Council of the European Union

Brussels, 18 December 2023
(OR. en)

16676/23

LIMITE

EF 397
ECOFIN 1360
CODEC 2471

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

REPORT

From:	Presidency
To:	Permanent Representatives Committee (Part 2)
Subject:	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010 - Progress report

I. GENERAL REMARKS

1. **On the 28th of June 2023 the European Commission put forward the Payment Package**. The Package includes a proposal for a Directive and a Regulation on payment services in the internal market (hereinafter, "PSD3" and "PSR", respectively). These proposals are aimed at addressing the pending challenges that were identified by the Commission in the context of the evaluation of the impact and application of Directive (EU) 2015/2366, on payment services in the internal market (hereinafter, "PSD2"), as well as to adapt the payment rules to new market developments.

2. **The review of the Second Payment Services Directive showed that, while the PSD2 has provided significant added value in the EU payment services market**, **there are remaining and new challenges that justify its review**. The PSD2 met largely its objectives of increasing competition, innovation, consumer protection and security. Indeed, since the adoption of PSD2, there has been a considerable increase of players in the payment market, which has allowed for more innovation and thus greater choice for consumers. In addition, strong customer authentication (SCA) has proven a useful tool for the reduction of fraud. However, the complexity of SCA poses challenges from a financial inclusion perspective (especially elderly population and persons with low digital skills). In parallel, new forms of fraud (namely, social engineering) are arising, where strong customer authentication alone may not be sufficient. Also, there remain problems regarding divergent national transposition, implementation and supervision of the rules and requirements of PSD2 throughout the Union. Additionally, payment institutions and e-money institutions, while providing services that share many characteristics are subject to different regimes and requirements. Also, differently from credit institutions, payments institutions and e-money institutions do not have at this stage direct access to payment systems, (the political agreement reached during the Spanish presidency in Instant Payments Regulation grants said access to these institutions) which undermines the level playing field. Last, the pro-competitive effects of PSD2 open banking provisions, while having greatly contributed to the creation of new markets, have been partially mitigated by the existence of different barriers to accessing payments data.

3. **The Spanish Presidency of the EU Council, that started on the 1st of July 2023, immediately started working on these files.** The Presidency organized an introductory Council Working Group on July 12th, framing the discussion around the new structure of the PSD3/PSR package which comprises of a Directive and a Regulation in replacement of the current Directive (PSD2), and, at the same time, the merger of the former PSD2 and the Electronic Money Directive (EMD2), which, as pointed by some Member States, poses a few conceptual challenges, starting with the need for a clear distinction between electronic money and scriptural money stored in a payment account.

4. **The Presidency strived to promote an open and wide debate among Member States**. Already from the start of July, the Presidency invited Member States to provide their views on which topics should be prioritized during the discussions, given the complexity and amplitude of the proposals. During the semester, the Presidency held six Council Working Group meetings, while keeping a continuous engagement with national delegations, the European Commission and the industry. Also, the Presidency recognizes the efforts of those Member States that further contributed to the legislative process by submitting several non-papers to deepen the understanding of the Council Working Group on some concrete areas.

5. **The Presidency ensured coherence with other legislation in the field of digital finance and payments discussed in the Council,** for instance with the proposal for Instant Payments Regulation. In this context, the Presidency agreed not to initiate discussions on the provisions of the PSD2 review regarding access to payment systems until the negotiation of the Instant Payments Regulation is concluded. The political agreement reached with the European Parliament on the Instant Payments proposal includes amendments to the Settlement Finality Directive to allow payment institutions and e-money institutions to directly access designated payment systems. The amendment constitutes a significant step regarding competition in payment services. Cooperation with the Council Working Party discussing the proposal for a Regulation on a framework for Financial Data Access ensured transparency among delegations on how each of the files was evolving and allowed Member States to raise concerns on topics common to both proposals (namely, moving from open banking to open finance) or to put light on the remaining specificities of open banking, such as the absence of contractual relations between third party providers and account servicing payment service providers.

