Council of the European Union
General Secretariat

PUBLIC

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

Brussels, 01 September 2025

WK 10772/2025 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:	Presidency
To:	Working Party on Financial Services and the Banking Union (Payment Services/ PSR/PSD) Financial Services Attachés
Subject:	Working Party on Financial Services and the Banking Union (PSD/PSR) 8 September 2025 - Preparatory note for the second PSD3/R trilogue: Fraud

Danish Presidency
Council of the European Union

PUBLIC

Working Party on Financial Services and the Banking Union

Payment services package proposals (PSD3/PSR)

Date: 8 September 2025

Brussels, 8 September 2025

Preparatory note for the second PSD3/R trilogue: Fraud

PUBLIC

1. Fraud and consumer protection

In this discussion note the Presidency will present some differences between the Council and European Parliament (EP) text especially focusing on areas where the EP has introduced amendments differing from the Council text and the Commission's proposal. The aim is to identify potential flexibilities from the Council towards the EP mandate but also to identify concerns which the Presidency in particular should be aware of before entering into trilogues and technical meetings on the topic of fraud.

At the trilogue on the 9th of July it was agreed to proceed with further discussions of the following fraud related topics in upcoming trilogues:

- Impersonation fraud (line 716-722, PSR)
- Electronic communication service providers (line 268b-268d, 723-723d, 723e-723i, 877b, and line 880b-880c, PSR)
- Fraud preventive measures:
    - Verification of payee (line 660-668 and 705-713, PSR)
    - Spending limits, cooling off, blocking payment instruments, mobile phone apps (line 669-673e, PSR)
    - Burden of proof (line 692-695a, PSR)
    - Blocking of transactions (line 765-770 and line 868h, PSR)
    - Freezing of funds (line 790b, PSR)
    - Transaction monitoring mechanism (line 859-874a, PSR)
    - Fraud data sharing (line 875-878g, PSR)
    - Education and awareness (line 879-880a and 881-882a, PSR)

2. Impersonation fraud (art. 59, PSR – line 716-722)

At the trilogue on the 9th of July 2025 it was agreed that impersonation fraud (art. 59) should be further discussed in upcoming political trilogues. Art. 59 is closely linked to art. 49 (line 652 - 659) on authorisation and the EP's suggestion for a definition of authorisation in art. 3(34a) (line 247a). These two articles were not discussed at the kick-off trilogue, but the Presidency is aware of the positions of Member States in this regard.

In art. 59(1) (line 717) the EP suggests that refund rights for impersonation fraud should also cover "*any other relevant entity of a public or private nature*". Several Member States argue that PSPs cannot control the communication between PSUs and other entities and thus rejects the proposal from the EP.

The Presidency would like to consult the Member States on whether flexibility towards the EP's proposal to extent art. 59 can be shown. Specifically, the Presidency would like to consult the Member States on whether art. 59 could be extended to cover impersonation of both

PUBLIC

relevant public or private entities – or to only one of those entities. The EP provides two examples of relevant (public) entities in recital 79 (line 89): "*a relevant entity which could reasonably be linked to a trusted source of the customer, such as a central bank or government authority*". No guidance for relevant private entities is given. Further, if refund rights for authorised transactions are to be extended in art. 59, the Presidency would like to consult Member States on whether further safeguards should be provided in order to meet the concern of the Member States raised above. For example, this could include requiring the entities to which the scope is potentially extended to communicate only in certain ways or through secure channels. It could also involve the use of centralised lists specifying how, or through which email address/phone number an entity would contact citizens. Another possibility could be the requirement of clear identifications in messages being send with digital signatures or QR codes verifying the sender. The Presidency is open to receive suggestions from the Member States regarding which types of safeguards they would deem necessary if the scope of article 59 is to be extended.

Regarding the burden of proof and duty to cooperate, the Council has added requirements at the end of art. 59(1) (line 717) while the EP has added requirements in art. 59(3) (line 721). The Council has suggested that it should be the PSP requesting information and that requirements for PSU documentation should be limited to what the PSU can reasonably be expected to have. The EP has added that PSPs would not have to refund in accordance with art. 59(1) if the consumer refuses to comply with the PSPs investigation or if the consumer refuses to provide relevant information. However, the EP does not specify if the consumer would proactively need to provide relevant information or if it should be the PSP who requests this information.

Lastly, the EP has amended art. 59(2)(b) (line 720) in a way that the interpretation of the article could be that the justification for refusal of a refund should only be sent to the relevant national authority and not the consumer. The Presidency is unsure whether this is actually the intention of the EP since the reasons for rejection of a refund would indeed be very relevant for the consumer to receive. However, the relevance of introducing a mandatory reporting requirement on reasons for refusal to the relevant national authority could be discussed. Initially, the Presidency notices some concerns from a number of Member States to add this requirement. One Member State questions whether the relevant national authority is to be understood as the national competent authority (NCA) or a civil law court. The EP has included the same proposal in art. 56(2)(b) (line 700) on PSP's liability for unauthorised payments.

Q1: Could Member States be open to extend art. 59 to cover impersonation of either public entities, private entities, or both?

Q2: Do Member States believe that further safeguards would be necessary to extend the liability regime in art. 59? If deemed necessary, which further safeguards could Member

PUBLIC

States see as a viable option forward if art. 59 is to be extended to either public entities, private entities, or both?

Q3: Should PSPs be required to report the reasons for refusing to refund PSUs to the relevant national authority in art. 59 (if not otherwise stated, the Presidency will assume the answer is the same in relation to art. 56)

Q4: Do Member States have other comments regarding the EP amendments to the provisions on impersonation fraud?

3. Electronic communication services providers and providers in scope of the Digital Services Act (COM and EP version: art. 59, PSR. EP version: art. 3(55a), art. 83(5b), and 84(1a)(sub-paragraph 1 and 2), PSR. Council version: art. 59a, PSR) – line 268b to 268d, line 723 to 723d, line 723e to 723i, line 877b and line 880b and 880c)

An obligation for electronic communication services providers (ECSPs) to cooperate with PSPs in the event of PSP employee impersonation fraud was included in the Commission's original proposal. Both the Council and the EP have expanded the scope of requirements and specified the entities which they believe should adhere to such requirements. At the trilogue on the 9th of July it was clear that the EP will prioritise bringing online platforms in scope of the PSR to prevent fraud initiated through their platforms.

