Council of the European Union
General Secretariat

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

Brussels, 24 April 2025

WK 5226/2025 INIT

LIMITE

EF
ECOFIN
CODEC

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Financial Services and the Banking Union (Payment Services/ PSR/PSD) Financial Services Attachés
Subject:	Presidency Discussion Note on fraud-related issues in the Payment Services Regulation (authorisation, liability, gross negligence, cooperation with ECSPs)

POLAND25.EU

Polska Prezydencja w Radzie UE
Polish presidency of the Council of the EU
Présidence polonaise du Conseil de l'UE

Payment services package proposals (PSD3/PSR)
Brussels, 29 April 2025

Presidency Discussion Note
on fraud-related issues in the Payment Services Regulation
(authorisation, liability, gross negligence, cooperation with ECSPs)

Authorisation

In the written comments submitted to the Presidency following the 4 April CWP, the majority of Member States expressed a willingness to accept the direction of the latest amendments proposed by the Presidency, but were in favour of retaining the content of Article 49(2) in situ rather than moving it to the recitals. Those Member States argued that a mere reference in a recital lacked the appropriate legal backing that the provision should have, in particular given that it represents a change in approach compared to the current PSD2 framework. The Presidency noted the same high level of support for replacing the words '*initiated or modified*' with the words '*carried out*', which according to some Member States would introduce a well-defined, clear and balanced concept of authorisation. Three Member States pointed out that Article 49(7) should specify that the consent of the PSU to execute a payment transaction may be withdrawn by the payer at any time, *but no later than the moment of irrevocability in accordance with Article 66 PSR*, as such a reference exists in Article 64(3) PSD2. Those Member States argued that, if done otherwise, this would make it possible for a PSU to withdraw its consent even after the moment of irrevocability of the payment order, which would lead to significant difficulties and increased legal uncertainty. In addition we also propose to delete first paragraph of Recital 69a, as it seems too unclear after recently proposed changes to authorisation.

See the proposed wording in Recital 69a and Article 49(2) and (8) PSR in the Annex

Liability

On the basis of Member States' written comments following the 4 April CWP, the Presidency noted that opinions were quite divided on whether to refer to bank employee impersonation fraud in a more precise or more general way (i.e. without specifying the different elements of fraud). However, it appears that most Member States are inclined to favour a more general approach in order to make it future-proof. In an attempt to reconcile the two diverging views, the Presidency proposes to delete specific elements of fraud from Article 59(1), while at the same time mentioning them as examples in Recital 80a. The Presidency hopes that this approach will constitute a compromise that could be acceptable to Member States. Also in Article 59, in line with one Member State's comment, we have tried to clarify, by changing the wording, that once the PSU has become aware of a fraud, the obligation to report it without undue delay arises (and not the other way round). A few Member States pointed out that the current wording gives the impression that it has to be the actual website or mobile application of the PSP that a fraudster uses to impersonate a bank employee, which is rarely the case, and requested a clarification in the recitals that fake ones created by fraudsters (in an attempt to mirror the genuine channels) would also fall within the scope of the provisions.

As in the 4 April CWP, the vast majority of Member States, in their written comments, were also opposed to shifting the obligation to report a fraud to the police from the PSU to the PSP. Those Member States argued that such a shift would not be legally sound, and that the PSU, as the victim of the fraud, is in possession of all the relevant information and is therefore better placed to report the fraud to the police. However, in order to take into account financial inclusion concerns, some Member States suggested considering an obligation for the PSP to assist the PSU in reporting a fraud to the police. In addition, one Member State suggested changing the order of the wording of Article 59 and Recital 80a, so that the PSU's obligation to notify its PSP is mentioned first, followed by the obligation to report the fraud to the police, which would better reflect the urgency of informing the PSP before reporting to the police.