6. **The Presidency put fraud at the center of the discussions.** Fraud is a key challenge for EU citizens as regards trust in digital means of payments, primarily due to the rapid emergence of new types of fraud (in particular, social engineering fraud through digital means of payment). Member States recognize the need to adjust the currently existing rules for fraud prevention to new business models and market developments that have emerged since the implementation of PSD2 (e.g., the tokenization of payment instruments mentioned below). In addition, the Presidency believes fighting against fraud constitutes one of the main guiding principles of the proposal affecting the scope, the definitions, the authorization and supervision regime, as well as many rights and obligations of the different actors or the tools given to payment service providers to efficiently tackle this issue. The Presidency believes that organizing thematic debates helps having transversal and profound discussions.

7. **The Presidency progress report on the work of the Council Working Party on the PSD PSR file represents the Presidency view on the progress achieved during the Spanish Presidency of the Council**, and it does not preclude any future discussion or decision of the Council regarding the content of the proposals.

8. **The Presidency will share with the incoming Belgian Presidency the technical work and drafting suggestions that have been prepared and discussed in the Council working party during the Spanish Presidency.** As the technical debates have moved forward, the Spanish Presidency has worked during the whole semester on concrete drafting suggestions that have been frequently shared with Member States for scrutiny and may serve as the basis for more in-depth discussions going forward. Spain considers that those materials constitute a good starting point for the work ahead and is ready to collaborate with the Belgian Presidency in the upcoming months.

II. A REVISION OF THE FRAUD REGIME IN THE PAYMENTS PACKAGE

Need for clarity on authorized and unauthorized transactions to allocate liabilities

9. **During the discussions in the Council Working Party on the fraud regime, the majority of Member States argued for the need to clearly delineate authorized and unauthorized transactions as a first step.** While the concept of authentication refers to a technical process of verifying the identity of the payer or the validity of the use of a specific payment instrument, the notion of authorization includes the element of the payer´s will. For the next months, Member States have expressed their wish to deepen the debates around the provisions that regulate the liability of the payer, of the payment service provider or of the technical service providers and, also, possibly, between the latter and technical service providers or operators of payment schemes. The practical scope of this discussion will allow, namely, a clarification on the extension of Article 59 of the PSR Proposal ('PSP's liability for impersonation fraud'), which is limited to 'fraudulent authorized payment transactions'.

Gross negligence is one of the key elements to improve anti-fraud measures

10. **Generally, Member States agreed on the need to clarify the concept of gross negligence given its relevance for allocating liabilities in case of fraudulent transactions.** The concept of "gross negligence on the side of the payer" is key to the respective liabilities of the payer and of the payment service provider. However, the assessment of gross negligence in the behavior of the payer could have consequences in the payer's incentives to act vigilantly to prevent fraud and could result in a possible loss of protection of the payer. Hence, the Presidency considers that further work is needed on this fundamental concept.

11. **Most Member States agreed that a non-exhaustive list of examples could further illustrate the concept of gross negligence and ensure a common understanding of this notion.** Most Member States noted difficulties in having a definition of gross negligence in the provisions of the text considering the heterogeneity of national civil laws that have interpreted so far this notion. Therefore, most Member States have expressed the will to include a list of examples in the recitals of the Regulation. However, some Member States also highlighted the challenge of elaborating a list of examples that might become outdated relatively quickly or even used by fraudsters to elaborate new social engineering methods, and hence consider that an EBA Regulatory technical standards in the topic would be a great complimentary to the level 1 provisions. Several Member States also generally agree to include a non-exhaustive list of illustrating criteria to help assessing the payer's gross negligence. Nevertheless, further work is necessary to draft such list, with the possible help of the respective case laws of Member States.

