To: Mairead McGuinness
Commissioner for Financial services, Financial stability and Capital Markets Union
European Commission

Brussels, 26 May 2023

Subject: Review of the second Payment Services Directive

Dear Commissioner McGuinness,

We are writing to you with regard to the ongoing review of the second Payment Services Directive (PSD2) that is expected to lead to a legislative proposal later this quarter. The Payment Services Directive is a cornerstone of EU payments legislation and hence fundamentally important in ensuring high levels of consumer protection and security of transactions, and fostering an innovative and competitive EU payments market, that needs to be characterised by a level playing field between all providers of payment services. European banks are keen to continue to contribute to the realisation of these objectives.

Ahead of the finalisation of this review, we would like to highlight two aspects that are crucial for the banking sector: first, combating authorised push payment scams and fraud, and second, ensuring a fair distribution of value and risk in open banking.

1. Combating Authorised Push Payment scams

Online scams (or, more accurately, Authorised Push Payment (APP) scams) are a major social problem. The issue is increasingly important in a context where methods continuously evolve, with new ways to exploit human vulnerabilities and mislead customers. It is clear that the fight against scams is a priority, both for our members and for regulators and supervisors. In the fight against APP scams in particular, the emphasis should be on preventing the scam and identifying the criminals. All parties in the chain, including governments, companies and consumers, must be part of the fight against scams.

APP scams occur when the consumer is misled into authorising a payment. This is facilitated by the fact that it is easy for scammers to act anonymously and pretend to be someone else on the internet. For example, in banking voice scams (vishing), scammers use prepaid SIM cards to call their victims completely anonymously. In dating scams, scammers create fake profiles. Similarly, in help request scams, scammers

pretend to be an acquaintance or friend of the victim via WhatsApp, for example. Online shopping scams are also largely possible due to the anonymity of buyers and sellers on the internet. Preventing such scams requires efforts from all entities in the chain, including telecom operators, big tech companies, social media, messaging platforms and digital marketplaces.

In addressing this important issue, a number of measures should be taken as part of the PSD2 review. Our main points are briefly listed below (for more detailed proposals please see the Annex to this letter).

- **All relevant actors must come under legal obligations to fight scams**
  Due to the fact that scams occur outside the payment transaction, it is extremely challenging for banks to detect them. Banks do not know the context that leads to a payment, and are unaware of the consumer's intention for it - they are the last part of the chain. This limits banks' capabilities to prevent scams when the customer has given the instruction for a payment. We would therefore urge you to **bring under adequate and proportionate legal obligations for fraud prevention, detection and mitigation, all actors in the relevant areas and in the payments chain**, including telecom operators, internet platforms, and parties that participate in the user authentication or payment initiation, such as wallet providers**.** With the recent Digital Operational Resilience Act (DORA), the Commission marked a milestone in cyber security and resilience in financial services by acknowledging the importance of all actors in the ecosystem playing their part to that end. As a result, DORA introduces, among others, a new oversight framework for critical third-party providers of ICT services to banks. The review of PSD2 should take inspiration from the approach taken in DORA.

- **A generalised refund right would increase scams**
  PSD2 correctly ties any refund rights to the existence of an unauthorized payment. It is paramount to maintain this principle. In particular, **measures to combat fraud should not include a generalised refund right for authorised payments** as this would eventually compromise the resilience both of consumers and of PSPs, while significantly increasing the costs of payments. More specifically:
  - **A more comprehensive reimbursement policy would support the 'criminal business model' and therefore make EU citizens more vulnerable to scams.** It would contribute to increasing fraud levels and moral hazard, as consumers would not have an incentive to be vigilant and would gradually pay less attention to signs of scams when instructing their payments. This would result in fraudsters being encouraged to perpetrate fraud at the expense of PSPs, using a generalised refund possibility to their advantage. In the long run, disincentivising consumers from keeping alert to online scams would affect negatively their general digital security and wellbeing, as reduced attention to online risks would spill over their use of all kinds of digital services, leaving them more exposed to cyber risks.

  - Moreover, a refund right for authorised transactions **would bring significant uncertainty in the payment system and to payment finality** by essentially considering all payments non-final – it would conflict with an underlying principle and cornerstone of the legal framework to the detriment of PSPs, consumers and businesses alike. Such a refund right would

inevitably also lead to more friction in the customer journey as banks and other PSPs would have to attempt to assess the context of each payment a customer makes, and might reduce the incentives to develop and implement user-friendly SCA solutions in order to get additional assurance about the will of the customer. In general, a refund right for authorised payments would not be in line with the principle of proportionality.

