidence that third parties may have used the PSU's payment instrument and its personalised security details, without the PSU's knowledge and will, during the initiation of a payment transaction which is confirmed in the manner agreed between the parties and which is disputed by the PSU, and where there is only the PSU's subjective explanation of the fact, then such a payment transaction should normally be deemed as properly authorised.' IT (MS comments): **IT**. No. Of course, its actual content largely depends on the concrete circumstances of the case, so that only broad indications can be given by the legislator. HR (MS comments): No further clarification is needed. DK (MS comments):

	Currently no. But this is quite important for making it work in practice and to ensure that people cannot just falsely claim to have been frauded and expect for it to be impossible for the PSPs to discover. Thus, we are curious to see if other member states believe elements are missing, and we are curious to see the actual drafting on this. However, generally we support what is written in the note. We support the more principle-based approach with references to cooperating in good faith, as we fear that if we e.g. begin to give PSUs specific deadlines in the communication with the PSP, they might not be adequately aware of such deadlines, and this should not be an escape ticket from liability for PSPs. It would also be difficult for us to predict and write in to the level 1 act all of the ways in which it would be possible to not "cooperate in good faith". Thus, it would be better to let the courts assess this if the PSPs claim that a PSU has not cooperated in good faith. DE (MS comments): see above CZ (MS comments): We would welcome explanation in a recital. It should be bear in mind that in some cases, PSU cannot prove anything and on the other hand, PSP does not have any information about the case. CY (MS comments): We have no further comments. BG (MS comments): We would like to see a more detailed framework for the duty to cooperate. Moreover, we are of the opinion that the consequences, stemming from a failure to comply with this obligation, should be outlined after the framework has been defined.

Would you add any examples of gross negligence in the recitals? If yes, which examples?	AT (MS comments): No. We support the work of BE-PCY on this topic and do not deem any additions necessary. ES (MS comments): We consider that the concept of gross negligence is key to allocation of liability, and, as such, it should be part of the provisions in the law. Particularly, those examples where there is consensus could be included in the articles, while additional examples could be in the recitals. All in all, we favour a clear definition of this concept in order to avoid divergent interpretation amongst Member States. SK (MS comments): Listing the examples could be helpful. As an example, we would welcome explicit mention of the sharing the account credentials with the person without the right of disposal. SI (MS comments): In our opinion, it is not necessary, considering that this is a matter of civil law, which is not harmonized at the EU level, and gross negligence is a legal standard defined by the courts. SE (MS comments): No. RO (MS comments): We support the examples of gross-negligence outlined in Option D, however we see merit in giving a mandate to the EBA to issue guidelines regarding the concept of gross negligence in the context of the PSR, as, in our opinion, there should be applied a flexible regime based on lessons learned and taking into consideration emergent

	complex and innovative scenarios. This approach, will facilitate a more flexible regime and it would be less burden from a judicial perspective to update a , rather than a regulation, if needed. PT (MS comments): We prefer to mandate the EBA to issue guidelines on gross negligence (see last answer bellow). NL (MS comments): Yes. Under the Belgium Presidency we discussed a list of examples of gross negligence. We would support to include these in the recitals and indicate that this is a non-exhaustive list. LV (MS comments): We support a general and flexible approach, with the possibility to set our own examples at national level, based on case law. An example of gross negligence could also be where, prior to confirming a transaction/remote transaction with the SCA, the customer is explicitly told what they are confirming, e.g. "Warning! By entering PIN1 you grant permission to connect to online banking". Same for PIN2 showing the payee's details and the amount. LT (MS comments): We would be not against giving some examples of gross negligence in the recitals. However, since fraud typologies, or better to say, the ways frauds and scams are executed, change very quickly as well as the social environment, we believe it is much better to give an inexhaustive list of criteria on how to determine whether the PSU in question acted grossly negligent. IT (MS comments): **IT**. We think the conclusions reached in the previous WPs on the issue are satisfactory. IE (MS comments):

