Council of the European Union
General Secretariat

PUBLIC

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

Brussels, 31 March 2025

WK 4266/2025 INIT

LIMITE

EF
ECOFIN
CODEC

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

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Financial Services and the Banking Union (Payment Services/ PSR/PSD) Financial Services Attachés
Subject:	Presidency Discussion Note: Discussion on electronic communications services providers

POLAND25.EU

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

PUBLIC

Payment services package proposals (PSD3/PSR)
Brussels, 4 April 2025

Presidency Discussion Note
Discussion on electronic communications services providers

PUBLIC

Obligation for ECSPs and PSPs to collaborate

During the previous discussions on Article 59, it was clear to some Member States that parties other than PSPs that are involved in the transaction chain should also have some obligations, including an obligation to cooperate with PSPs. Cooperation of this kind is crucial to the collective fight against fraud.

On the basis of the discussion at the 21 February Council Working Party (CWP) meeting and subsequent written comments, the Presidency noted that several Member States were questioning its proposal to create a basis for future provisions on this issue and, for the moment, to only introduce a review clause for the Commission (presented in Recital 81a and Article 108(1b) below). Member States would welcome the review clause (so we propose to keep it), but some argued that this approach was not sufficient and there was a need to have targeted obligations for specific players as part of the current work on the Payment Services Regulation (PSR).

Moreover, some Member States pointed out that the duty of cooperation for ECSPs should not be limited to cases of impersonation of a PSP employee and would be useful in all cases of fraud and for all PSUs (not just consumers).

Meanwhile, the proposal included in IE non-paper, presented during the 21 February CWP received strong support from Member States. However, some Member States only supported Ireland's proposals on the condition that they were in line and consistent with other relevant provisions, such as those contained in the Digital Services Act[1] (DSA) or the ePrivacy Directive[2]. After some additional analysis, it turned out that some of the proposed solutions, like removing/blocking access to content, could be problematic and go against the rules of the ePrivacy Directive. Similarly, some Member States argued that the proposed verification of advertisers seemed to be in conflict with the provisions of the DSA (i.e. Article 8 DSA on general monitoring obligations). Moreover, the preliminary assessment of the Council Legal Service also indicates, for similar reasons, that the introduction of the above provisions would be quite problematic.

Therefore the Presidency would like to propose for consideration an alternative solution, in the form of a new Article 59a dedicated to cross-sectoral cooperation, which would include the establishment of dedicated communication channels between ECSPs and PSPs for faster and more effective information sharing (based on the IE proposal) and provisions for leveraging on the DSA as regards action and notification mechanisms, the trusted flagger status and the voluntary code of conduct. The Presidency also proposes a number of new recitals clarifying rules already laid down in the DSA and linking them to the context of fraud (in particular, for the purpose of risk assessment and mitigation measures).

See the proposed wording in Recitals 81, 81a-f, 59a, 91 and 108(1b) PSR

> ***Q1.*** *Could Member States accept the proposed approach? If not, please provide your suggestions.*

Recital 81

Given their obligations to safeguard the security of their services in accordance with Directive 2002/58/EC of the European Parliament and of the Council and Directive (EU) 2022/2555 of the European Parliament and of the Council, publicly available electronic communications services providers have the capacity to contribute to the collective fight against 'spoofing' fraud. Therefore, and without prejudice to ~~the obligations laid down in national law implementing that Directive~~ those

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Directives, electronic communications services providers should cooperate with payment service providers with a view to preventing further occurrences of that type of fraud. This cooperation could include establishing dedicated communication channels for the sharing of relevant information in order to facilitate fraud prevention and detection in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC. Furthermore, providers of electronic communication services could also assist the fight against fraud by exchanging with payment service providers fraud scenarios, trends and threats identified in relation to the use of their services, as doing so may help to improve the effectiveness of transaction monitoring mechanisms and the educational campaigns and training on fraud implemented in accordance with this Regulation and without prejudice to Directive 2002/58. ~~Therefore, and without prejudice to the obligations laid down in national law implementing that Directive, electronic communications services providers should cooperate with payment service providers with a view to preventing further occurrences of that type of fraud, including by acting promptly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC. Any claim by a payment service provider against other providers, such as electronic communications services providers, for financial damage caused in the context of this type of fraud should be made in accordance with national law.~~

