Council of the European Union
General Secretariat

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

Brussels, 13 May 2025

WK 6225/2025 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 Summary Note on fraud-related issues in the Payment Services Regulation

POLAND25.EU

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

Payment services package proposals (PSD3/PSR)
Brussels, 15 May 2025

Presidency Summary Note
on fraud-related issues in the Payment Services Regulation

Authorisation, liability and gross negligence

On the basis of the discussion held at the 29 April CWP and the written comments received from MS, the Presidency, aware of the broad support for the proposals, made only minor changes to the provisions on authorisation, liability and gross negligence. As the recently proposed wording "carried out" in Article 49 was strongly criticised by some MS, we have reinstated the previous wording '*initiated or modified*', which some MS consider preferable to "carried out", as it more clearly covers cases where the third party manipulates the communication between the payer and the PSP (such as in man-in-the-middle/browser attacks and similar types of fraud). In Article 49(1a) we have reverted to the previous wording with only a minor change in order to maintain an explicit reference to the most prominent case of 'unauthorised transactions', while not excluding other forms of fraud which do not necessarily involve the fraudulent acquisition of the PSU's credentials (e.g., certain cases of man-in-the-browser attacks). As one MS strongly disagreed with the complete deletion of any reference to any communication channel, we have introduced a more general wording instead. In addition, at the request of some MS, we have deleted the reference to the employee of the consumer's PSP, in order to cover also situations, where the fraudster uses mobile apps or websites, to impersonate the PSP as an institution, rather than its employees. We have also deleted the last sentence of Recital 80a, as it was reported to be both misleading and of little added value. In Recital 82, we have aligned the wording of the provisions by replacing *ADR* with *dispute resolution bodies*. We have also added a reference to EU courts in the same recital, for which the criteria should also not be binding.

The amendments have been introduced in Recitals 69a, 79, 80a, 82 and Articles 49 and 59 PSR.

Obligation for ECSPs and PSPs to collaborate

On the basis of the written comments from Member States following the 4 April and 29 April CWPs, the Presidency was able to conclude that the proposed new Article 59a on cross-sectoral cooperation and the accompanying recitals were considered by many Member States to be a step in the right direction. On the basis of the written comments submitted by MS, the Presidency decided to make only minor changes to the wording of the provisions. In Recital 81f we have introduced some changes to better reflect the provisions in the EECC and to avoid inconsistencies between the PSR and the EECC on the legal basis for blocking of access to numbers or services. In Article 59a(1), at the request of two Member States, we have deleted the reference to '*eliminating fraud',* as they argued that it cannot be reasonably expected that fraud can ever be 'eliminated', in particular by the measures envisaged in this Article. We have also replaced the reference to measures with instruments, as it was argued that the term 'measures' was confusing in this context. Finally, following the preference of the majority of MS, in Article 91(5) we have limited the definition of ECSPs to the providers listed in Article 2(4)(b) of Directive (EU) 2018/1972 (on the European Electronic Communications Code).

The amendments have been introduced in Recital 81f and Articles 59a(1) and 91(5) PSR.

Q1: Do Member States identify any red flags with regard to the fraud-related provisions proposed in this Note?

Annex (the newly introduced amendments are highlighted in RED)

Recital 69a

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

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

Recital 79

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

Recital 80a

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

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

Recital 82

(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all the individual circumstances of the case. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness, ~~that should be assessed depending on the individual circumstances of the case.;~~ for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties~~.; sharing account credentials with the person without the right of disposal, i.e. is not eligible to use the payment instrument; if the loss of a payment instrument is not reported to the payment service provider immediately after the loss is discovered; where the payment service user has ignored a clear, concrete and case-specific warning by the payment service provider about how to react in the type of fraudulent situation which then occurred and led to the damage; where the payment service user has failed to check if the elements which are dynamically linked and displayed during the strong customer authentication in accordance with Article 85 are correct.~~

When assessing the possible gross negligence on the part of the payment service user, ~~account should be taken, for example, to~~ all the factual circumstances should be taken into account, for example: ~~. For this purpose, one or more of the following circumstances may be taken into account, such as the (a) payment service user's behaviour or communication with third parties, where relevant; (ab) of the~~ innovativeness and~~,~~ complexity of the fraud, ~~and the~~ means or strategies used by third parties to illegally take over the payment service user's personalised security credentials; ~~of payment instruments owned by the payment service user~~; ~~(c) innovativeness, complexity of fraud~~; ~~(bd)~~ whether the payment service user has previously fallen victim of the same type of fraud; ~~(ce)~~ in the case of ~~the fraudster's means or strategies constitute~~ a new type of fraud, whether the payment service providers have complied with ~~fulfilled~~ their obligations under Article 84, ~~with particular~~ including with regard to their most vulnerable groups of customers; ~~(df)~~ whether the payment service user has taken adequate steps in order to properly ensure the confidentiality of their personalised security credentials ~~of the payment instruments~~;