	Guidance in the Recitals should be further fleshed out with a list of non-exhaustive, non-cumulative and non-binding factual circumstances that may be taken into account when assessing possible gross negligence, aligned to the EBA Opinion on new types of payment fraud and possible mitigants HR (MS comments): No DK (MS comments): Generally, we do not support the inclusion of a list of gross negligence at all. However, if other MS wish to include this we can live with a non-exhaustive, non-cumulative list in the recitals of non-binding nature, which the courts can use as inspiration if they decide to. DE (MS comments): The degree and evidence of negligence should generally be evaluated according to national law by the court which is confronted with the case at hand, as it is primarily a civil law question. As already stated, a non-exhaustive list of criteria to be considered when assessing gross negligence could be useful and promote uniform application in all MS. Courts should take those criteria into account at their discretion when evaluating negligence in accordance with national law, but should not be bound by them when the individual circumstances of the case at hand call for a different evaluation. Our drafting suggestions already submitted included some illustrative examples „if the loss of a payment instrument is not reported to the responsible office immediately after the loss is discovered“/“Enabling spying when entering access data at ATMs is not sufficient by itself to justify gross negligence.“/“Inexperience and unskillfullness of the payment service user may exclude gross negligence in individual cases.“/ „where the payment service user has ignored a clear, concrete and case-specific warning by the payment service provider about how to react in the type of fraudulent situation which then occurred and led to the damage or where the payment service user has failed to check if the elements which are dynamically linked and displayed during the strong customer authentication in accordance with Article 85 are correct” The last scenario which – according to German case law – seems to occur quite regularly and should form a further example of gross negligence is connected to Strong Customer Authentication (SCA). The duty of PSPs to perform

	SCA is – alike the warning duty - aimed at preventing fraud. If customers fail to perform their part of the SCA procedure, they can be regarded as acting with gross negligence. This is especially the case if they ignore the specific amount and specific payee which is dynamically linked to the transaction and displayed to the customers (cf. Article 85 (8) PSR). However, gross negligence should always depend on the circumstances of the individual case and only apply if there is a sufficient connection between the warning and the conduct of the payer that led to the damage. CZ (MS comments): Current proposal of recital is sufficient. CY (MS comments): We have no further examples to add. BG (MS comments): We would consider it helpful to have some additional examples in the recitals, following further reflections on this subject. We would also support an approach to include a non-exhaustive list of circumstances that PSPs should take into consideration in order to determine if a case constitutes “gross negligence”, as proposed by the Lithuanian non-paper (during Spanish Presidency).

Do you agree with the potential amendments proposed in Option D to the list of non-exhaustive, non-cumulative and non-binding list of circumstances which can be taken into account when assessing gross negligence on the part of the PSU? If no, please explain.	AT (MS comments): We support the work of the BE PCY on this topic and do not deem any additions necessary. ES (MS comments): Yes. SK (MS comments): We see the merit, but more discussion needed. SI (MS comments): In our opinion, it is not necessary, considering that this is a matter of civil law, which is not harmonized at the EU level, and gross negligence is a legal standard defined by the courts. If necessary, the Court of Justice of the EU can provide guidance. SE (MS comments): No, the gross negligence concept should be left to civil law. We are especially concerned about the proposed circumstances in d and h in Option D. **Concerning d:** It is a well-known problem that fraudsters pass on information on vulnerable groups that already have fallen victim of fraud and are desperate to get their money back. They are therefore much more likely than other groups to be targeted again. This should not be used against them. **Concerning h:** The significance of failing to check the information displayed when using SCA should not be over-emphasised, as **PSUs are reliant on how and in which format the PSP choose to display the information.** In Sweden for example, the same mobile application and format is used when identifying yourself on the web page of your local library or when making a EUR 2 million transaction to a foreign account. The details of the information given is easily overlooked. Especially in cases where the fraudster is providing conflicting information

