Council of the European Union
General Secretariat

PUBLIC

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

Brussels, 13 November 2025

WK 15441/2025 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:	Working Party on Financial Services and the Banking Union (PSD/PSR) 17.11.25 - Preparatory note for the Political trilogue on the 26th of November: Issues related to non-PSPs (electronic communication service providers, providers of hosting services/online platforms, and technical service providers)

Danish Presidency
Council of the European Union

PUBLIC

Working Party on Financial Services and the Banking Union

Payment services package proposals (PSD3/PSR)

Date: 17 November 2025

Brussels, 17 November 2025

Preparatory note for the Political trilogue on the 26th of November: Issues related to non-PSPs (electronic communication service providers, providers of hosting services/online platforms, and technical service providers)

PUBLIC

1. Introduction

This note covers issues related to non-PSPs such as ECSPs, hosting services (online platforms), and technical service providers. This includes topics which will be discussed at the political trilogue on the 26 November. Furthermore, it also includes topics which will be dealt with at the interinstitutional technical meetings (ITMs).

Discussions on the provisions related to non-PSPs (providers of electronic communication services (ECSP), providers of hosting services, and technical service providers (TSP)) have so far been reserved for discussions at the political trilogues. However, at technical level there has been an exchange of positions for those articles. This to better understand each other's intentions and amendments. In order to create a basis for the discussions the Commissions' DG CNECT have shared a non-paper concerning the legal framework for the actors described above. This paper has also been distributed to Member States.

2. Providers of electronic communications services (ECSPs) (line 268b, 268c, 723 (first part from Commission proposal), 723a, 723b, 723e-723g, 723i, 880b, 880c, 880d)

At technical level the European Parliament (EP) has agreed that a more specific definition of ECSPs should be found, in order to distinguish the requirements imposed on the various actors. Furthermore, if requirements are to be imposed on providers of hosting services (or specific subcategories thereof), they should get their own definition and requirements separate from those of ECSPs.

At the ITMs the Commission agreed that the Council proposal to omit spoofing in Article 59a is preferred as Member States are already empowered to implement measures against spoofing within the telecommunication sector legislation. Furthermore, different initiatives against spoofing are being implemented across Member States. Thus, the Presidency finds a general reference to prevention of fraud in Article 59a(3) as the most appropriate phrasing, in line with the Council mandate, and will defend this position in the trilogues.

However, should the EP insist on keeping the initial wording of Article 59(5) (only the part of the text which was included in the proposed by the Commission) (line 723), or the proposed wordings in Article 84 (line 880b and 880d), the Presidency would like to ask Member States whether flexibility in regards to this can be shown. For Article 59(5) the Presidency notices that this is a reactive requirement when impersonation fraud cf. Article 59(1) has already

PUBLIC

taken place, Article 84 covers the more proactive side, where ECSPs and PSPs should cooperate to prevent spoofing of phone numbers and mail addresses.

With regard to the last part of Article 59(5) (line 723), which has been added by the EP. The EP has clarified that this should be read only to cover providers of hosting services – not ECSPs.

Q1: Could Member States be flexible in including the first part of line 723 (the text from the Commission's original proposal), line 880b, and line 880d?

3. Providers in scope of the Digital Services Act (DSA)[1] (line 268b, 268d, 723 (EP addition only), 723a, 723b, 723h, 877b, 880c, 880d, 967g)

At the ITMs the EP has kindly clarified some of its positions regarding actors in scope of the DSA. The Presidency understands that liability is central and there is a need to consider, for the purposes of the PSR, that the DSA provides only exceptions from the general liability exemption for hosting services (Article 6 of the DSA). From the Presidency's reading of its exchanges with the EP, there seems to be a wish to explicitly place liability on providers of hosting services for non-removal of illegal content leading to fraud, which the provider of hosting services has already been notified about in accordance with the notification procedure in Article 16 of the DSA. However, the EP acknowledges that this should respect the DSA and finds that this can be constructed in a legally sound way.