  - If the liability were to be put on PSPs also for authorised payments, we see a potential risk that the incentives to develop and implement user-friendly SCA solutions would suffer. Furthermore, **a liability shift would come with a risk of reducing competition in the financial sector**, as covering for the increased risk from providing payments services would be harder for smaller banks and PSPs.

- **Consumer awareness and resilience need joint efforts**
  Strengthening consumer resilience to online risks through education and awareness-raising is a continuous and large-scale endeavour. Numerous activities are currently undertaken by banks and other actors, often in public-private partnerships, aimed at effectively promoting financial and digital literacy. Banks see this as part of their responsibility towards their customers and would welcome more joint efforts with the public sector to further promote this shared goal at larger scale and for all segments of the population. In addition to this, efforts to better understand how fraud patterns originate in the sphere of all actors offering digital services, such as internet platforms, search engines or telecommunication companies, and how these can be effectively reduced, should be undertaken.

- **Targeted measures needed for prevention and mitigation**
  The revised PSD should include targeted amendments to allow PSPs to better prevent and mitigate scams and fraud more generally, e.g. in terms of information sharing and the possibility to urgently block incoming funds suspected of being fraudulent in order to prevent losses. Legal tools should be provided for PSPs (both the payer's PSP and the payee's PSP) to e.g. suspend the provision of payment services when they detect behaviours suspicious of fraud. That includes the initiation of payments, even instant payments, and the obligation to make funds immediately available to the payee.

2. Fair distribution of value and risk in open banking

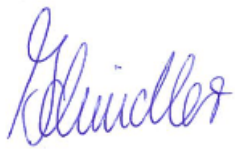
A second crucial aspect of the PSD2 review is the opportunity **to create an 'open banking' framework with fair distribution of value and risk that corrects the imbalances resulting from the approach taken in PSD2**. A key lesson learnt from the assessment of the PSD2 implementation is that a competitive ecosystem only works when there are benefits for all.

The reviewed legislation should guarantee that both sides of the market can draw benefits from open banking, which is the only way to create a thriving and healthy open banking ecosystem. Therefore, the possibility for Account Servicing PSPs (ASPSPs) to charge Third Party Providers (TPPs) for the access to

payment accounts should be allowed. This would align with the Commission's overarching data-sharing strategy, as seen already in the negotiations on the Data Act, which serves as a foundation for the upcoming sector-specific legislation on open finance. Alignment between the Payment Services Directive and the Data Act would contribute significantly to the much needed regulatory harmonisation of the Single Market. Importantly, a fair distribution of value and risk would provide incentives for ASPSPs and create the basis for future development of the market by delivering and maintaining high quality and high performing APIs, while not disrupting the business models of TPPs. Moreover, it would provide ASPSPs compensation for ongoing costs while facilitating account access. It can reasonably be expected that the systems will need to be continuously maintained, updated and improved, to support the further growth of the market but also for cyber security and operational resilience purposes. Amending the PSD2 'legacy' to allow for compensation is a much-needed improvement.

We thank you for your consideration of these fundamental points for the European banking sector.

Yours sincerely,



Nina Schindler	Wim Mijs	Peter Simon
CEO	CEO	Managing Director
European Association of Co-operative Banks	European Banking Federation	European Savings and Retail Banking Group

Annex: Amendments needed in PSD2 review to help PSPs fight scams and fraud

1. **Obligations on non-PSPs:**

- An obligation for **telecom operators** to prevent that text messages or calls appear to come from a PSP, to block text messages and spoofed numbers, immediately block mobile numbers used to commit fraud and to screen for bulk messages being sent including URLs. A European solution providing a register of alias of SMS sender in order to avoid spoofing could be explored.
- **Software providers** (i.e. Apple, Android, Huawei) to technically prevent SMS or phone calls that are displayed with the same alias than a bank, from being queued in the same thread.
- An obligation on **internet platforms** to control that the information provided is correct and to verify the identity of their customers and assess their risk profile. Further measures that could be considered include the closure or suspension of potentially fake/scam websites in a centralized manner, the revocation of the authentication web certificate of the website and stricter requirements during the verification process of Hosting Providers for opening a website.
- Commitment to Know Your Customer (KYC) and Strong Customer Authentication (SCA) for all parties in the chain: KYC and SCA should become the standard for all entities offering digital services (including telecom operators, social media, message platforms and digital marketplaces).
- Establishing a legal basis for data sharing with different parties in the chain, which would allow them to make a better assessment of whether any action is fraudulent and then take the right measures. A desirable outcome, for example, is data sharing between banks and telecommunications companies. Banks see that scammers often call victims to scam them with a babbling trick. Allowing banks to give phone numbers from which victims are called to telecommunication companies, they could take action against the users behind these connections. Another example is data cooperation to combat dating fraud: allowing banks to pass on which profiles victims are contacted from via social media or dating sites, the providers of these platforms could take action against these users and permanently ban them from their platforms. However, to enable this kind of data sharing, a clear legal basis needs to be established. Since this information could qualify as data relating to criminal offences (the IBANs used in scams or by money mules say something about the involvement of the data subject in such criminal offences), a clear legal basis should be created, allowing the processing of data relating to criminal offences and providing for appropriate safeguards for the rights and freedoms of the data subjects.