	in real time over the phone, providing plausible explanations for why the information does not match or creates a stressful situation where the victim does not have time to double-check the information given. RO (MS comments): Yes, we agree with the potential amendments proposed in Option D to the list of non-exhaustive, non-cumulative and non-binding list of circumstances which can be taken into account when assessing gross negligence on the part of the PSU. PT (MS comments): We strongly oppose that approach (see last answer bellow). NL (MS comments): It is not clear to us which examples are meant. D does not contain any new examples. LV (MS comments): We support this approach. LU (MS comments): In our view such list of criteria is better placed in a recital. LT (MS comments): We disagree with the suggestion to delete points a) and i) as they can give a valuable insight into how the PSU in question behaved under known circumstances compared to how far such behavior falls short to the standard 'duty of care' that any PSU (except the vulnerable ones) would be expected to meet. E.g., if the defrauded PSU uses its payment instrument against its typical usage, even for that PSU (gives away PSU's payment card personal security credentials 'to receive funds in the payment card account'), his or her behavior could be considered too far from the standard of 'duty of care'. IT

	(MS comments): **IT**. Yes. HR (MS comments): We support non-exhaustive, non-cumulative and non-binding list of circumstances which can be taken into account when assessing gross negligence on the part of the PSU as proposed by BE PRES. We do not support option D. FI (MS comments): FI: In case a list of circumstances will be maintained, we are of the view that the reply received by the PSU for the IBAN Name Check/Verification of Payee could be added to the list, e.g., as follows: "*whether the PSU received "no match" as reply for the Verification of Payee*". DK (MS comments): We do not have any objections to the amendments to the examples. However, as previously mentioned, we do not support a list of gross negligence, but if other MS wish to include this we can live with a non-exhaustive, non-cumulative list in the recitals of non-binding nature, which the courts can use as inspiration if they decide to. DE (MS comments): In general, we share the view that a non-exhaustive, non-cumulative and non-binding list of criteria to be considered when assessing gross negligence could be useful and promote uniform application in all MS. Courts should take those criteria into account at their discretion when evaluating negligence in accordance with national law, but should **not be bound** by them when the individual circumstances of the case at hand call for a different evaluation. The list should focus on scenarios which occur regularly and are readily ascertainable (e.g. in terms of usual means of evidence). As to the proposals in Option D:

	- the first part of (e) (means and strategies constitute a new type of fraud) is, in our view, already included in (b) (innovativeness) - (g): in German law negligence is assessed not in an entirely subjective way, but by regarding a certain group of people objectively (e.g. the level of care might be different between different groups of people (e.g. a layperson and a policeman involved in the investigation of bank fraud cases), but not for each person individually (e.g. it would not be considered that the specific person (e.g. policeman) has e.g. less knowledge, is younger…). This should be kept in mind/clarified. We consider the other proposals (b – j) the right way forward. CZ (MS comments): We do not agree. The decision about the concept of gross negligence should be completely left on the decision of national courts/ADR bodies. We are open to some examples in recitals, but definitely not in operative text. CY (MS comments): We place a negative scrutiny reservation on referring to gross negligence in the PSR. Should such a reference be made, it must be accompanied by a clear provision that national legal frameworks and court rulings on the matter should be respected. BG (MS comments): We agree with the Presidency's proposal.

Do you have any additional proposals on how gross negligence could be covered in PSR?	AT (MS comments): We support the work of the BE PCY on this topic and do not deem any additions necessary. ES (MS comments): As stated above, we consider that the concept of gross negligence is key to allocation of liability, and, as such, it should be part of the provisions in the law. SI (MS comments): / SE (MS comments): No. RO (MS comments): No. PT (MS comments): (see last answer bellow) NL (MS comments): - LT (MS comments): No additional proposals. IT

	(MS comments): **IT**. No. HR (MS comments): No DK (MS comments): It should not be. Gross negligence plays a very important role since if PSUs act with gross negligence the PSP should not be liable. However, we believe that this should be up to the courts to assess. CZ (MS comments): If the wording of Article 49(2) BE/HU proposal would be adopted, it should be also limited by the gross negligence of the PSU (it is currently not the case in the BE/HU proposal). CY (MS comments): We place a negative scrutiny reservation on referring to gross negligence in the PSR. Should such a reference be made, it must be accompanied by a clear provision that national legal frameworks and court rulings on the matter should be respected.