In relation to the above the EP has clarified that the intention of their addition to Article 59(5) (line 723) is not to make providers of hosting services liable for the particular fraud case where the provider is first notified of the illegal content. However, if anyone else at a later stage is defrauded by the exact same piece of content due to the provider's decision not to remove said content, liability should arise.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065

PUBLIC

This line of thinking is mirrored in Article 6(1)(b) of the DSA. In that case, however, it is phrased as the exception to the exemption from liability as laid out in Article 6(1) of the DSA instead of explicit liability as drafted by the EP for the PSR.

The Presidency finds that requirements and liability for providers of hosting services are important to the EP. The Presidency will in the next section present three suggestions for strengthening fraud preventive measures in relation to ECSPs and providers of hosting services.

4. Suggestions for provisions on ECSPs and providers of hosting services (online platforms)

Below, the Presidency will present three suggestions:

1. An amended version of the Irish non-paper regarding advertisement of financial services on very large online platforms (VLOPs) and very large online search engines (VLOSEs).

2. Strengthening of fraud data sharing between PSPs on the one side and providers of hosting services/online platforms and ECSPs on the other side

3. A new datapoint to be shared between PSPs in Article 83a

4.1 Advertising for financial services on VLOPs and VLOSEs

Recalling the discussions in the spring regarding the advertisements for financial services on VLOPs and VLOSEs, the Council Legal Service and the Commission made it clear that violation of the "no general monitoring obligation" in Article 8[2] of the DSA could potentially be foreseen. This was primarily due to an assessment that the requirement would place to much of a task on the VLOPs and VLOSEs, as it would be difficult for the VLOPs and VLOSEs to decide whether an advertisement was for a financial service, and whether the advertiser then had a license to provide financial services.

The Presidency would suggest an amended wording which builds on the Irish non-paper. The legislative text in the PSR should refer to the information, which VLOPs and VLOSEs are

[2] "No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers."

PUBLIC

already required to possess for the purposes of the ad repository cf. Article 39 of the DSA. This information includes the subject matter of the advertisement and the natural or legal person on whose behalf the ad is presented. In the Presidency's understanding this information is self-reported. However, Article 39(1) of the DSA does require VLOPs and VLOSEs to "*make reasonable efforts to ensure that the information is accurate and complete*". This would include whether information about the subject matter and whether the information about the identity of the natural or legal person is accurate.

Given that the VLOP or VLOSE should know whether an ad is placed for a financial service, the Presidency suggests that the platform should check whether the entity for which the ad is placed is present on the ESA's (EBA[3], ESMA[4], and EIOPA[5]) public registers of providers with a license to provide financial services within the union. The Presidency finds that this approach makes it possible for VLOPs and VLOSEs to comply with the requirement in an easy and clear way and could therefore be considered in compliance with the DSA.

Please see the drafting in the annex (section 1): Drafting suggestion regarding advertisement for financial services.

Q2: Can the Member States support the Presidency's proposal regarding advertisement for financial services, including the drafting (as presented in section 1 in the annex)?

Q3: Do Member States have any comments on the list included as the definition of financial services and whether the scope of this list is too narrow or broad?

Q4: Do Member States agree that the public registers provided by the ESA's are adequately covering the relevant providers?

[3] https://www.eba.europa.eu/risk-and-data-analysis/data/registers-and-other-list-institutions

[4] https://registers.esma.europa.eu/publication/searchRegister?core=esma_registers_upreg

[5] https://register.eiopa.europa.eu/

PUBLIC

4.2 Strengthening of fraud data sharing between PSPs on the one side and providers of hosting services/online platforms and ECSPs on the other side

In the Council mandate Article 59a(1) requires ECSP's to establish dedicated communication channels for fraud prevention purposes. Here, information can be shared from a PSP to ECSP or the other way around. However, the information which can be shared is limited to what is allowed within GDPR, and providers of hosting services/online platforms are not included in this provision either.