Cooperation and information sharing agreements between entities are valuable tools

12. **Another key element of the fight against fraud is cooperation among all actors in the payments market.** In this sense, most Member States welcomed the proposal of the Commission to include electronic communication service providers in the scope of the Regulation to facilitate cooperation when a payment service provider detects that the electronic communication network is being used to commit fraud. The Presidency considers that further work is needed in delineating the scope and consequences of this obligation, determining whether this cooperation also involves sharing of relevant (personal) data, and the conditions of a possible liability of the electronic communication service provider in case of breach of their obligations. Also, several Member States argued for the extension of the cooperation requirement to online platforms hosting content that could trigger fraudulent transactions.

13. **Generally, Member States agreed that cooperation among payment service providers through information sharing agreements is also a very powerful tool to combat fraud.** The Regulation proposal of the Commission includes the option for payment service providers to enter into information sharing agreements among themselves in order to share information, such as IBAN, that is linked to fraudulent transactions, within the limits of the General Data Protection Regulation (GDPR). Additionally, most Member States supported extending the scope of the information to be shared in order to facilitate fraud prevention, (due to the limitations which the sole sharing of IBAN allows, namely, hindering the possibility for payment service providers to assess if an individual has a 'track record' on fraud-related cases), always in full compliance with the GDPR. Some Member States also supported to make this information sharing mandatory. Moreover, some Member States also agreed that information sharing between payment service providers and other relevant authorities could be a powerful tool to combat fraud that this issue should be addressed. Further discussion is needed on specifying these relevant authorities.

Member States recognized the need to further discuss the issuance of virtual IBANs

14. **Most Member States acknowledged the risks that could be posed by the irregular use of virtual IBANs.** While recognising the benefits of these additional identifiers for certain uses, such as contributing to the fight of certain unlawful practices, such as IBAN discrimination, most Member States were also in favor of revisiting this matter once the EBA publishes its evidence gathering exercise on the uses of virtual IBANs, expected for Q12024.

Strong customer authentication should still be at the centre of fraud combatting, also bearing in mind the need to preserve financial inclusion

15. **Member States agreed on the important role of strong customer authentication (SCA), introduced in PSD2, to combat fraud.** Under this procedure, the payer authentication needs to be based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is). Generally, Member States agreed that the new provisions could contribute to further clarify and harmonize the rules on SCA. Nonetheless, most Member States pointed out that the new Regulation should not change the existing requirement of performing SCA based on two or more elements that necessarily belong to different categories, since this characteristic has proven useful in the fight against fraud and is already well-established within the payments market as a procedure applied by payment service providers and generally understood by users. However, a minority of Member States suggested that it should be possible to use elements from the same category as long as they are independent from each other (for instance, elements related to biometrics and behavior under the inherence category).The Presidency suggests exploring these two different approaches further. Additionally, most Member States supported the Presidency's suggestion to highlight the importance of performing SCA when creating a token of a payment instrument or enrolling a payment card, a technical procedure that would reinforce the security in the market for digital wallets and reduce fraudulent enrolment of payment cards.

.

16. **Member States considered it relevant to reflect upon the relation between SCA and liability**. The SCA rules allow payment service providers, to voluntarily exempt the obligation to perform SCA in certain cases. The Presidency considers that further work is needed on the liability regime for the payment service providers that voluntarily exempt SCA.

17. **Member States agree to clarify the concept and implications of merchant-initiated transactions (MITs) and mail order telephone order transactions (MOTOs).** Merchant-initiated transactions are gaining popularity in the digital economy since they constitute a key ingredient of business models based on subscriptions, where the payer does not need to authenticate himself prior to a payment transaction being executed. In order to prevent fraud in this kind of transactions, some Member States find it key that the SCA is performed when setting up the mandate to authorize subsequent payment transactions.

18. **During the discussions, Member States agreed on the importance of financial inclusion when setting the SCA rules.** The fight against fraud can create problems of financial exclusion especially for those persons with low digital skills and elderly population. Member States agree that the performance of SCA cannot generally be dependent on the possession of a smart device (e.g., such as a mobile device). Payment service providers should enable vulnerable people to perform SCA with accessible instruments.