Would you support to give a mandate to the EBA to issue guidelines on gross negligence as in the EP's proposal (option E)?	AT (MS comments): No, as this issue relates to questions of civil law, not supervisory law. ES (MS comments): No, in our view delimiting the concept of gross negligence is crucial for a balanced liability regime and should be kept at co-legislators level. SK (MS comments): We are open to consider such mandate. SI (MS comments): / SE (MS comments): No, we strongly oppose this. It is not suitable to define a civil law concept in level 2 regulation. RO (MS comments): Yes, we support this approach as to it would give flexibility to update eventually the guidelines based on innovative and complex fraud scenarios and also on lessons learned. PT (MS comments): We support the suggestion advanced by the EP (option E) that mandates the EBA to describe a list of situations – merely examples and not legally binding in respect of each MS national law – that could provide for some guidance on what constitutes gross negligence. This approach would have the advantage to be more flexible, as it is easier to change Guidelines, an aspect particularly relevant due to the constant evolution in this field. The EBA should be

	enabled to share centralized information on new types of fraud identified at a national level, as well as what, in their view, qualifies as 'gross negligence' in specific cases. Such an approach would promote a harmonized supervision. In our view, introducing a definition of 'gross negligence' in PSR itself would pose significant challenges as MS would have difficulties agreeing on a universal definition of 'gross negligence' due to potential variations in national laws. This definition inherently involves a case-by-case analysis, with the burden of proof being a crucial factor. Therefore, we believe that the proposal should not only retain the traditional definition but also provide additional guidance. This guidance should introduce a principle-based approach, avoiding the listing of examples in the context of the PSR, which, in our understanding, will never be unequivocal and will become easily outdated. That additional guidance would also be achieved with the introduction of examples of gross negligence in the context of EBA Guidelines, as referred before. NL (MS comments): We do not think this is necessary, but do not oppose this. LV (MS comments): If clarification on gross negligence is included in recitals and there is a list in annex, than we do not see a necessity for a guidelines, but otherwise for more clear understanding we could support EBA mandate. LU (MS comments): No, we should avoid adding a further layer of complexity via additional EBA mandates. This might also be in contradiction with national case law. LT (MS comments): Yes, probably the best way to give guidance on how the concept of 'gross negligence' should be interpreted is lay out criteria in the guidelines. On the other hand, we also think that such guidelines, in case impersonation and other type of APP frauds are regarded as 'unauthorised' or reimbursable, could entail a detailed description of 'duty of care', that PSUs would be expected to fulfil.

	IT (MS comments): **IT.** We do not have strong objections against the proposal. However, we point out that the criteria to assess "gross negligence" may differ between MSs (e.g. due to different social situations; the most common types of fraud; the degree of digital literacy; etc.) In any case, case law should probably play a more important role than abstract and general guidelines. IE (MS comments): We could support an EBA mandate here to ensure consistency in application HR (MS comments): We would support to give a mandate to the EBA to issue guidelines on gross negligence, but as already mentioned above, we do not support option E. FI (MS comments): FI: No. DK (MS comments): No. We would be strongly against this. This should be left for the courts to decide. DE (MS comments): As under PSD2, the degree and evidence of negligence should generally be evaluated according to national law by the court which is confronted with the case at hand. Whether the PSU acted negligently and to what degree is primarily a civil law question. EBA should not be mandated.

	CZ (MS comments): No. CY (MS comments): We place a negative scrutiny reservation on referring to gross negligence in the PSR. Should such a reference be made, it must be accompanied by a clear provision that national legal frameworks and court rulings on the matter should be respected. BG (MS comments): We believe that the concept of gross negligence should continue to be interpreted in accordance with national law because gross negligence falls entirely in the remit of the national courts.
Additional remarks	