To strengthen this tool, the Presidency would propose to mirror the article for fraud data sharing between PSPs in Article 83a, to provide a legal basis for sharing of more specific information from PSPs to ECSPs and providers of hosting services/online platforms (and the other way around) just as Article 83a provides this possibility for data sharing between PSPs. Fraud data sharing is not only relevant between PSPs but could also prove effective in fraud prevention if relevant data could be shared with ECSPs and providers of hosting services/online platforms. For instance, the Presidency understands from the payment sector that many advertisements containing fraudulent content are paid with stolen payment cards. If information could be shared by PSPs to providers of hosting services/online platforms about compromised payment instruments, the advertisement(s) could then be removed if it was paid for by a stolen payment instrument. Similarly, device and session data would be relevant to share since it could target the setup of the fraudster and their possibilities to place fraudulent content online.

The Presidency has included drafting in the *annex (section 2*). If the suggestion is supported, the Presidency proposes to add it to a new Article 59c for data sharing between PSPs and ECSPs and providers of hosting services/online platforms. One could argue that a simpler solution would be to add the extension to Article 83a where the provisions on data sharing are already placed. In this regard the Presidency would like to note that Article 83a refers to the data points in the transaction monitoring mechanism, which is specifically drafted with a payment service user in mind. However, this terminology is not used in the context of hostings services/online platforms and ECSPs. Therefore, the Presidency suggests this minorly redrafted list of data categories and data points to be placed separately to take account of this.

Lastly, it should be decided whether this should apply to all providers of hosting services, online platforms, or only to the VLOPs and potentially also VLOSEs. The Presidency notes that many small providers are providing hosting services or online platforms. It might therefore be more proportionate to only require VLOPs and VLOSEs to participate in such information sharing arrangements. However, fraud takes place through many different channels, and it could therefore also be considered necessary to include more providers than just the very

PUBLIC

large ones. Thus, the Presidency seeks input as to which providers in scope of the DSA should be encompassed by the potential requirement for participating in data sharing arrangements.

Q5: Can Member States support to allow sharing of information between PSPs and ECSPs and providers of hosting services/online platforms as proposed by the Presidency?

Q6: Which providers in scope of the DSA should the requirement to participate in data sharing arrangements with PSPs apply to? (1) Providers of hosting services, 2) Online platforms, 3) Very large online platforms, 4) Very large online search engines?)

Q7: Do Member States have any comments on the specific data categories/datapoints?

4.3 A new datapoint to be shared between PSPs in Article 83a

The Presidency has noticed a particular challenge in relation to the liability exemptions for hosting services in Article 6 of the DSA. To the Presidency's knowledge, there is no way for anyone else but the provider of hosting services and the one who makes a notification in accordance with Article 16 of the DSA about fraudulent content, to know that such notification was in fact made. This means that if a costumer of **PSP "A"** is defrauded, and **PSP "A"** then notifies the provider of hosting services about the illegal content, but the provider of hosting services decides not to remove the content, another consumer who is a customer of **PSP "B"** could be defrauded from that same content. For the costumer of **PSP "B"**, the liability exemption in Article 6 of the DSA would no longer be valid for the provider of hosting services since it has gained "actual knowledge" of the fraudulent content through the notification made by **PSP "A"**. Hence, it should be possible for the customer of **PSP "B"** to apply (potentially to the courts) for a refund from the provider of hosting services. However, since **PSP "B"** has no way of knowing that this exact same content has already been notified, their customer would have no concrete evidence, that the liability exemption would not apply for this specific content which would harm the customers possibility to get a refund.

In summary, the lack of information sharing means that customers defrauded by the same illegal content that has already been flagged might not be able to get a refund because only the platform itself and the PSP who made the first notification actually know that this notification has been made. Other PSPs would, however, not have this information.

The Presidency believes that this could partially be solved in Article 83a by requiring PSPs to share information about which content they have made a notification about cf. Article 16 of the DSA. This would allow other PSPs to know when the exception in Article 6(1)(b) of the

PUBLIC

DSA (the provider of hosting services has gained "actual knowledge" of the illegal content) would apply and the liability exemption would be invalid for that particular content.

This would, however, not solve the apparent information gap completely since many, also apart from PSPs, would be notifying about illegal content, but it could at least improve the likelihood that providers of hosting services could become liable if they have chosen not to remove fraudulent content.

On this background, the Presidency would thus suggest adding in Article 83a that information about notifications made by the PSP cf. Article 16 of the DSA can be shared as well.