The Presidency would like to highlight that bringing platforms into the scope of PSR would imply obligations for two different categories of actors: 1) ECSPs (providers in scope of the European Electronic Communications Code[1] (EECC)), and 2) Online platforms (providers within the scope of the Digital Services Act[2] (DSA)). The latter providers are only covered by the Councils current proposal to a very limited extent. These two respective actors have different tools available and are regulated by different pieces of EU legislation. As a result, they also have different requirements to comply with. The Presidency would like to note that depending on the service, some providers may be within the scope of both the EECC and the DSA - for example, web-based email service providers and internet-based messaging services are both interpersonal communication services for the purpose of EECC and mere conduits

[1] https://eur-lex.europa.eu/eli/dir/2018/1972/oj/eng

[2] https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

PUBLIC

for the purpose of DSA. However, for the purposes of this note, the Presidency would like to separate the discussion and thereby the note is structured into two parts, the first part covering providers in scope of the EECC and the second part covering providers in scope of the DSA. While this distinction is not as clear in practice for the reasons mentioned above with a few instances of overlaps, the Presidency believes that it will be beneficial for the discussions to be very clear on which providers we are having in mind for different requirements, liability, etc.

The note will cover: 1) Definitions, 2) requirements, and 3) liability for both categories of providers. Some parts of this note relating to the EP amendments may be repetitive from earlier notes. This is because the Presidency has found it difficult to interpret whether the EP intends for specific requirements to target providers within the scope of the DSA, the EECC, or both.

3.1 ECSPs (Providers in scope of the EECC)

3.1.1 ECSPs: Definition (EP version: art. 3(55a) (line 268b and 268c). Council version: art. 59a(1) – line 723d)

While both the EP and the Council refer to ECSPs, the definitions include different actors.

In the EP text reference is made to any provider that falls within the scope of the EECC (and of the DSA but this will be treated in section 3.2 of this note), while the Council has narrowed the definition to encompass only a specific type of provider. Consequently, in the EP text all providers of the services listed in table 1 below are proposed to be in scope of the PSR, i.e., all providers of electronic communications services.

In the Council version reference is made only to a subcategory of providers of electronic communications services. Here, only providers of services in art. 2(4)(b), EECC, are within scope of the PSR. Thus, in the Council text, art. 59a PSR only applies to providers of interpersonal communications services as defined in art. 2(5) of the EECC and which covers both number-based and number-independent interpersonal communications services as defined in art. 2(6) and 2(7), EECC.

The Presidency acknowledge that the Council mandate is a result of extensive discussions. The Presidency intends to defend the Council position by only referring to the providers of interpersonal communications services in the upcoming trilogue.

PUBLIC

Table 1: Different providers in scope of the European electronic communications code

CATEGORY	SUBCATEGORY	DEFINITION IN THE EECC
ELECTRONIC COMMUNICATIONS SERVICES *(ART. 2(4))*		(Umbrella term covering all services within scope of the EECC) 'electronic communications service' means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services: (a) 'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120; (b) interpersonal communications service; and (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting;
INTERNET ACCESS SERVICE *(ART. 2(SUBPARAGRAPH 2, POINT 2) OF REGULATION (EU) 2015/2120[3])*		'internet access service' means a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used.
INTERPERSONAL COMMUNICATIONS SERVICE *(ART. 2(5))*		'interpersonal communications service' means a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service;
	Number-based interpersonal communications service *(art. 2(6))*	'number-based interpersonal communications service' means an interpersonal communications service which connects with publicly assigned numbering resources, namely, a number or numbers in national

[3] https://eur-lex.europa.eu/eli/reg/2015/2120/oj/eng

		or international numbering plans, or which enables communication with a number or numbers in national or international numbering plans;
	Number-independent interpersonal communications service *(art. 2(7))*	'number-independent interpersonal communications service' means an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans;
ART. 2(4)(C)		services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting;

3.1.2 ECSPs: Requirements

An obligation for ECSPs to cooperate with PSPs in case of PSP employee impersonation fraud is included in the Commission's proposal. Further, ECSPs shall, when informed about such PSP employee impersonation fraud, "*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*" (line 723).

Both the Council and EP texts expand the obligations in relation to combatting fraud to cases of not only PSP employee impersonation fraud but to fraud more generally (lines 723c and 723d). In the EP text the requirement for ECSPs to cooperate closely with PSPs is extended to cover not only cases of PSP employee impersonation fraud but also both impersonation of relevant public or private entities. This is due to the reference in art. 59(5) (line 723) to types of fraud in scope of art. 59(1) which the EP has expanded. Further, line 723c also entails a cooperation obligation in case of APP fraud. In the Council text art. 59a(1) refers to fraud in general.

The Council text includes specific requirements for ECSPs to establish or participate in communication channels for sharing of information which could help prevent or detect fraud. In addition, the Council text includes a general obligation for ECSPs to have all reasonable measures in place to detect and prevent fraud within their sphere of competence. Lastly, a requirement for the Commission and the European Board of Digital Services are mandated to develop a voluntary code of conduct for ECSPs and providers of intermediary services more broadly (art. 59a (line 723d and 723f to 723i)).

In the EP text, it has been added in art. 59(5) (line 723) that ECSPs shall remove fraudulent and illegal content after being informed of its presence. This is one of the places where the Presidency believes the discussion would benefit from clarifying the exemption from liability set out in the DSA, as well as the obligations of such providers under the DSA and providers

PUBLIC

under the EECC. As one Member State comments, ECSPs (here understood as providers in scope of the EECC) are not able to remove content. However, if the EP intends for the requirement to apply more specifically to providers of hosting services (in scope of the DSA), clarifications are needed. Thus, the Presidency considers it necessary to uncover which providers the EP intends to apply the provisions to.

In art. 59(5a) (line 723a) the EP proposes that ECSPs shall warn their customers of new online scams, how to identify and avoid fraud as well as how to report cases of fraud to the ECSP. This could apply to intermediary providers in a broader sense. Several Member States indicates openness to the proposal while one Member State points out that the wording applies to online platforms but not to telcos. In art. 59(5b) (line 723c) the EP has included an obligation similar to the one in art. 59a(3) (line 723i) in the Council text. Several Member States indicate openness, while other Member States prefer the Council text.

In art. 84(1a)(sub-paragraph 2) (line 880b) the EP has added that *"Payment service providers, in cooperation with electronic communications services providers, shall take adequate prevention and robust technical safeguards to prevent cases where fraudsters replicate and misuse the payment service provider's name, mail address or telephone number for misleading payment service users into making fraudulent transactions."* The Presidency believes that this would relate to providers of services within the scope of the EECC and not the DSA but once again a more precise wording is needed.

In art. 84(1a)(subparagraph 3) (line 880c) the EP seems to have duplicated yet expanded the requirements already included in art. 59(5) (line 723). The only substantial difference seems to be that the requirement in art. 84 is more general whereas the requirement in art. 59 only applies when the ECSP is informed of the occurrence of impersonation fraud cf. art. 59(1) by a PSP. Consequently, art. 59(5) could be interpreted as a reactive obligation while art. 84(1a)(subparagraph 3) could be interpreted as a proactive obligation.