2. Amendments to help PSPs prevent scams and fraud

In general we suggest to keep in mind the distinction between payments fraud and payment scam. Payment fraud occurs when the criminal gains access to the customer account and then initiates the payment. Payment scams occur when the consumer is misled and makes the payment him/herself - this is also known as authorised push payments scam. This distinction is meaningful for a variety of goals: addressing the awareness actions of the institutions, identifying the gross negligence of the customer and improving the quality of the fraud reporting process (by including only frauds and not scams in the data, which would enable to better evaluate the effectiveness of a PSP's internal monitoring systems).

- Providing for the possibility and the legal grounds for legitimate exchange of information relating to identified or identifiable natural or legal persons between the PSPs in the payments chain, with the appropriate safeguards. For example for the processing of data for the sharing of IBANs of "mule accounts" and other relevant information, between PSPs through appropriate means , for example warning systems. These could help that payments to accounts that belong to a money mule or to an account that has been involved in a criminal activity to be put on hold before the money further disappears. Currently, the situation differs across member states; under some national interpretations, information sharing is permitted, whereas in other communities do not consider the interplay with GDPR clear enough, or even that there are legal grounds available, in spite of current article 94(1) of PSD2. Since this information could qualify as data relating to criminal offences (the IBANS used in scams or by money mules say something about the involvement of the data subject in such criminal offences), a clear legal basis should be created, allowing the processing of data relating to criminal offences and providing for appropriate safeguards for the rights and freedoms of the data subjects.
- Strengthening collaboration among NCAs so that loopholes in countries that record a very high rate of fraud are avoided.

3. Amendments to help PSPs remedy scams and fraud

- Reconciling article 64 of PSD2 with Guideline 1 *"Payment transactions and fraudulent payment transactions"* of the EBA Guidelines on fraud reporting under the PSD2 in order to ensure that the same concept of un/authorized transactions is foreseen and is clear for all providers.
- Not having to make funds immediately available to the beneficiary as the beneficiary bank or to execute the payment when there is suspicion or evidence of fraud (which should apply also in the case of instant payments). The elements which constitute 'suspicion/evidence of fraud' would benefit from clear definition/criteria to allow PSPs to properly apply the rule also

according to Article 73(1). They could be determined in relationship with fraud patterns previously observed by PSPs, and at national authorities' disposal, as well as commonly observed patterns defined by the relevant authorities and recommended to PSPs to be followed. Both are needed to fight fraud in a changing environment where fraud moves.

- Recovering or at least blocking funds from the payee's account (when available) for transactions under fraud suspicion with the necessary caution (compared to fraud patterns defined), and in particular if there is a formal complaint of fraud, and formal police declaration by any of the parties involved. The possibility for banks to recover funds (if still available) that have been wrongly credited should be included in PSD, especially by clarifying what the PSP's rights and obligations are when it identifies a fraudster among its customers. In some cases those efforts are made but rules should be set at EU level to facilitate the blocking and retrieving of money transferred fraudulently to address legal and operational issues that are slowing down the process of retrieving the money fraudulently transferred, especially cross-border. For this purpose and considering that Article 87 states that the payee's PSP shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account unless where certain conditions are met, a new condition - point (c) – should be added in article 87 concerning availability of funds as follows: *the transaction is not under fraud suspicion*. This obligation shall also apply to payments within one payment service provider (on-us transactions).
- Allowing payer's PSPs to freeze the execution of payment transactions if they find evidence or suspect (always according to patterns defined) that the payment order is a fraudulent one.
- Identifying common rules and procedures to make effective and efficient the regulatory provision to be introduced related to the cooperation required from PSPs in order to recover the user's funds, making reasonable efforts also regarding the communication of all relevant information and personal data, in case of fraud. In particular, the required dispositions should consider the following aspects:
    - A non-exhaustive list of information that could be provided in order to have a standardization starting point of the available and useful information that should be exchanged. The list should be conceived future oriented and therefore to be a starting point but not limited to, in order to accommodate evolution of fraud modus operandi.
    - In case of a complaint of a payer's towards their PSP, supported by appropriate documents (e.g. police report or other evidence) in order for the PSP of the payee to provide the personal data of the payee to the PSP of the payer that the payer presumes with reasonable certainty to be directly or indirectly involved in fraud, we need to balance the respect of privacy of the beneficiary and his/her rights under GDPR with the interest of the payer and of the payer's PSP to avail themselves of the personal data of the beneficiary.