Please kindly provide any other comments, explanations which did not fit in the above questions, but you consider them as important.	ES (MS comments): We have no further comments. SI (MS comments): / NL (MS comments): - LT (MS comments): No additional remarks. IT (MS comments): **IT.** We are in favour of introducing **more clear rules on the procedure** to be followed by the PSP when assessing the PSU's refund request, in order to avoid a protracted period of uncertainty between the parties. See our preliminary drafting proposal of art. 56 PSR in the "HU PCY drafting suggestions on art. 49-84" following the WP of last 26 november. We also think it important to evaluate the introduction of a **rule on "contributory negligence",** which could help to make the liability system more flexible and balanced (the PSD2 leans towards an on-off liability mechanism). For example, in cases where the PSU has been grossly negligent but the PSP is also at fault (e.g. obviously suspicious transaction not intercepted; lack of real time alert, if introduced in the PSR; lack of information to the PSU about new types of fraud, etc.), then it would be possible that the refund to the PSU may be reduced. The extent of this reduction would be left to the prudent assessment by the court/ADR, in the individual case, of the respective faults of the parties and their causal contribution to the harmful event.

	In Italy, such a mechanism has been widely applied with positive results. IE (MS comments): Regarding the fight against payment fraud, as we have noted previously, we would suggest that the whole value chain, including the role of ECSPs, should be examined. All actors relevant to social engineering fraud, including ECSPs, need to at least be part of the discussion on how best to tackle and address the consumer detriment caused by payment fraud. We also note that that fraud and liability remain open issues for the file, and look forward to continuing productuve discussions moving forward. DK (MS comments): **Preference for combination of options C and D and with some elements option F):** Generally, we support the BE PCY proposal for article 49 while some of the supporting articles from option D could be added. However, we do not support article 49 in option D. We would not support moving the last part of article 49(2) into the recitals as we believe that it makes sense to have this explicitly mentioned in the article which covers unauthorized payments. From the UK – along with some of the options already included in option D – we can also support that in case of romance or investment scams the transaction should be deemed as unauthorised. **Extra category to authorised/unauthorised:** It could be considered to add a third category to the current two in article 49. We would support adding a new category for impersonation fraud so instead of just having two categories (authorised and unauthorised), we would have three categories: • 1) Authorised and authenticated. • 2) Unauthorised but authenticated. • 3) Unauthorised and unauthenticated. In category 1 there would be no question of liability since the payment was authorised and authenticated.

	In the second category we would have the impersonation fraud. Here, the PSP would be liable but e.g. claim excess and caps could apply but generally the PSP would be liable. The liability could also be shared by the PSPs. However, in category 3 the payer's PSP would be fully liable – no caps, no claim excess, and no shared liability. **Definition of consent (SE non-paper):** Denmark is in favour of a principle-based approach in regard to liability and fraud fighting in general – due to the dynamic nature of this topic. We agree with the problem identification in the Swedish non-paper for the current liability regime, and we agree that we should aim for a fairly wide scope, including cases where social engineering fraud has taken place. In such cases the PSU should be eligible for a refund. Regarding the Swedish drafting suggestion, we generally support it. Firstly, we believe the right way forward is to try to make a workable definition. Thus, we would be most open to a combination of amending both the articles and recitals. We thereby appreciate the suggestions for both. Regarding the use of the word ”misled” in the drafting of both the recital and article. We would prefer the word “manipulated” instead, which SE also indicated their openness to at the WP. The word ”manipulated” was also used by the BE presidency in their discussion note in June in the drafting for a new art. 49(2) which we support, and thus would prefer an alignment of the wording between the two. Regarding the proposed wording for the article, we would prefer to include the wording from the recital ”with regard to the amount of the payment transaction or the payee” in the article as well. However, as mentioned we generally support the additions in both the recital and the article. **Additional fraud preventing measures:** We believe that when we extend the liability for PSPs, we also need to give them better tools to mitigate fraud risks.