Q8: Can Member States support the Presidency's proposal allowing PSPs to share information about which content they have notified as fraudulent in accordance with Article 16 of the DSA?

5. Technical service providers (Article 58 and 87)

At the working party on 8 September 2025, the Presidency wrote in its discussion note that it was not aware of the rationale behind the EP amendments to Article 57 and deletion of Article 87. At the ITMs, the EP has explained that they consider it covered by Article 32 of the Digital Operational Resilience Act (DORA)[6] and by the proposed EBA mandate in Article 89(1)(d) (This mandate includes a reference to Article 87. Here, this reference to Article 87 should be deleted if the article is deleted, but the EP believes that the mandate should be kept even if Article 87 is deleted). The Commission has argued that this is not covered adequately by DORA since SCA should not be understood as operational resilience, and that it is important to ensure that PSPs contractually have the right to audit and control the technical service providers (TSPs).

With regard to Article 58, the EP argues that their amendments ensure a more proportionate sharing of the financial damage, and that no other liability provisions allow for liability above the amount of the transaction in question. The Commission has argued that the article should also be understood to encompass liability for TSPs for lost revenue for businesses. This would

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

PUBLIC

apply in cases where a failure on the part of the TSP made the payer unable to purchase the service of the payee.

Q9: Do Member States have any comments regarding Article 58 and 87 on outsourcing? Can Member States show flexibility towards the EP's amendments to Article 58 and deletion of Article 87?

PUBLIC

Annex: Drafting with regard to ECSPs and providers of hosting services:

Section 1: Drafting suggestion regarding advertisement for financial services

Recital x

To ensure transparency and integrity in advertisements for regulated financial services on very large online platforms and very large online search engines, clear verification requirements are necessary for disseminating to the public advertisements for financial services.

Very large online platforms and very large online search engines should only disseminate advertisements for regulated financial services if the advertiser is authorised or exempt under the law of the relevant Member State or is acting on behalf of such an entity. The European Supervisory Authorities – EBA, ESMA, and EIOPA – already maintain public registers of financial service providers under the applicable legislation. Very large online platforms and very large online search engines should use these registers to confirm whether the potential advertiser is listed as an authorised entity in one of these registers.

Definitions: Article 3(x)

'advertisement' means 'advertisement' as defined in Article 3, point (r), of EU Regulation 2022/2065;

'dissemination to the public' means 'dissemination to the public' as defined in Article 3, point (k), of EU Regulation 2022/2065;

'financial service' means

i. Any of the services and activities listed in points 1 to 15 of Annex I to Directive 2013/36/EU;
ii. Any of the services and activities listed in Section A of Annex I relating to any of the instruments listed in Section C of Annex I to Directive 2014/65/EU;
iii. Any of the services and activities as defined in point (16) of Art 3 of Regulation (EU) 2023/1114;
iv. Any of the services and activities set out in Annex I to Directive 2015/2366;
v. Any of the services and activities set out in Annex I and Annex II of Directive 2009/138/EC;

PUBLIC

vi. Any service or activity involved in presenting, offering, advising on, intermediating, broking and proposing any of the preceding categories of services or activities or of carrying out other work preparatory to the conclusion of contracts for those services or activities.

Article 59b Verification of advertisers of financial products

1. Very large online platforms and very large online search engines, within the meaning of Article 33 of EU Regulation 2022/2065, shall not engage in the dissemination to the public in any Member State of any advertisement for any regulated financial service in that Member State unless the advertiser:

   a. is a regulated financial service provider that is
      i. authorised to provide that regulated financial service in that Member State; or
      ii. an entity authorised to do so as a result of it establishing a branch or by providing services, where it is authorised and supervised by the competent authorities of another Member State, provided that such activities are covered by the authorization, or
      iii. an entity otherwise authorised to provide those services by the competent authorities of that Member State;

   or

   b. is exempt under the law of that Member State from requiring to be authorised to provide that regulated financial service in that Member State and can provide evidence of such exemption; or
   c. is acting on behalf of or as agent of a regulated financial service provider that itself is authorised to provide that regulated financial service in that Member State, can provide evidence of a contractual relationship with the financial service provider; or
   d. is acting on behalf of or as agent of an entity that is exempt under the law of that Member State from requiring to be authorised to provide that regulated financial service in that Member State, can provide evidence of a contractual relationship with an entity which has such exemption.