See the proposed wording in Recitals 79 and 80a and in Article 59(1) PSR in the Annex

In order to refer to all the proposals presented during the 4 April CWP, the Presidency would like to clarify that the proposed amendment to Article 60(1) (concerning the powers of the dispute resolution bodies and NCAs to reduce the liability of the payer) has been accepted by the vast majority of Member States. To that end, the Presidency considers that the text of Article 60(1) has been agreed.

Gross negligence

Although the majority of Member States welcomed the Presidency's approach to removing specific examples of gross negligence from Recital 82, some were concerned about the proposed new wording, which also deleted many criteria. Those Member States requested the reintroduction of some of the recently deleted criteria, such as the characteristics of the PSU or the warnings sent by the PSP, in order to provide some guidance in the assessment of the gross negligence, without prejudice to the case-by-case basis, and so as to ensure a minimum degree of harmonisation in the application of the concept of gross negligence. In addition, some Member States pointed out that the new proposed wording no longer makes it clear that the criteria are non-binding, and suggested reinstating the words '*This list is not exhaustive and does not prejudice the discretion of national courts and/or ADR entities. The circumstances as mentioned are not cumulative and are not binding.*' In line with certain comments made during the meeting, the Presidency also reintroduced the example of gross negligence, which had been present in the Commission's proposal and in PSD2, as it did not give rise to any further problems.

See the proposed wording in Recital 82 in the Annex

> ***Q1.*** *Could Member States accept the proposed approach with regard to authorisation, liability and gross negligence?*

Obligation for ECSPs and PSPs to collaborate

On the basis of the written comments from Member States following the 4 April CWP, the Presidency was able to conclude that the proposed new Article 59a on cross-sectoral cooperation was considered by many Member States to be a step in the right direction. However, a few Member States questioned the need to introduce Recitals 81b to 81f, arguing that they merely refer to other EU legal acts which would apply without prejudice to the PSR. In response, the Presidency would like to explain that those recitals serve to clarify rules already laid down in Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive (EU) 2000/31/EC (Digital Services Act), as well as to link them to the context of fraud (in particular, for the purpose of risk assessment and mitigation measures).

Some Member States requested the further alignment of Recital 81 with the wording of Article 59a, so as to impose on providers of electronic communication services an obligation (rather than an option) to cooperate. One Member State suggested further aligning the scope of those provisions (as the scope of Article 59a includes all types of fraud as well as preventive measures), and introducing a distinction between different ECSPs in the service chain. Another Member State stressed that the provision contained in Article 59a(1) does not cover network-internal measures by ECSPs (without the involvement of PSPs). A few Member States considered that the specific provision contained in Article 59a(2) had little added value, as it seemed to only repeat the relevant mechanisms as provided for in the DSA, and suggested that it be moved to the recitals.

A new Recital 81g was proposed in order to clarify a possible mechanism for processing communications and the related traffic data in order to prevent fraud. Some Member States did not support the wording of Recital 81f as proposed by the Presidency, pointing out, for example, that there should be more clarity on how the involvement of competent authorities on a 'case-by-case' basis should work in practice in order to avoid reducing the effectiveness of certain measures, or pointing out that the proposal seems to go beyond cases where numbers are used without or in violation of number usage rights, e.g. spoofing, where the blocking of numbers should be a possible measure to be taken by ECSPs to fulfil their legal obligations in this regard.

One Member State requested clarification that multilateral dedicated communication channels would fulfil the requirement of Article 59a(1), i.e. not all ECSPs would have to have their own communication channel, but a channel involving several ECSPs would also be acceptable. That same Member State

also suggested two amendments to Article 91(5)(a): the addition of the words '*insofar as permitted by national law*', as the processing of communications data is subject to conditions, inter alia, under the ePrivacy Directive 2002/58/EC and the national laws transposing it, and Member States may also have other laws governing the processing of such data which should be taken into account when processing them. The second amendment, changing the words '*could be relevant*' to '*necessary*', as the powers to obtain information also concern personal data, is intended to ensure consistency with Article 5(1)(c) GDPR on data minimisation.