In the Council, there were discussions of more specific obligations. These were met by strong concerns from many Member States who only supported a more general obligation. This is a very technical topic, and the fraudsters methods are quickly adapted. Thus, a less prescriptive and more futureproof approach with a general obligation were included.

3.1.3 ECSPs: Liability

In art. 59(5) (line 723) the EP has added that ECSP's, as broadly defined by the EP, are liable to the PSP for "*the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without any delay, reported the fraud to the police and notified its payment service provider*" if the ECSPs "*do not remove the fraudulent or illegal content, after being informed of its occurrence*". As mentioned above, the Presidency believes it is necessary to clarify whether the obligations are intended for providers of electronic

PUBLIC

communication services in the context of EECC, or also to other intermediaries (e.g., hosting services or online platforms); it could prove technically unfeasible for ECSPs to comply with the requirements proposed by the EP. However, if the mentioned liability is intended for ECSPs, the Presidency believes that this has been discussed in the Council with no support for such extension.

The EP also mentions liability in recital 80 and 81 (line 90 and 91). In these recitals it is clear that the EP proposes liability on e.g. telcos since spoofing is mentioned. The liability on ECSPs is proposed to apply in case of a lack of cooperation with PSPs in the fight against fraud. However, this phrasing is not included in the actual provisions and the wording of the recital seem very broad. Again, the Presidency believes that liability for ECSPs has already been discussed and rejected in the Council.

Q5: Do Member States agree that the definition of ECSPs in PSR should be limited to art. 2(4)(b) of the EECC as agreed in the Council?
(If not, please indicate very specifically what kind of provider should be within scope)

Q6: What kind of general, as well as specific requirements, could Member States support for ECSPs as defined in art. 2(4)(b) in the EECC?
(If Member States indicated a preference above for expanding the definition of ECSPs please indicate what kind of requirements should apply to each specific type of provider).

Q7: Do Member States agree that liability for non-removal of illegal content should not be imposed on ECSPs as defined in art. 2(4)(b) in the EECC?
(If Member States believe liability could be imposed on ECSPs please indicate in which specific situation or a breach of which specific requirements should lead to liability and to what extent for each specific provider).

Q8: Do Member States have other comments related to ECSP's in scope of the EECC?

3.2 Other intermediary service providers within scope of the DSA

Below, the discussion of definition, requirements, and liability for other intermediary service providers in scope of the DSA (e.g. online platforms and online search engines) is laid out. When references are made to ECSPs below, it should be interpreted as places where the Presidency either are unsure whether, or assumes that, the EP had providers in scope of the DSA in mind.

PUBLIC

3.2.1 Other intermediary service providers within scope of the DSA: Definition (EP version: art. 3(55a) (line 268b and 268d).

In the EP text, the scope of the PSR for specific obligations has been extended to also cover providers of services in scope of the DSA. In art. 3(55a) in the EP proposal the definition includes all providers in scope of the DSA and defines these as electronic communications services providers, even though this is not a terminology used in the DSA.

However, the intention of the EP might be to only cover providers of hosting services (and online platforms more specifically). The Presidency assumes, that this might be the case since the only providers within the scope of the DSA whom the EP refers to are hosting services and online platforms (and in one instance to digital platforms but the Presidency assumes the reference was meant to be made to online platforms since digital platforms is not a terminology used in the DSA). In recital 81a (line 91a) the EP explains that online platforms also have a role to play in combatting fraud but makes no mention of other types of providers. Further, e.g. art. 59(5b) (line 723c) and art. 2(9a) (line 209a) the EP uses the wording *"electronic communications services providers and online/digital platforms"*. This could indicate that the EP perceive online platforms as a separate item even though online platforms are already included in their definition of ECSP's in art. 3(55a) (line 268b). However, in other instances references are made solely to ECSPs and it is not clear to the Presidency whether the EP intends for this to include or exclude online platforms, hosting services, and providers of other services in scope of the DSA or only to the providers within the scope of the EECC.

In the table below, the different services within scope of the DSA are listed. In principle, the EP suggests that providers of all the services mentioned should be within scope of the PSR.

In the Council text, providers under the DSA have generally not been proposed to be within the scope of PSR, except from services with potential overlaps between the DSA and EECC as mentioned in the introduction to section 3 of this note. Furthermore, two other exceptions are covered in section 3.2.2 for art. 59a(2) and art. 108(1c)). However, in the recitals, references are made to the DSA in recital 81a to 81e (lines 91a to 91e). In the Council version references are made to providers of intermediary services, hosting services, and online platforms.

Table 2: Different providers in scope of the Digital Services Act

CATEGORY	SUBCATEGORY	DEFINITION IN THE DSA
INFORMATION SOCIETY SERVICE *(ART. 3(A))*		(Umbrella term covering all providers within scope of the DSA)

PUBLIC

		'information society service' means a 'service' as defined in Article 1(1), point (b), of Directive (EU) 2015/1535; Art. 1(1)(b) of directive (EU) 2015/1535[4]: "'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request. An indicative list of services not covered by this definition is set out in Annex I"
INTERMEDIARY SERVICE *(ART. 3(G))*		'intermediary service' means one of the following information society services:

[4] https://eur-lex.europa.eu/eli/dir/2015/1535/oj/eng

PUBLIC

		(mere conduit' service (art. 3(g)(i)), caching service (art. 3(g)(ii)), 'hosting' service (art. 3(g)(iii)))
	mere conduit' service *(art. 3(g)(i))*	a 'mere conduit' service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;
	caching service *(art. 3(g)(ii))*	a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;
	'hosting' service *(art. 3(g)(iii))*	a 'hosting' service, consisting of the storage of information provided by, and at the request of, a recipient of the service;
ONLINE PLATFORM *(ART. 3(I))*		(subcategory to providers of hosting services) 'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation;

PUBLIC

	Very Large Online Platform (VLOP) *(Art. 33(1))*	online platforms which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines pursuant to paragraph 4.
ONLINE SEARCH ENGINE (OSE) *(ART. 3(J))*		'online search engine' means an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found;
	Very Large Online Search Engine (VLOSE) *(Art. 33(1))*	online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines pursuant to paragraph 4.

3.2.2 Providers within scope of the DSA: Requirements

Generally, all requirements made towards ECSPs in the EP version also apply to providers within the scope of the DSA due to the definition in art. 3(55a) (line 268b-268d). In addition, and as already mentioned, there are also instances where the EP refers to specific types of providers in scope of the DSA. This leads the Presidency to believe that the requirements in art. 84(1a)(sub-paragraph 2 and 3) are not necessarily targeted towards providers in scope of the DSA due to the requirements mentioned (but instead to providers in scope of the EECC).