Financial literacy and fraud awareness are important complementary measures to fulfil anti-fraud objectives

19. **Member States have a common understanding on the high importance of financial literacy and fraud awareness** and agreed to explore additional safeguards in the Regulation proposal. In this context, the Presidency recalled the current obligation under Directive 2019/713[1] for Member States to take appropriate action, including through the internet, such as information and awareness-raising campaigns and research and education programs, aimed to reduce overall fraud, raise awareness and reduce the risk of becoming a victim of fraud.

III. SCOPE OF THE PAYMENTS PACKAGE

20. **The discussion on fraud is also connected to the scope of the Directive and the Regulation**. A key element of the discussion was to provide absolute clarity on the scope of the Regulation. Many non-financial entities, although not subject to authorization under the Directive, have important obligations under the Regulation. The Presidency believes that if this is not reflected upfront in the positive scope of the Regulation, this may lead to legal uncertainty compromising the level playing field and fight against fraud, key objectives of the Regulation.

[1] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

Clarifying the scope of the Package, including technical services providers, operators of payment systems and schemes, electronic communication service providers and cash activities, is key for supervisory objectives and financial inclusion

21. **Member States agreed to clarify the positive scope of the Regulation for technical service providers, operators of payment systems and schemes and electronic communication service providers.** In this sense, it would be clearer to express that some non-financial entities, that do not provide payment services, such as technical service providers, operators of payment systems and schemes, and providers of electronic communication services are all within the scope of the Regulation for the purposes of certain provisions. Most of these provisions are related to the fight against fraud (for example, liability of technical service providers when supporting to or directly performing the strong customer authentication) or to the level playing field (for example, the right to access to payment systems by payment institutions and e-money institutions). Also, some Member States suggested that further debate is needed to identify categories of critical technical service providers (such as payment processors or digital wallets) for the purposes of adding, among others, some requirements in terms of operational resilience, as contemplated in the review clause of the Regulation 2022/2554 (DORA) or ensure supervision of these actors, while ensuring conformity with the Eurosystem's PISA framework. Furthermore, it was also pointed out that this extension of the scope of the Regulation must be accompanied by a careful assessment of the remit of national authorities to supervise such non-financial entities. In this context, some Member States have also pointed out that the introduction of any additional provisions should avoid replicating provisions and obligations that are already regulated under existing EU legislative acts. Against this background, it may be useful for the discussions ahead to analyse which obligations are already covered by other EU regulations and whether they provide the functional equivalent to the obligations proposed in the Payments Package.

22. **Cash availability and financial inclusion is a key element of the Payments Package.** In this sense, Member States agreed on the importance to ensure consumer protection by requiring cashback providers to be transparent on possible fees. Also, Member States welcomed the opportunity to discuss the inclusion of cash-in-shop services in the Regulation, attending to their possible role the legal regime provided in the Directive. Some Member States consider that there are risks and challenges associated with this service, while some others do not share this view. Lastly, Member States welcomed the consideration of ATM deployers (formerly known as independent ATMs) as payment institutions with a requirement to register upon the national competent authority.

23. **The Presidency considers that further work is needed on the exclusions to the Regulation.** In the case of the limited network exemption, some Member States were in favour of further narrowing the applicability of this exemption, as a significant volume of transactions that are being processed outside of the scope of the Regulation. However, other Member States considered to further explore the relevance of the exemption of business-to-business models. Member States agreed that certain payment instruments, narrowly linked to national law, such as meal vouchers or social vouchers, should remain outside of the scope of the Regulation.

Clarity on the authorization requirements and smoother transitional regime are welcomed.

24. **Regarding the authorization process for payment institutions, the Presidency focused on further clarifying the authorization requirements, and on smoothing the transitional regime for existing payment institutions once PSD3 comes into force.** The Presidency conducted a gap exercise to ensure that existing payment institutions and e-money institutions only need to comply with those additional requirements under the new package as compared to the previous version of the Directive with sufficient time granted to both authorized institutions and national competent authorities in charge of such re-assessment. In addition, the majority of Member States supported the Presidency's proposal of introducing a grandfathering regime for ATM deployers, to facilitate the transition towards the new registration regime.