In relation to Article 59a, Article 59(5) seemed to have less added value as it referred only to the type of fraud mentioned in Article 59(1), and the Presidency has therefore decided to delete it. Furthermore, the Presidency proposes to extend the review referred to in Article 108 to include the role played by other entities, such as payment service providers and intermediary service providers, as the current wording of the proposal may be too limited and may not allow for a full assessment and possible effective changes, if it only considers the effectiveness of ECSPs.

Finally, a few Member States questioned the new definition of ECSPs falling under the providers listed in Article 2(4)(a) and (b) of Directive (EU) 2018/1972 (on the European Electronic Communications Code). Those Member States argued that the introduction of measures for all providers of internet access services covered by Article 2(4)(a) of that Directive would mean the imposition of an administrative burden, which was contrary to the current policy of the European institutions. It was emphasised that the PSR should not impose additional obligations on SMEs, as most fraud-related issues occur on very large online platforms and search engines. It was therefore suggested that the definition of ECSPs could only refer to Article 2(4) letter (b) of Directive (EU) 2018/1972.

See the proposed wording in Recitals 81, 81a, 81b, 81f, 81g, and Articles 59 (5), 59a, 91(5) and 108(1b) PSR in the Annex

Q2. *Could Member States accept the proposed wording of the above-mentioned provisions?*

Q3. *Would Member States support limiting the definition of ECSPs only to Article 2(4) letter (b) of Directive (EU) 2018/1972?*

Annex (the newly introduced amendments are highlighted in RED)

Recital 69a

(69a) ~~Authorisation is based on an intention or a contribution in fact. If the payment service user uses its security credentials in a responsible manner when executing a payment transaction, the validity and authenticity of the authorisation will be easier to assess. The set of payment transactions can be divided into two distinct categories, those that are considered authorised and those that are not, called unauthorised. The payment transaction operates as a process and requires the active participation and approval of the payment service user.~~

A payment transaction or a series of payment transactions should be assessed as authorised only if the payer has given its consent for the execution of the payment transaction in a manner agreed on between the payer and the account servicing payment service provider. It should not be deemed to be authorised where the transaction was carried out ~~initiated or modified~~ by a third party who is acting without the consent of the payment service user, e.g. where the third party is using the personal security credentials of the payment service user fraudulently obtained.

Recital 79

(79) Consumers should be adequately protected in the context of certain fraudulent payment transactions that they have authorised without knowing these transactions were fraudulent. The number of 'social engineering' cases where consumers are manipulated ~~misled~~ into authorising a payment transaction to a fraudster has significantly increased in recent years. 'Spoofing' cases where fraudsters pretend to be employees of a customer's payment service provider and misuse, for example, the payment service provider's name, e-mail address, ~~or~~ telephone number, website or mobile application to gain the customers' trust and trick them into carrying-out some actions, are unfortunately becoming more widespread in the Union. Those new types of 'spoofing' fraud are blurring the difference that existed in Directive (EU) 2015/2366 between authorised and unauthorised transactions. Means through which the consent may be assumed to be granted are also becoming more complex to identify, as fraudsters can take control of the whole consent and authentication process including of the strong customer authentication completion. The conditions under which the customer authorised a transaction by giving his or her consent ~~permission~~ to it should be taken into due consideration, including by courts, to qualify a transaction as being authorised or unauthorised. A transaction may indeed have been authorised in circumstances where such authorisation was granted on manipulated premises affecting the integrity of the consent ~~permission~~. It is therefore no longer possible, as was the case in Directive (EU) 2015/2366, to limit refunds to unauthorised transactions only. It would however be disproportionate and financially very costly to payment services providers to open every fraudulent transaction, authorised or unauthorised, to a systematic refund right. It might also cause moral hazard and a reduction in the customer's vigilance.