In art. 83(5b) (line 877b) the EP has, however, added a requirement which is specifically addressed towards PSPs implying that PSPs should make use of the notification mechanisms set up in accordance with art. 16 of the DSA, rather than the trusted flaggers framework

PUBLIC

which has been discussed in the Council. Since the trusted flaggers framework proved difficult for the Council to include explicitly in the articles, the concept was included in recital 81b (line 91b). Thus, the Presidency believes that it is worth discussing whether to include the EP's proposal of including an obligation for PSPs to use the notification mechanisms set up under art. 16 of the DSA to notify hosting service providers of illegal content linked to fraud present in their services, in addition to trusted flagger notices. According to this framework (art. 22 DSA), online platforms are required to prioritize notices from trusted flaggers higher than what is required for a regular notification of illegal content from a non-trusted flagger under art. 16 of the DSA. Since it is not possible to oblige PSPs to apply to become trusted flaggers, the requirement proposed by the EP could function as a parallel path to try to achieve the goal of getting fraudulent content removed from online platforms. The Presidency notices that this part of the obligation in art. 83(5b) is on the PSPs – not the hosting services or online platforms (they would, however, have to react within the framework of the DSA).

The EP further proposes in art. 59(5a) (line 723a) that ECSPs should inform customers of new fraud trends and how to report fraud. The Presidency is, however, not aware if the EP intends also to apply this requirement to providers in scope of the DSA.

Lastly, the EP has introduced a requirement in art. 59(5b) (line 723c) that ECSPs and digital platforms (the Presidency assumes the EP means online platforms) should have "*the appropriate organisational and technical measures are in place to safeguard the security of payments users when making transactions. Payment service providers, electronic communications service providers and digital platform service providers shall have in place fraud prevention and mitigation techniques to fight fraud in all its configurations, including non-authorised and authorised push payment fraud*." One Member State points out that the requirements in the EP text overlaps with the DSA (art. 35) while they consider the Council's version better aligned with other parts of the EU legislation.

In the Council, discussions have been held especially in relation to the Irish non-papers on advertisements for providers of financial services on VLOPs and VLOSEs. Here, it was clear from the intervention of the Council Legal Service that further work would be necessary for compliance with the requirement not to impose a general monitoring obligation for providers of intermediary services such as VLOPs and VLOSEs, cf. art. 8 of the DSA.

In the Council no providers under the DSA have been proposed to be directly within scope of the PSR. However, references are made to providers of intermediary services, hosting services, and online platforms. In art. 59a(2) the Commission and the European Board of Digital Services shall facilitate a voluntary code of conduct for prevention of payment fraud for providers in scope of the DSA, and in the recitals, references are made to the DSA in recital 81a to 81e (lines 91a to 91e). The Council has also included providers of intermediary services in the review clause in art. 108(1c) (line 1105f).

PUBLIC

3.2.3 Providers within scope of the DSA: Liability

In art. 59(5) (line 723) the EP has added an obligation which the Presidency assumes applies to providers of hosting services within the meaning of the DSA. Here, the EP proposes that such providers, if they decide not to remove fraudulent content after being notified of its occurrence (which could be through the obligation in art. 83(5b) (line 877) referring to art. 16 in the DSA) should be liable towards the PSP for the full amount of the fraudulent authorised payment transaction. It is not clear to the Presidency whether the proposed liability should cover the fraud which already have taken place or whether it is liability in case of fraud arising from the same content in the future. Further, the first part of the added sentence seems to somewhat duplicate the notice and action systems which already exist in art. 16 of the DSA as well as it somehow overlaps with the trusted flaggers framework which is more detailed. If it is decided to include potential liability for online platforms, the Presidency believes a better approach here would be to refer to the existing provisions in the DSA (e.g. in the same way that the EP do in line 877b) and further, it should as mentioned above be clarified in what instances this liability would arise.

Moreover, in recital 81a (line 91a) the EP clarifies that online platforms "*should be held liable where fraud has arisen as a direct result of fraudsters using their platform to defraud consumers, if they were informed about fraudulent content on their platform that and did not remove it.*" In the DSA there are liability exemptions in art. 4, 5, and 6 for mere conduit, caching, and hosting services respectively. As such, the online platforms are covered by the exemption in art. 6 of the DSA and "*shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider: (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content*".

If the Member States support expanding liability to online platforms in the PSR, the Presidency believes a better option than establishing such liability explicitly in the PSR would be to clarify in PSR under which conditions in the DSA the liability exemption (which for hosting services is included in art. 6 of DSA) is forfeited with regards to art. 16 concerning the notification procedure (as suggested by the EP) and art. 22 regarding the trusted flaggers arrangement (as suggested by the Council). In such case, it could if necessary be clarified in the recitals of the PSR how "*actual knowledge of illegal activity or illegal content"* and "*upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content"* should be interpreted in the DSA from a payment context. In the DSA, the notification system in art. 16 (specifically art. 16(3)) already clarifies that "*Notices referred to in this Article shall be considered to give rise to actual knowledge or awareness for the purposes of Article 6 in respect of the specific item of information concerned where they allow*

PUBLIC

a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination."

Further, if a modified version of the proposal from the Irish non-paper on advertisements for providers of financial services on VLOPs and VLOSEs is included, it could be worth discussing how the question of liability is handled for such requirements including the interplay with art. 26 and art. 29 of the DSA.

Q9: Do Member States have any comments regarding which types of providers in scope of the DSA that could be included in the scope of the PSR?

Q10: Could Member States support a general cooperation requirement for specific providers in scope of the DSA?

Q11: Could Member States support any specific requirements for providers in scope of the DSA? And if so, for which providers? (If legally possible, this could be done by adjusting the content of the Irish non-paper but other suggestions are also much welcomed)

Q12: Could Member States support the EP's suggested reference in art. 83(5b) to the procedure in art. 16 of the DSA?

Q13: Do Member States have any other comments on requirements for providers in scope of the DSA?

Q14: Do Member States have any comments regarding potential liability for providers in scope of the DSA as regards to not removing illegal content?

4. Fraud preventive measures

This section concerns fraud preventive measures which include:

- Verification of payee (art. 50 and 57, PSR – line 660 to 668 and 705 to 713)
- Spending limits, cooling off, blocking payment instruments, installation of mobile phone applications (art. 51, PSR – line 669 to 673e)
- Burden of proof (art. 55, PSR – line 692 to 695a)
- Blocking of transactions (art. 65, PSR and in the EP version art. 83(2)(sub-paragraph 2), PSR – line 765 to 770 and line 868h)
- Freezing of funds (art. 69(2a), PSR – line 790b)
- Transaction monitoring mechanism (art. 83, PSR – line 859 to 874a)
- Fraud data sharing (COM and EP version: art. 83, PSR. Council version: art. 83a, PSR – line 875 to 878g)

PUBLIC

- Education and awareness (art. 84, PSR – line 879 to 880a and 881 to 882a)

Below, the Presidency has included a table which provides an overview of whether the different tools proposed are mandatory for PSPs to use and whether some kind of liability related to unsatisfactory use of those tools are either explicitly included, implied or not included. The intention of the table is to give Member States an overview of the similarities and divergences between the approaches of the EP and Council.