	This is important for our support for extending the liability in general. In some cases, we might extend liability to cases where it would be difficult if not impossible with the current rules for the PSPs to do anything about the specific fraudulent transactions. Thus, we need to actually give them the appropriate tools to combat fraud if we want to extend possible liability to further cases than today. These tools could include better abilities to 1) share information 2) block transfers of funds (for the payer's PSP) and 3) freeze funds (for the payee's PSP). **Freezing of funds:** Denmark would like to propose that also the payee's PSP should have additional tools available to prevent fraud. When a transfer of funds has taken place, it should be possible for the payees PSP to freeze those funds if there is a reasonable suspicion of fraud – either if the payee's PSP suspects this themselves or if the payee's PSP is contacted by the payers PSP. This would allow a transfer to go through to the payee but would still give time for the PSP to investigate immediately of fraud was involved. It would be especially important to give these extra tools also to the payee's PSP in case we decide to expand liability to be shared between the payer's and the payee's PSP. Drafting for new article 69(2a) to allow freezing of funds: "*If the transaction monitoring mechanisms, c.f. article 83, indicates reasonable grounds to suspect a fraudulent payment transaction from either the payer's payment service provider or the payee's payment service provider, then the payee's payment service provider can postpone making the funds available to the payee. If the potentially fraudulent payment transaction is identified by the payer's payment service provider either through the transaction monitoring mechanism or by being contacted by the payer, the payer's payment service provider can contact the payee's payment service provider and share the reasonable grounds for its suspicion in order for the payee's payment service provider to postpone making the funds available to the payee. The payee's payment service provider shall without undue delay as necessary uncover whether the transaction is in fact fraudulent and either make the funds available to the payee or, if the transaction is deemed fraudulent, return the funds to the payer's payment service provider*."

	Spending limits (article 51): We support the amendments for article 51. We agree that the PSPs should be obliged to offer the PSUs the possibility to make use of spending limits. However, while we do support the amendments which has been made, we have some additional comments For instance, how should the spending limit be understood? Should it be a daily spending limit or a transaction-based spending limit? For now, it looks like it is only a transaction-based spending limit, but, for instance, if a fraudster tries to trick someone into transferring them money, they probably don't care if they can get 10,000 euros at once if they can just convince the victim to make two transfers of 5,000 euros instead. We believe both a daily and a transaction-based spending limit should be included. **Cooling off-period**: Denmark also believes that the PSP should be obliged to offer a cooling off period. As we read the last sentence of article 51(1) it would be relatively easy for a fraudster to convince their victim to change their spending limits and then afterwards transfer a larger sum of money. Thus, we believe that the PSP should be required to offer a cooling off period – which the PSU can of course decide if they want to make use of or not. **Transaction monitoring**: We believe that transaction monitoring should be both a requirement for the payer's and the payee's PSP. However, we are generally opposed to a prescriptive set of data that should be used in transaction monitoring. We would much prefer a framework requirement that allow individual PSPs to implement a transaction monitoring mechanism that works best for them in their particular situation. This would also be more future proof as it would not require and update of PSR to add new data points. Alternatively, we could support mandating EBA to make this list which could provide for a bit more flexibility than a level 1 review. **Information sharing**: We are very supportive of extending the possibilities for sharing information.

	However, we do fear that making an explicit list could quickly become outdated. We see how fraud has evolved since PSD2 and there is no reason to believe that it will stop evolving. Therefore, we believe that the best and most futureproof way to go would be the more principle-based approach and to allow the sharing of all relevant information. The current list should either be made non-exhaustive or be moved to the recitals. We believe that the drafting for article 83 (1a) and (1b) and (2) provides adequate safeguards for extending the possibilities for sharing information further than what is on the table right now. Alternatively, we could support mandating EBA to make this list which could provide for a bit more flexibility than a level 1 review. DE (MS comments): As we have already laid out, we would strongly suggest a prohibition for the PSU to set off any claims the PSP might have against the PSU stemming from the same payment transaction. For example, if the PSP has justified grounds for suspecting gross negligence on the side of the PSU, the PSP could have a counterclaim for compensation for the entire loss, which he should not be able to set off against the PSUs claim. We already suggested corresponding wording to be added in Art. 56. CZ (MS comments): The questionnaire left only limited space for support of other options than C or D. Therefore, we have to highlight that for us, **option A** (the PSD2 approach) with regard authorised and unauthorised transaction **is the only option**. We are, however, open to some elements of other proposals. **We have never supported Article 59 PSR and we also do not support new Article 49(2) PSR of BE/HU proposal**.

	CY (MS comments): We have no further comments to add.