Recital 80a

(80a) Cases of bank employee impersonation (spoofing) fraud affect the good repute of the bank financial entity, of the banking financial sector as a whole and may cause significant financial damages to Union consumers, affecting their trust in electronic payments and in the banking financial system. A ~~good-faith~~ consumer who has been the victim of such manipulated transactions, namely 'spoofing' fraud, where fraudsters pretend to be employees of a customer's payment service provider and misuse, for example, the payment service provider's name, e-mail address, ~~or~~ telephone number, website or mobile application, should therefore be entitled to a refund of the full amount of the fraudulent payment transaction from the payment service provider on a shared-damage basis, unless the payer has acted fraudulently or with 'gross negligence'. Where the fraud concerns the payment service provider's website or mobile application, the refund right should encompass both the appropriation of those channels by the fraudster and fraudulently created versions of the website or mobile application that mirror the contents of the real ones. As soon as the consumer becomes aware that he or she has been a victim of that type of spoofing fraud manipulation, the consumer should without undue delay report the incident ~~to the police, preferably via online complaint procedures, where made available by the police, and~~ to his or her payment service provider, providing ~~and provide~~ the payment service provider with all the relevant information requested by it, ~~the payment service provider~~ and that the consumer ~~payment service user~~ can reasonably be expected to have regarding the events leading to the disputed payment transaction~~, providing supporting evidence ,~~ and to the police, preferably via online complaint procedures, where made available by the police. No refund should be granted where those procedural conditions are not fulfilled. Given that especially vulnerable consumers may have difficulties in reporting the fraud to the police in a timely manner, payment service providers are encouraged to assisst the consumer in such reporting, where necessary. Although the payment service provider may have perceived the payment transaction as authorised, the customer was the victim of a fraud, so in order to establish customer protection and maintain trust in the financial system, a ~~properly designed~~ damage sharing framework can ensure a real balance between the interests of the consumer and the payment service provider in such manipulation cases. Without prejudice to the right of customers to bring action in courts, the rules of refunds based on shared compensation between the payer and the payment service provider can only be considered as a temporary (preliminary) measures ~~way~~.

Recital 81

Given their obligations to safeguard the security of their services in accordance with Directive 2002/58/EC of the European Parliament and of the Council and Directive (EU) 2022/2555 of the European Parliament and of the Council, publicly available electronic communications services providers have the capacity to contribute to the collective fight against fraud, including 'spoofing' fraud. The extent of such capacity differs between different electronic communications service providers, and is dependent on their position in the service chain. Therefore, and without prejudice to ~~the obligations laid down in national law implementing that Directive~~ those Directives, electronic communications services providers should implement preventive and responsive measures and cooperate with payment service providers with a view to preventing further occurrences of ~~that type of~~ fraud, including 'spoofing' fraud. This cooperation should ~~could~~ include establishing dedicated communication channels for the sharing of relevant information, or participating in a system for effective communication, or in an information-sharing mechanism, in order to facilitate fraud prevention and detection in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC.

Furthermore, providers of electronic communication services should ~~could~~ also assist the fight against fraud by exchanging with payment service providers fraud scenarios, trends and threats identified in relation to the use of their services, as doing so may help to improve the effectiveness of transaction monitoring mechanisms and the educational campaigns and training on fraud implemented in accordance with this Regulation and without prejudice to Directive 2002/58/EC. ~~Therefore, and without prejudice to the obligations laid down in national law implementing that Directive, electronic communications services providers should cooperate with payment service providers with a view to preventing further occurrences of that type of fraud, including by acting promptly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC. Any claim by a payment service provider against other providers, such as electronic communications services providers, for financial damage caused in the context of this type of fraud should be made in accordance with national law.~~