TOOL	SHALL/MAY	LIABILITY FOR PSP
VERIFICATION OF PAYEE	EP: Shall Council: Shall	EP: Yes Council: Yes
SPENDING LIMITS	EP: Shall Council: Shall	EP: Implied Council: Implied
COOLING OFF	EP: N/A Council: Shall	EP: N/A Council: Implied
BLOCKING OF PAYMENT INSTRUMENTS	EP: Shall Council: May	EP: Yes (explicit mention) Council: No
INSTALLATION OF MOBILE PHONE APPLICATIONS	EP: N/A Council: Shall	EP: N/A Council: Implied
BLOCKING OF TRANSACTIONS	EP: May (however, blocking of payment instruments is mandatory) Council: Shall	EP: No (but closely connected to blocking of payment instruments) Council: Implied
FREEZING OF FUNDS	EP: May Council: May	EP: No Council: No

PUBLIC

TRANSACTION MONITORING	EP: Shall Council: Shall	EP: No Council: Yes
DATA SHARING	EP: Shall participate (in the Presidency's interpretation of the EP's wording), shall exchange information Council: May participate, shall exchange information with participants	EP: Yes Council: No

During the CWP in July, several Member States indicated that they could show flexibility towards the EPs more principle-based approach to fraud preventive measures. Thus, the Presidency seeks, among other things, input regarding where Member States see room for a more principle-based approach as regards to the fraud preventive measures described above.

4.1 Verification of payee (art. 50 and 57, PSR – line 660 to 668 and 705 to 713)

The Council general approach aims, in art. 50, to ensure consistency with the Instant Payments Regulation (IPR) [5]. The Presidency is aware of the positions of Member States on this topic after the discussion at the CWP in January 2025. It should, however, be noted that the EP suggests broadening the understanding of unique identifiers (see e.g. the definition in art. 3(39) (line 252) or the amendments to the recitals 104, 104a, and 104b (lines 114-114b). The EP has suggested that the EBA shall develop an RTS specifying what should be accepted as a unique identifier (art. 3(sub-paragraph 2, 3, and 4) (line 268q to 268s) and art. 89(1)(gb) (line 926b)). Furthermore, in recital 70, the EP suggests that for some entities the "name" might not be the relevant factor. They suggest it instead could be "*the name, or other identifier such as a fiscal number, a European unique identifier as referred to in Article 16(1), second subparagraph, of Directive (EU) 2017/1132 of the European Parliament and of the Council, or a legal entity identifier (LEI), that unambiguously identifies of the payee*". This elaboration is only covered by the recital and has not been added in art. 50 (recital 70 – line 80). This would if included of course also affect the functioning of the Verification of Payee service in PSR.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400886

PUBLIC

Regarding art. 57, the Council has aligned the text to the IPR in order not to create two separate refund regimes for credit transfers (including instant credit transfers) denominated in euro and for credit transfers (including instant credit transfers) in other EU national currencies. As some Member States mentioned during the Council negotiations, another approach could have been to align the provisions of IPR with the ones proposed by the Commission in PSR instead. This is because the proposed provisions of PSR could provide for a clearer refund regime. A Member State argues that the original PSR proposal covered some important issues not addressed by the IPR in art. 57(2), 57(4), and the first part of art. 57(5) (the part of (5) where it is stated that the first paragraphs shall not apply if the payer has acted fraudulently).

From the discussion at the CWP in January 2025 it was clear that the Member States supported alignment with IPR. However, since the Parliament has decided to keep the abovementioned provisions in the PSR, the Presidency would like to ask Member States whether they believe that the insertion of art. 57(2), 57(4), and the first part of art. 57(5) from the original Commission proposal into the IPR could be a viable way forward, should the Parliament insist on keeping these provisions.

Q15: What is the position of Member States regarding the EP's suggestion that the EBA should develop an RTS listing other methods than IBAN which can be used as a unique identifier?

Q16: What is the position of Member States regarding the EP's suggestion that in some cases other kinds of identification could be more relevant than the "name" of the payee?

Q17: Could the Member States consider adding art. 57(2), 57(4), and the first part of art. 57(5) from the original Commission proposal into the IPR, should the Parliament insist on keeping these provisions?

Q18: Do Member States have other comments regarding the provisions on verification of payee?

4.2 Spending limits, cooling off periods, blocking payment instruments, mobile phone applications (art. 51, PSR – line 669 to 673e)

Spending limits and cooling off periods (line 670 to 670c and 673e)

The Council has in its text finetuned the provisions on spending limits. This includes making spending limits mandatory, making it possible to have several spending limits for different payment instruments, means of payment as well as on a transaction and daily basis. However,

PUBLIC

in recital 73b (line 83b) it is specified that there should only be one limit for credit transfers and instant credit transfers initially, but these should be possible to modify individually at a later stage by the PSU. Furthermore, the Council has in its text required the application of Strong Customer Authentication (SCA) to increase the spending limits as well as the PSP is required to inform the PSU of any modifications to the spending limits to make them aware of fraudsters potentially trying to increase the spending limits. An increase in spending limits requires a cooling off period of 4 to 12 hours in the Council text. In art. 51(1c) the Council also explicitly introduces a requirement for the PSP to not execute a payment order which would exceed the relevant spending limit. In such cases the PSP should inform the PSU thereof and inform the PSU of how to modify the spending limits. Lastly, the Council has in art. 51(6) (line 673e) made it clear that the requirements in this article should prevail over the similar requirements in IPR, should they be in conflict, which was broadly supported after the CWP in April 2025.

Blocking of payment instruments (line 671 to 673)

The EP has decided to make the blocking of payment instruments mandatory in the following situations: 1) objectively justified risks relating to the security of the payment instrument, 2) the suspicion of unauthorised or fraudulent use of the payment instrument, or 3) in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil its liability to pay.

The Council has kept the approach from the Commission proposal and only made it a possibility for PSPs to block the payment instruments in all those situations mentioned above. The Council has added that the PSP may block the instrument if it is used by the PSU for activity that is prohibited by other relevant Union or national law.