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

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

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

~~(gj)~~ whether the payment service providers offered clear, specific~~concrete~~ and ~~case-specific~~ bespoke warnings ~~against currently used frauds methods that were brought directly~~ to the ~~attention of~~ payer~~,~~

~~that are transaction specific, and payment service providers actions, taken in order to familiarise the payment service user with the risks and methods of fraud in the electronic space, as well as the meaning and legal consequences of the safe misuse of identification means and payment instruments issued by the payment service user, the disclosure of their personalised security data, etc. the specificity and nature of any intervention made by the sending payment service provider in the payment flow,~~ whether the payment service user failed to have regard to specific, directed interventions made by their payment service provider~~, and whether those interventions offered a clear assessment of the probability that an intended payment was fraudulent.~~ This list is not exhaustive, cumulative or binding and does not prejudice the discretion of national or EU courts and/or dispute resolution bodies ~~ADR entities~~. ~~The circumstances as mentioned are not cumulative and are not binding.~~ ~~The fact that a payment service user consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again victim of the same type of fraud could, depending on the circumstances of the case, be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent *modus operandi*.~~

Article 49 [Authorisation]

1. A payment transaction or a series of payment transactions shall be authorised only if the payer has given its ~~permission~~ consent for the execution of the payment transaction ~~including as regards the amount of the payment transaction and the payee~~. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the account servicing payment service provider, after the execution of the payment transaction.
1a. A payment transaction shall not be deemed as authorised ~~where the payer was manipulated through social engineering into initiating the payment transaction in favour of a third party which was not the intended payee, or~~ where the transaction was ~~carried out~~ initiated or modified by a third party who is acting without the consent of the payment service user, including by using the personal security credentials of the payment service user fraudulently obtained.
2-7. […]

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

1. Where a payment services user who is a consumer was manipulated by a third party pretending to be ~~an employee of~~ the consumer's payment service provider using communication channels attributed to the consumer's payment service provider ~~using the name and or e-mail address or name and telephone number or website or mobile application of that payment service provider unlawfully~~ and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer, when becoming aware of the fraud, has without undue ~~any~~ delay ~~reported the fraud to the police and~~ notified its payment service provider ~~when becoming aware of the fraud~~, providing the payment service provider with all the relevant information requested by the payment service provider and that the

consumer ~~payment service user~~ can reasonably be expected to have regarding the events leading to the disputed payment transaction, and reported the fraud to the police ~~providing supporting evidence available to the consumer~~. 2-4 […] ~~5. Where informed by a payment service provider of the occurrence of the type of fraud as referred to in paragraph 1, electronic communications services providers shall cooperate closely with payment service providers and act swiftly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC, including with regard to calling line identification and electronic mail address.~~

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

1. For the purpose of preventing and detecting ~~and eliminating~~ fraud, including that referred to in Article 59(1), providers of 'electronic communications services' as defined in Article 2(4), points (a) and (b), of Directive (EU) 2018/1972 shall have in place existing instruments ~~measures~~, including instruments ~~measures~~ to ensure effective cooperation with payment service providers, having regard to the technical characteristics of each of their services.
For the purpose of the first subparagraph, without prejudice to Directive (EU) 2022/2555, Directive 2002/58/EC or Article 91 of this Regulation, electronic communications services providers shall establish dedicated communication channels with payment service providers or participate in a system for effective communication, or in an information sharing mechanism, to allow for faster and more effective sharing of any information that could be useful in the prevention and detection of fraud within the meaning of this Regulation and in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC.
[…]

Article 91 [Competent authorities and investigatory powers]

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

(iv) providers of electronic communications services as defined in Article 2(4), points ~~(a) and~~ (b), of Directive (EU) 2018/1972 ~~electronic communications services providers within the meaning of Article 59(5);~~
iv(a) providers of intermediary services as defined in Article 3, point (g), of Regulation (EU) 2022/2065, in accordance with Article 10 of that Regulation; […]