Recital 81a

(81a) In view of the increasing role of electronic communications services providers in the transaction chain, the Commission should review the impact of the newly adopted provisions contained in Article~~s 59 and~~ 59a in relation to obligations imposed on electronic communications services providers. The review should ~~take place~~ be carried out a sufficient amount of time after the entry into force of those provisions ~~e above-mentioned legislations~~. The Commission's report based on this review should, in particular, assess the risks and challenges posed by these ~~this~~ obligations ~~in view of~~ as regards the effectiveness of the cooperation between electronic communications services providers and payment service providers under Article~~s 59 and~~ 59a. On the ~~grounds~~ basis of this assessment, the Commission should ~~conclude~~ determine in its report, whether it is necessary to introduce any further measures regulating the involvement of electronic communications services providers, payment service providers or providers of intermediary services,~~' involvement~~ in~~to~~ the security of payment transactions at EU level and, if appropriate, submit a legislative proposal together with the report.

Recital 81b

Regulation 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) lays down fully harmonised rules on the provision of intermediary services in the internal market and on specific due diligence obligations tailored to certain specific categories of providers of intermediary services ('mere conduit', 'caching' and 'hosting' services). In particular, it imposes specific due diligence obligations on online platforms and online search engines, including those designated as very large online platforms or very large online search engines. Such due diligence obligations play an important role in preventing the proliferation of illegal content online, such as financial scams. For instance, hosting services providers are obliged to put in place user-friendly notice and action mechanisms to allow the reporting of illegal content, such as illegal offers of financial services or attempted fraud, to the hosting service. Online platforms are also obliged to address notices from trusted flaggers as a priority. Payment service providers ~~may~~ should also be able to make use of the notification mechanisms referred to in Article 16 of Regulation (EU) 2022/2065 to notify providers of hosting services of the presence on their service of specific items of information that they consider – including on the basis of notifications received from payment service users – to be illegal content within the meaning of this Regulation. Payment service providers ~~may~~ should therefore also

be able to apply for the ~~to be awarded~~ trusted flagger status pursuant to Article 22 of Regulation (EU) 2022/2065. [moved from Article 59a(2)]

Recital 81f

National competent authorities can play an important role in combating the type of fraud referred to in this Regulation by requiring providers of electronic communications services on a case-by-case basis to block access to numbers or services when fraud is reasonably suspected or once said fraud has been committed using electronic communications services and ascertained by a competent authority. In such cases, ~~If a~~ national competent authorities~~yhas ascertained the occurrence of the type of fraud referred to in this Regulation, they~~ may, on an ad hoc basis or on the basis of guidelines issued by national competent authorities, require providers of public electronic communications networks or publicly available electronic communications services to block access to numbers or services, in accordance with Article 97(2) of Directive 2018/1972/EU, without prejudice to the ability of providers of electronic communications services to block access to numbers or services in the case of infringements of number usage rights.

Recital 81g [new]

Where provided for in legislative measures adopted in accordance with Article 15(1) of Directive 2002/58/EC, electronic communication service providers may process communications and the related traffic data for the purpose of preventing, investigating and detecting of fraud targeting electronic communications end-users. This could include, for example, with regard to impersonation fraud, the processing of traffic data or communications data in order to prevent or end reasonably suspected fraud.

Recital 82

(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all the individual circumstances of the case. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness, ~~that should be assessed depending on the individual circumstances of the case.;~~ for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties~~.; sharing account credentials with the person without the right of disposal, i.e. is not eligible to use the payment instrument; if the loss of a payment instrument is not reported to the payment service provider immediately after the loss is discovered; 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; 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.~~

When assessing the possible gross negligence on the part of the payment service user, ~~account should be taken, for example,~~ ~~to~~ all the factual circumstances should be taken into account, for example: ~~. For this purpose, one or more of the following circumstances may be taken into account,~~