Further, the EP has made a liability shift by adding that the PSP should be liable if it does not block a payment instrument despite reasonable grounds for suspecting fraud – except where the payer acted fraudulently. The Presidency notices the deviation of the wording here compared to the requirement in the abovementioned listing of situations. Thus, the Presidency is unsure if the EP only suggests that PSPs can be liable if they fail to comply with the requirement of blocking the payment instrument in the situation listed as “the suspicion of unauthorised or fraudulent use of the payment instrument” or in all listed situations. The Presidency further notices that the EP defines their understanding of “objectively justified reasons” in line 868h (art. 83). Here the EP refers to blocking of a payment order, but this might also be meant to refer to the blocking of a payment instrument since the same wording “objectively justified reasons” is used in art. 51 (line 671). It is, however, unclear if this is or is not the intention of the EP. Further, the Council states, in line 765f, that the fact that a payment order is unusual shall not by itself constitute reasonable grounds to suspect fraud. If the EPs proposal is included in relation to payment instruments it could be beneficial to also include the Council’s proposal as to what does not constitute reasonable grounds in art. 51 as well.

PUBLIC

The Presidency noticed strong opposition towards the EPs proposal to make blocking of an instrument mandatory. However, the Presidency would like to ask Member States for input on whether they could see specific situations where blocking a payment instrument could be mandatory. If such situations exist, the Presidency would also like to hear suggestions on how to mitigate the risk of excessive de-risking by the PSPs, at this concern is cited by many Member States as the reason for their opposition to the EPs proposal.

Lastly, the Council is suggesting a period of two business days for PSPs to assess whether the reasons to block the payment instrument are still justified. The Presidency notices support for this approach.

Installation of mobile phone applications (line 673a to 673d)

The Council has added several requirements regarding the secure installation of mobile phone applications. The proposal received broad support in the Council and has been refined during the negotiations. Such requirements have not been included in the EP text.

However, to defend the position of the Council, the Presidency would like to focus on a comment from one Member State. The Member State is concerned that the current wording could imply that the delay period might in the end apply to the activation of the primary application that is also to be used for the onboarding of clients. Further, the Member State understand that the aim of the provision is that it should not apply to the primary mobile application, but to any subsequent installation on a new device. Otherwise, it could risk disrupting the remote onboarding process which is becoming widespread. The Presidency is unsure of the intention here and would therefore like to ask Member States if they believe the provision should also apply to the primary application for onboarding. Or if Member states believe the provision should only be to subsequent installations of apps on other devices when a customer relationship is already established. The Presidency notices that the provisions in art. 51(5a) and (5b) (lines 673c and 7673d) seems to imply that the PSP already has access to the correct contact details for a PSU, which could imply that the provision only applies to subsequent installations of mobile applications. If the provisions also apply to the installation of the primary mobile application, where a new customer is onboarded, it could not be expected that the PSP has the correct contact details and could therefore not comply with paragraph (5a) and (5b).

Q19: Can Member States see specific situations where it could be made mandatory to block a payment instrument? And in that case, how could the risk of excessive de-risking by PSPs be mitigated?

Q20: Do Member States believe that the provisions regarding the installation of mobile phone applications also should apply to the primary mobile application for onboarding or not?

PUBLIC

Q21: Do Member States have any other comments regarding art. 51?

4.3 Burden of proof (art. 55, PSR – lines 692 to 695a)

The Presidency notices strong support for the Council amendments to art. 55(2) – line 695 – including the amendment to refer to authentication instead of referring to the use of a payment instrument as well as the inclusion of the word "necessarily". Further, the Council has added new requirements in art. 55(3) – line 695a – as to what can be expected from the PSU in relation to cooperation and documentation.

It should be noted that the burden of proof in relation to art. 59 on impersonation fraud is discussed in agenda point 2.1 on impersonation fraud.

Q22: Do Member States have any comments regarding the burden of proof in art. 55?

4.4 Blocking of transactions (art. 65, PSR and in the EP version art. 83(2)(subparagraph 2), PSR – line 765 to 770 and line 868h)

On the blocking of transactions, the Presidency initially notices that the EP has not decided to make it mandatory to refuse to execute a payment order where fraud is suspected, whereas the Council has decided to do so. However, since the EP has made the blocking of a payment instrument mandatory, this could be seen as a different approach to achieve a comparable result. If the payment instrument gets blocked the transaction would also be blocked. The primary difference between these two approaches is that mandatory blocking of a single transaction as proposed by the Council could be considered less intrusive than mandatory blocking of a payment instrument as proposed by the EP. The latter could also lead to further de-risking as mentioned above in 4.2 (Blocking of payment instruments).

In art. 83(2)(subparagraph 2) (line 868h) the EP has added their definition of "objectively justified reasons" for suspecting fraud. In the Council text the duly justified and reasonable grounds to suspect that the transaction is fraudulent could be either based on the transaction monitoring mechanism or on any other relevant information available to the PSP (line 765c). Further, the Council specifies in line 765f what does not constitute reasonable grounds to suspect fraud.

The Council has introduced specific requirements for how to handle blocking of a regular transaction compared to an instant credit transfer. In this regard, the Council text has been

PUBLIC

quite extensively discussed. The added requirements seem to add a level of further security regarding instant payments, and flexibility regarding other transactions, where the PSP should make all reasonable efforts to contact the payer before taking a decision regarding the suspended transaction. The Presidency believes that the Council position here is to a great extent clear and would be beneficial to incorporate.

Q23: Do Member States have any comments regarding the blocking of transactions?

4.5 Freezing of funds (art. 69(2a), PSR – line 790b)

The Council and the EP has introduced quite similar provisions regarding freezing of funds by the payee's PSP. In both cases it is framed as a "may" provision for PSPs. The Council has added that a decision to postpone making the funds available could also be based on any relevant information available to the PSP. The EP has only included the transaction monitoring mechanism as a valid reason thereof. Further, the Council text includes references to AMLR and has added an investigation period of 2 business days. The Council text also includes requirements to contact both the payee and the payer's PSP in order to assess the situation before making any decision about whether to make the funds available to the payee or return them to the payer's PSP. The Presidency believes the Council mandate has been quite extensively discussed in the CWPs.

Q24: Do Member States have any comments regarding the freezing of funds proposal?

4.6 Transaction monitoring mechanism (art. 83, PSR – line 859 to 874a)

With regards to the transaction monitoring mechanism (TMM) the Parliament and Council approaches deviates in a few areas, including:

- The Council has added that the PSP is liable if it fails to apply TMM on a specific transaction which turns out to be fraudulent. The burden to prove that the TMM did in fact take place is on the PSP (lines 863b and 863c).

- The Council has added that the transaction monitoring shall be done prior to the execution of the transaction (therefore real-time in the case of instant credit transfers) by the payer's PSP (line 863a).