Recital 81a [proposed during 21 Feb CWP]

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

Recital 81b

Regulation 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) lays down fully harmonised rules on the provision of intermediary services in the internal market and on specific due diligence obligations tailored to certain specific categories of providers of intermediary services ('mere conduit', 'caching' and 'hosting' services). In particular, it imposes specific due diligence obligations on online platforms and online search engines, including those designated as very large online platforms or very large online search engines. Such due diligence obligations play an important role in preventing the proliferation of illegal content online, such as financial scams. For instance, hosting services providers are obliged to put in place user-friendly notice and action mechanisms to allow the reporting of illegal content, such as illegal offers of financial services or attempted fraud, to the hosting service. Online platforms are also obliged to address notices from trusted flaggers as a priority.

Recital 81c

In particular, very large online platforms and very large online search engines within the meaning of Regulation (EU) 2022/2065 are already obliged to diligently identify, analyse and assess any systemic

risks posed by their services, including the dissemination of illegal content through their services, such as malicious or fraudulent online content within the meaning of this Regulation. Where applicable, further to that assessment, very large online platforms and very large online search engines should put in place reasonable, proportionate and effective mitigation measures in accordance with Article 35 of Regulation (EU) 2022/2065 to address those risks, under the direct supervision of the Commission.

Recital 81d

Regulation (EU) 2022/2065 encourages and facilitates the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of that Regulation, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks, such as fostering prevention, enhancing security and combating payment fraud and financial scams. The drawing up of a voluntary code of conduct at Union level in the areas covered by this Regulation should also be facilitated.

Recital 81e

Any claim by a payment service provider against other providers, such as electronic communications services providers or providers of intermediary services, for financial damage caused in the context of fraud should be made in accordance with national law. Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive (EU) 2000/31/EC (Digital Services Act) sets up a framework for the conditional exemption from liability of providers of intermediary services, under certain conditions and as interpreted by the Court of Justice. The exemptions from liability established in Regulation (EU) 2022/2065 should not affect the possibility of injunctions of different kinds against providers of intermediary services. Such injunctions could, in particular, consist of removal orders and information orders by courts or administrative authorities, issued in compliance with Union law.

Recital 81f

National competent authorities can play an important role in combating the type of fraud referred to in this Regulation by requiring providers of electronic communications services on a case-by-case basis to block access to numbers or services once said fraud has been committed using electronic communications services and ascertained by a competent authority. If a national competent authority has ascertained the occurrence of the type of fraud referred to in this Regulation, they may require providers of public electronic communications networks or publicly available electronic communications services to block access to numbers or services, in accordance with Article 97(2) of Directive 2018/1972/EU.

Article 59a [new]: Cross-sectoral cooperation for the purpose of fraud prevention and detection

1. For the purpose of preventing and detecting fraud, including that referred to in Article 59(1), providers of 'electronic communications services' as defined in Article 2(4), points (a) and (b), of Directive (EU) 2018/1972 shall have in place measures to ensure effective cooperation with payment service providers, having regard to the technical characteristics of each of their services.

For the purpose of the first subparagraph, without prejudice to Directive (EU) 2022/2555, Directive 2002/58/EC or Article 91 of this Regulation, electronic communications services providers shall establish dedicated communication channels with payment service providers to allow for faster and more effective sharing of any information that could be useful in the prevention and detection of fraud within the meaning of this Regulation and in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC.

2. Payment service providers may make use of the notification mechanisms referred to in Article 16 of Regulation (EU) 2022/2065 to notify providers of hosting services of the presence on their service of specific items of information that they consider, including based on notifications received from payment service users, illegal content within the meaning of this Regulation. Payment service providers may also apply to be awarded trusted flagger status pursuant to Article 22 of Regulation (EU) 2022/2065.
3. The Commission and the European Board of Digital Services shall encourage and facilitate the drawing up of a voluntary code of conduct at Union level to foster prevention, enhance security and combat payment fraud and financial scams, under the conditions set out in Article 45 of Regulation 2022/2065.

Article 91 [Competent authorities and investigatory powers]

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

Article 108 [Review clause] [proposed during 21 Feb CWP]

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