~~such as the (a) payment service user's behaviour or communication with third parties, where relevant; (ab) of the~~ innovativeness and~~,~~ complexity of the fraud, ~~and the~~ means or strategies used by third parties to illegally take over the payment service user's personalised security credentials; ~~of payment instruments owned by the payment service user~~; ~~(c) innovativeness, complexity of fraud~~; ~~(bd)~~ whether the payment service user has previously fallen victim of the same type of fraud; ~~(ce)~~ in the case of ~~the fraudster's means or strategies constitute~~ a new type of fraud, whether the payment service providers have complied with ~~fulfilled~~ their obligations under Article 84, ~~with particular~~ including with regard to their most vulnerable groups of customers; ~~(df)~~ whether the payment service user has taken adequate steps in order to properly ensure the confidentiality of their personalised security credentials ~~of the payment instruments~~;

~~(eg)~~ any ~~the~~ known characteristics of the payment service user that might make the user more likely to fall victim to fraud~~, for example the user's age, or level of education or profession;~~

~~(fh) in the event that the payment service user used its means of identification, the circumstances, whether and what the payment service user saw in its messages asking to enter its security credential that confirmed the disputed payment or where the payment service user has failed to check if the elements which are dynamically linked and regarding the amount and the payee that were displayed during the strong customer authentication in accordance with Article 85 are correct, and, where the applicable, the circumstances why the payment service user authenticated the payment without having regard to the information displayed during the authentication process;~~

~~(i) whether the personalised security credentials of the payment instrument have been appropriated by third parties, while the payment service user was using the payment instrument according to its purpose;~~

~~(gj)~~ whether the payment service providers offered clear, specific~~concrete~~ and ~~case-specific~~ bespoke warnings ~~against currently used frauds methods that were brought directly~~ to the ~~attention of~~ payer~~,~~ ~~that are transaction specific, and payment service providers actions, taken in order to familiarise the payment service user with the risks and methods of fraud in the electronic space, as well as the meaning and legal consequences of the safe misuse of identification means and payment instruments issued by the payment service user, the disclosure of their personalised security data, etc. the specificity and nature of any intervention made by the sending payment service provider in the payment flow,~~ whether the payment service user failed to have regard to specific, directed interventions made by their payment service provider~~, and whether those interventions offered a clear assessment of the probability that an intended payment was fraudulent.~~

This list is not exhaustive, cumulative or binding and does not prejudice the discretion of national courts and/or ADR entities. ~~The circumstances as mentioned are not cumulative and are not binding.~~

~~The fact that a payment service user consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again victim of the same type of fraud could, depending on the circumstances of the case, be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent *modus operandi*.~~

Article 49 [Authorisation]

1. A payment transaction or a series of payment transactions shall be authorised only if the payer has given its ~~permission~~ consent for the execution of the payment transaction ~~including as regards the amount of the payment transaction and the payee~~. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the account servicing payment service provider, after the execution of the payment transaction.
1a. A payment transaction shall not be deemed as authorised ~~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, or~~ where the transaction was carried out ~~initiated~~ by a third party who is acting without the consent of the payment service user ~~using the personal security credentials of the payment service user fraudulently obtained~~.
2-6. […]
7. The payment service user may withdraw consent ~~permission~~ to execute a payment transaction or to access a payment account for the purpose of payment initiation services, at any time, but no later than at the moment of irrevocability in accordance with Article 66. ~~or~~ The payment service user may withdraw consent to access a payment account for the purpose of account information services ~~may be withdrawn by the payment service user~~ at any time. The payment service user may also withdraw consent ~~permission~~ to execute a series of payment transactions, in which case any future payment transaction shall be considered to be unauthorised.