PUBLIC

- The Council has added that also the receiving PSP should conduct transaction monitoring (which is a prerequisite for the provision on freezing of funds in art. 69(2a)) (line 863a). However, as opposed to the timeframes included for the sending PSP there has not been included a timeframe to conduct TMM for the receiving PSP.

- The EP has made the list non-exhaustive, while in the Council version the list is exhaustive (line 864). However, in the Council version each category of data is non-exhaustive if it can reasonably be linked to the headline of the category due to the word "*including (…)*" is used (line 865 to 868a).

- The Council has expanded on the datapoints which can be included in the TMM, including a new reference to device data (lines 868-868a). Further, the Council has included a corresponding list for datapoints which can be processed by the receiving PSP (lines 868b-868g). However, one Member State argues that for outgoing transactions the list does not include information about the payee (except its unique identifier) and for incoming transactions, the list does not include information about the payer (except for its name). Since information about both the payer and the payee can be shared within the information sharing arrangement, the Member state argues that the TMM should also allow for the processing of this information. E.g. with the current wording a fraudster could potentially just change PSP or get a new unique identifier at their current PSP. In this situation the sending PSP would no longer be aware of the risks related to transactions to this specific payee. This I because only the unique identifier of the payee and no other information related to the payee can be processed as part of the TMM.

- The EP has added that when the TMM's provide strong evidence for suspecting a fraudulent transaction, or when a police report is notified to the PSP this should be considered as objectively justified reasons for the blocking of a payment order. The Council has decided to include similar provisions directly in the relevant articles as mentioned above (art. 65 and 69(2a)), though not in art. 51 in relation to the blocking of a payment instrument (line 868h).

- It is not clear which information is referred to by the EP in line 868i. It is also difficult to see how data can be shared in time for it to be used in the TMM in cases of e.g. instant credit transfers. However, if the intention is for the payee's PSP to somehow also contribute to the TMM then the Presidency believes the Council version, where receiving PSPs are required to apply TMM as well, is already covering this topic efficiently.

- The EP has added that data stored in relation to both TMM cannot be stored for longer than 10 years after the termination of the customer relationship. The Council has deleted this. A limit has only been included in the new article on data sharing in

PUBLIC

the Council version – not in relation to TMM where the Council has deleted the wording in the Commission's proposal (line 869).

- The Council has deleted the list of risk-based factors for the TMM to take account of (line 869 to 874).

- The EP has made a proposal in line 874a regarding the inherence category. However, this is addressed in the note for fraud related issues for technical meetings. Similarly for line 861 and 863.

Generally, most amendments have been added by the Council. The Presidency believes that two amendments from the EP would merit discussion. The first being the period in which data can be stored (line 869). The second is whether the list of data to be processed should be exhaustive or not. The Presidency has taken note of that some Member States have a very strong preference for making the list exhaustive due to GDPR. The Presidency thus asks if some flexibility could be shown in relation to the Parliament's position here without making the list of categories non-exhaustive. This could for instance be by adding other relevant categories of datapoints which shall/may be processed as part of the TMM. This could e.g. include those mentioned above proposed by one Member State which could e.g. either be achieved by:

- 1) adding a category that available information on the payee (which could include specific information received through the data sharing arrangements) can be processed by the sending PSP. And adding a category that available information on the payer can be processed by the receiving PSP. In this case more specific descriptions of the datapoints in question could be added.

- 2) adding a category that data received by a PSP through the data sharing arrangements can also be used for the purposes of the TMM.

If Member States see other ways to achieve more flexibility without making the list of categories non-exhaustive the Presidency would also be interested in such approaches.

Q25: Do Member States believe that the period for storing of data as proposed by the EP could be included in the text?

Q26: Do Member States support the deletion of the risk-based factors? If so, please provide a reasoning.

Q27: Do Member States see other categories of data points which could be included in the list (e.g. one of the two options mentioned by the Presidency)? Or do Member States

PUBLIC

see other ways to provide more flexibility regarding the list of categories of data points to be included in the TMM without making the list of categories non-exhaustive?

Q28: Do Member States have other comments regarding the provisions on TMM?

4.7 Fraud data sharing (COM and EP version: art. 83, PSR. Council version: art. 83a, PSR – line 875 to 878g)

For fraud data sharing both the Council and the EP has extended the list of data which can be shared. However, in many instances the specific approaches deviate. Further, the Council has decided to extract the provisions on data sharing from art. 83(3) to (6) and place them in a separate article. Below, the positions of the co-legislators are summarised:

- While the Commission's proposal only included the possibility to share unique identifiers, the EP has extended the list to cover the unique identifier, name, personal identification number, organisation number, modus operandi and other transaction information of a payee (line 875). The Council, on the other hand, refer to the list of data points mentioned in article 83(2) on TMM as well as the PSP's account of the reasonable and objective grounds that gave rise to the suspicion of fraudulent behaviour on basis of that data. However, environmental and behavioural characteristics which are typical of the payer are excluded (line 878b).
  The Presidency believes that all points mentioned by the EP could be interpreted as already included in the Council version. In that regard, the Council version seems to be broader compared to the EP's list. Especially given the fact that each category of data in art. 83 is non-exhaustive.

- In the Council text the list of data which can be shared is exhaustive. In the EP text the wording "and other transaction information" seems to imply that the list is non-exhaustive if the information can be categorised as "transaction information" (lines 875 and 878b). However, considering that the Council version includes "transaction information" in a non-exhaustive way in art. 83. In addition, all data included under the TMM can also be shared "*to the extent strictly necessary to comply with their obligations in Article 83(1), point (c), where the payment service provider has reasonable and objective grounds to suspect fraudulent behaviour by a payment service user*". For these reasons, the Presidency believes that this category is covered within the Council position.

PUBLIC

- In both the EP and the Council text, data sharing within a data sharing arrangement is mandatory.

- In the Council text it has not been made mandatory to enter data sharing arrangements. In the EP text it could be interpreted as mandatory due to the deadline for entering data sharing arrangements mentioned in line 876 (12 months from the entering into force of PSR). If the EP did not intend to make it mandatory, the Presidency is not sure why a deadline would be necessary. However, if the intention of the EP indeed is to make data sharing arrangements mandatory this should be phrased more clearly (line 876). In the questions below the Presidency seeks Member States input into finding a way of ensuring the uptake of data sharing arrangements without making them mandatory.

- The EP suggests that EBA should establish an IT platform for the purpose of data sharing. This has earlier been discussed and rejected in the Council. The Council concluded that it should be up to the PSPs to agree on the details including matters related to dedicated IT platforms (line 876a and 878e).