2. To comply with the requirements in paragraph 1 of this article, very large online platforms and very large online search engines shall when complying with the

PUBLIC

requirements of article 39(2), point (a) of EU Regulation 2022/2065 specify if the subject matter of the advertisement is a financial service.

Where the subject matter of an advertisement is a financial service, the very large online platforms and very large online search engines shall confirm that the natural or legal person referred to in article 39(2), points (a) and (b) of EU Regulation 2022/2065 is authorised to provide that regulated financial service by confirming that the natural or legal person is included in the public registers of providers of financial services made publicly available by the EBA, ESMA, and EIOPA.

PUBLIC

Section 2: Drafting suggestions regarding data sharing between PSPs and ECSPs and online platforms

(Please notice that for now the Presidency has inserted online platforms in the drafting proposal. However, in Q6 the actual scope of providers within the DSA which this will apply to will be determined)

Art. 59c Fraud data sharing between payment services providers and online platforms and providers of electronic communications services

1. Payment service providers may exchange data with online platforms, as defined in article 3, point (i), of regulation (EU) 2022/2065, and providers of electronic communications services, as defined in Article 2(4), point (b), of Directive (EU) 2018/1972, and data may also be exchanged by online platforms and providers of electronic communications services to payment service providers who are subject to an information sharing arrangement as referred to in paragraph 4 to the extent necessary to enable payment service providers, online platforms, and providers of electronic communications services to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services, where the payment service provider, the online platform, or the provider of electronic communications services has objectively justified grounds to suspect fraudulent behaviour by a user of their service.

   The catalogue of data to be shared shall be limited to the data listed in this paragraph, including the payment service provider's, online platform's, or provider of electronic communications services' account of the objectively justified reasons that gave rise to the suspicion of fraudulent behaviour on basis of that data. Information on the environmental and behavioural characteristics which are typical of the user of one of the respective services including in the circumstances of a normal use of the personalised security credentials shall be excluded from data sharing under this Article;

a) Information on the user of the respective service;
b) Information on the payment account (including the payment transaction history);
c) Transaction information including the transaction amount, payment instrument, currency, date and time of execution, as well as unique identifier of the payment service user;
d) Session data, including the device internet protocol address-range from which the payment account has been accessed;
e) Device data, including device identifiers from which the transaction was initiated and from which the transaction was authenticated;

2. Participants in an information sharing arrangement shall implement appropriate technical and organisational measures, including measures to allow

PUBLIC

pseudonymisation, to ensure a level of security and confidentiality proportionate to the nature and extent of the information exchanged.

3. Participants in an information sharing arrangement shall not keep data obtained following the information exchange referred to in paragraph 1 for longer than it is necessary for the purposes of enabling payment service providers, online platforms, and providers of electronic communications services to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services, but no longer than 5 years after the suspected fraudulent transaction has taken place.

4. For the purpose of paragraph 1 of this article, without prejudice to Directive (EU) 2022/2555, Directive 2002/58/EC or Article 91 of this Regulation, providers of electronic communications services and online platforms shall establish information sharing arrangements 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.

5. The information sharing arrangements shall specify the details of participation and the details of operational elements, including the use of dedicated IT platforms. Before concluding such arrangements, participating payment service providers, online platforms, and providers of electronic communications services shall jointly carry out a data protection impact assessment in accordance with Article 35 of Regulation (EU) 2016/679 and, where applicable, prior consultation of the supervisory authority in accordance with Article 36 of that Regulation.

6. Payment service providers shall not rely solely on the information received in the context of the data sharing referred to in para. 1 to comply with the requirements of this Regulation and shall not draw conclusions or take decisions that have an impact on the business relationship with the payment service user or on the execution of a payment transaction on the basis of information received from online platforms and providers of electronic communications services who are subject to an information sharing arrangement without having assessed that information.