Article 59 [Payment service provider's liability for impersonation fraud]

1. Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer's payment service provider ~~using the name and or e-mail address or name and telephone number or website or mobile application of that payment service provider unlawfully~~ and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer, when becoming aware of the fraud, has without undue ~~any~~ delay ~~reported the fraud to the police and~~ notified its payment service provider ~~when becoming aware of the fraud~~, providing the payment service provider with all the relevant information requested by the payment service provider and that the consumer ~~payment service user~~ can reasonably be expected to have regarding the events leading to the disputed payment transaction, and reported the fraud to the police ~~providing supporting evidence available to the consumer~~. 2-4 […] ~~5. Where informed by a payment service provider of the occurrence of the type of fraud as referred to in paragraph 1, electronic communications services providers shall cooperate closely with payment service providers and act swiftly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC, including with regard to calling line identification and electronic mail address.~~

Article 59a Cross-sectoral cooperation for the purpose of fraud prevention and detection

1. For the purpose of preventing, ~~and~~ detecting and eliminating fraud, including that referred to in Article 59(1), providers of 'electronic communications services' as defined in Article 2(4), points (a) and (b), of Directive (EU) 2018/1972 shall have in place measures, including measures to ensure effective cooperation with payment service providers, having regard to the technical characteristics of each of their services.
For the purpose of the first subparagraph, without prejudice to Directive (EU) 2022/2555, Directive 2002/58/EC or Article 91 of this Regulation, electronic communications services providers shall establish dedicated communication channels with payment service providers or participate in a system for effective communication, or in an information sharing mechanism, to allow for faster and more effective sharing of any information that could be useful in the prevention and detection of fraud within the meaning of this Regulation and in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC.
~~2. Payment service providers may make use of the notification mechanisms referred to in Article 16 of Regulation (EU) 2022/2065 to notify providers of hosting services of the presence on their service of specific items of information that they consider, including based on notifications received from payment service users, illegal content within the meaning of this Regulation. Payment service providers may also apply to be awarded trusted flagger status pursuant to Article 22 of Regulation (EU) 2022/2065.~~ [moved to Recital 81b]
2.~~3.~~ The Commission and the European Board of Digital Services shall encourage and facilitate the drawing up of a voluntary code of conduct at Union level to foster prevention, enhance security and combat payment fraud and financial scams, under the conditions set out in Article 45 of Regulation 2022/2065.

Article 91 [Competent authorities and investigatory powers]

1-4. […] ~~3~~5. The competent authorities referred to in paragraph ~~4~~2 shall ~~possess~~ have all supervisory and investigatory powers and adequate resources necessary for the ~~performance of their tasks~~ exercise of their functions.
Those powers shall include at least:
(a) in the course of procedures to investigate potential breaches of this Regulation, the power to require, insofar as permitted by national law, ~~from, *inter alia*, the following natural or legal persons, all information necessary to carry out that investigation~~ any person to provide information and documents which the competent authorities consider necessary ~~could be relevant~~ for the performance of their duties, including the following natural or legal persons:
(i) payment services providers;
(ii) technical service providers and payment system operators;
(iii) ATM deployers which do not service payment accounts~~, including providers of intermediary services within the meaning of Regulation (EU) 2022/2065~~;
(iv) providers of electronic communications services as defined in Article 2(4), points (a) and (b), of Directive (EU) 2018/1972 ~~electronic communications services providers within the meaning of Article 59(5);~~
iv(a) providers of intermediary services as defined in Article 3, point (g), of Regulation (EU) 2022/2065, in accordance with Article 10 of that Regulation;

[…]

Article 108 [Review clause]

1b. The Commission shall, at the latest two ~~2~~ years after the date of entry into force of this Regulation, submit to the European Parliament, the Council, the ECB and the European Economic and Social Committee a report on the impact of the provisions contained in Article~~s 59 and~~ 59a in relation to obligation~~s~~ imposed on electronic communications services providers. This report will in particular assess whether those ~~this~~ obligations improve~~s~~ the effectiveness of the cooperation between electronic communications services providers and payment service providers under Article~~s 59 and~~ 59a. On the ~~grounds~~ basis of that~~is~~ assessment, the Commission should ~~conclude~~ determine in its report whether it is necessary to introduce any further measures regulating the involvement of electronic communications services providers, payment service providers ~~'~~or providers of intermediary services ~~involvement,~~ int~~o~~ the security of payment transactions at EU level and, if appropriate, submit a legislative proposal together with the report.