- The EP has added a liability shift. The EP proposes that if a PSP decides not to block a unique identifier, which the PSP has been notified about through a data sharing arrangement, then the PSP should be liable. However, it is unclear to the Presidency whether the EP intends for this to apply to the sending PSP (where the requirement would be to block the transaction intended for the unique identifier which has been fraudulently used). Or whether the requirement is on the payee's PSP to block the account associated with the unique identifier completely (line 877a). Initially, the Member States who have commented on this line are divided. Some Member States support the EP's approach while others have strong reservations due to the risk of de-risking and since such a provision could result in PSPs being liable, even in the case of PSU's gross negligence or in the case that the PSU acted fraudulently. The Presidency considers that if such liability is included it could prove difficult to convince PSPs to participate in data sharing arrangements. With the Council approach of not requiring mandatory participation, PSP's may be reluctant to join in data sharing arrangements if this voluntary move could result in increased liability. However, with the EP's approach where participation in data sharing arrangements is mandatory (if correctly understood by the Presidency) this could work more efficiently. Thus, these two provisions would have to be seen as highly interconnected. In the questions below, the Presidency seeks Member States input into whether they see a way of being flexible towards the EP and add some kind of liability for PSPs when not making proper use of the data sharing tool. This should be done without making PSPs liable for not blocking/freezing transactions to and from every single unique identifier which they have been notified about, and without

PUBLIC

dissuading PSPs from entering data sharing arrangements if these are kept as voluntary, cf. the paragraph above.

- The EP has kept the provision regarding the termination of a contract with an existing customer or the future onboarding of a customer. In addition, the EP has added that the relationship between the PSP and the existing/future customer can only be affected if *"a thorough fraud investigation conducted by the relevant authorities has concluded that the customer participated in the fraudulent activity"* (line 878). In the Council text this requirement not only relates to the business relationships between PSUs and PSPs but also includes that this requirement applies to the decision on whether to execute a transaction. The Council requires that the information received through the data sharing arrangement should at least be assessed by the PSPs (line 878 and 878f). Thus, in the EP text only a decision from the relevant authority can lead to the termination of a contract.

- The Council has included that data received through a data sharing arrangement shall not be stored "*for longer than it is necessary for the purposes laid down in Article 83(1a) but no longer than 5 years after the suspected fraudulent transaction has taken place*". The EP has not included a specific limit on the period in which the received data can be stored but writes that PSPs "*shall not keep information obtained following the information exchange referred to in this paragraph and paragraph 5 for longer than it is necessary for the purposes laid down in paragraph 1, point (c).*" (line 875 and line 878d).

- Both the Council and the EP have included the possibility for PSPs to share information with public authorities, nevertheless with slightly different wordings. In the EP version both PSPs, law enforcement agents, and public authorities can share information with public authorities "*to the extent necessary to comply with paragraph 1, point (c)*" (line 875a). In the Council version it is only the PSPs who – within the context of the data sharing provisions in art. 83a – are able to share information with relevant national authorities "*for the purposes of this article*" and "*according to national law*" (line 878g). In the Council version, the possibility for sharing information between NCAs and other authorities including tax authorities is regulated through a new provision art. 93(5) (line 980a). As such, law enforcement agents are not explicitly mentioned in the Council approach, but the Presidency assumes these are covered by the references to "relevant national authorities" in art. 83a(6) and "other authorities" in art. 93(5). The Presidency would like to ask Member States for their positions on data sharing including other entities than PSPs.

- A related point, which has also been discussed in the Council, is the threshold for when data can be shared. The EP has kept the original wording, where data can only be shared if two different PSUs who are customers at the same PSP each have

PUBLIC

reported situations with fraudulent credit transfers involving the same unique identifier to their PSP (line 875). In the Council version this has been broadened to the following: "*to the extent strictly necessary to comply with their obligations in Article 83(1), point (c), where the payment service provider has reasonable and objective grounds to suspect fraudulent behaviour by a payment service user*" (line 878b). While this might have been broadened in the Council text, the Council has also added other safeguards such as the pseudonymisation requirement when deemed appropriate.

- In art. 83a(1a) in the Council position it is included that PSPs should in some cases make use of pseudonymisation when sharing data for proportionality reasons (line 878c).

Q29: Regarding fraud data sharing, do Member States see any other categories of data points that should be possible to share? Alternatively, do Member States see other ways to provide for more flexibility without making the list of categories of datapoints non-exhaustive?

Q30: Could Member States be open to making participation in data sharing arrangements mandatory? Alternatively, do Member States see a way of ensuring satisfactory participation in data sharing arrangements without making it mandatory?

Q31: Do Member States see a way of being flexible and add some kind of liability for PSPs if they do not make proper use of the data sharing tool?

- **If so, how do Member States believe this can be done without making PSPs liable for not blocking/freezing transactions to and from every single unique identifier they have been notified about?**
- **Furthermore, how do Member States believe this can be achieved without dissuading PSPs from entering data sharing arrangements if participation remains voluntary?**

Q32: What are Member States' positions on the divergences between the Council and EP approach on fraud data sharing including other entities than PSPs?

Q33: Do Member States have other comments regarding the provisions on data sharing?

PUBLIC

4.8 Education and awareness (art. 84, PSR – line 879 to 880a and 881 to 882a)

In the upcoming trilogue, it is expected that the co-legislators will discuss more generally whether obligations towards Member States for education and awareness should be included in the PSR. If this can be agreed upon, the specific drafting could be delegated to technical level.

In art. 84 the Commission proposes that PSPs shall educate both their employees and their customers on fraud risks and trends. Both the EP and the Council have added a new paragraph (line 880a and 882a) specifying that also Member States have a responsibility in raising awareness regarding this topic. Furthermore, similar obligations for Member States are already included in the directive on combating fraud and counterfeiting of non-cash means of payment[6]. Here, art. 17 states that: "*Member States shall take appropriate action, including through the internet, such as information and awareness-raising campaigns and research and education programmes, aimed to reduce overall fraud, raise awareness and reduce the risk of becoming a victim of fraud. Where appropriate, Member States shall act in cooperation with stakeholders*."

In the EP's PSR text Member States shall inform not only the Commission but also the EP on their planned campaigns. The Presidency does not understand why such measures should be notified to the EP. The planned educational measures may in the EP text include a media campaign or lessons at schools. The Presidency notices that lessons at schools falls outside the competences of this Council formation. The EP has furthermore added that ECSPs and PSPs should cooperate free of charge with the Member States in regard to education and awareness.

Lastly, the EP has added that only relevant employees should take part in the training program that the PSP shall organize annually (art. 84(2) - line 881).

(Inputs from Member States regarding lines 880b and 880c are discussed in agenda item 2.2 regarding ECSP's.)

Q34: What are the Member States' positions towards the EP's proposals in art. 84?

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713