- We fully concur with the caution expressed by the EBA in its recent Opinion on its technical advice on the review of PSD2[1] (par. 266-271) about the changes to the current rules in connection with the possible usage of additional elements to identify the payee and various possibilities of name checking.

4. Narrowing down the technical provider exemption

Providers that are material to the provision of payment services, such as wallet providers and parties that participate in the authentication of the user currently fall outside the scope of PSD2. Article 3(j) providing an exclusion for technical service providers should be narrowed, as the full exclusion of all the different market participants that currently fall under this exclusion, is no longer adequate in light of market developments. It is important that all providers that are material to the provision of payment services are included in the scope and are covered by rules pertaining to transparency, business conduct and operational rules, fraud mitigation and prevention, security and operational resilience, and all have their rights, responsibilities, and duties. The criteria for inclusion should not only focus on the risks that such market participants pose to payment systems but should also consider how they impact all other participants in the payments chain, as many of the currently excluded market participants play a crucial role in segments material to the provision of payment services. There may not be a one-size-fits-all criterion but different criteria may need to be defined depending on the type of actor. Where legal obligations already exist, as in the case of payment initiation through a Payment Initiation Service Provider (PISP), these need to be reviewed with the goal of increasing their efficiency and sharpening the responsibilities of the actors involved.

For example, any party that participates in the authentication of a Payment Service User should be under the obligation to provide all relevant details of the authentication to the issuer/payer PSP (that is the first point of contact for the user claim) and might need to investigate whether it is liable for the authentication, but often relies on other parties (e.g., wallet providers, device manufacturers, payment HUBs) for carrying out SCA. Without a legal framework setting specific obligations on these parties, banks have very little power towards them. We acknowledge the EBA request (paragraph 314 of the EBA response to the Call for Advice) to clarify whether these situations would require an outsourcing agreement, however we are opposed to such an approach for several reasons and would call for legal requirements for parties participating in authentication instead. It would not be possible to apply outsourcing principles in such cases with the current outsourcing provisions as the idea of every delegator regularly auditing the company the authentication was delegated to, is impossible. Providers of such solutions would need to contract with several thousand PSPs and allow all such PSPs to monitor them. Every single PSP would need to assess the solution towards the same legal requirements. Providers often do not see these solutions as their main business model and they are therefore not willing to go through these processes with every single PSP. They may also have security

[1] EBA's response to the Call for advice on the review of PSD2.pdf (europa.eu)

concerns to share sensitive details about the solution. Also from a supervision perspective it seems more efficient to directly supervise a solution once, instead of supervising it indirectly via supervision of every single PSP that uses it. The possibilities of a single PSP to influence such providers are very limited in practice. Hence, rules should be defined for delegated payment authenticator service providers, which could then be audited and supervised by the NCAs. It should still be up to each ASPSP to decide which solution to use.

Furthermore, wallet providers should be subject to PSD at least with respect to security, antifraud collaboration requirements and liability provisions to the benefit of customers and of the security of the market. Major processors should be also brought into scope, even if they do not enter into the possession of funds or interact directly with PSUs, as any disruption in their services would cause major problems for PSPs in the provision of payment services. In this case, the rules should be focused on security, antifraud and operational resilience.

5. **Other aspects:**
   - Clarification of the **notions of "negligence" and "manipulation of the payer**". As for the first concept, clarifying its meaning (even by providing a wider range of examples, than those available as of today) would harmonize rules across the European Union, and reduce uncertainty when it comes to customers' refunds. The definition of (gross) negligence is very important for the correct distribution of responsibility and it becomes increasingly challenging with the development of innovative payment methods and solutions, therefore an effort to define at least its key elements in a harmonised manner at EU level should be made.. With regards to the "manipulation of the payer by the fraudster", we point out that, given the rise in social engineering-based fraud, it would be opportune to distinguish circumstances in which the fraud is perpetrated through technical elements (e.g., malware) and the instances in which the enabling factor is social engineering (e.g., voice phishing, romance scam, whatsapp scam in which case customers make the payment themselves following, for instance, the fraudsters' directions). The distinction would serve to allow a correct distribution of responsibility, in case of fraud, between financial institutions and customers: that is, in case of exploitation of social engineering techniques, customers' due diligence would allow them to identify fraudulent communication attempts (e.g., if during a phone call an operator asks the customer for their social credentials, they should know not to give them). Moreover, a better clarification is needed on how to classify those situations in which the customer is involved in the execution of the payment, namely those in which he/she has been induced by the fraudster to act in a certain way thus contributing/giving rise to the fraud and the PSP cannot do anything to interrupt the transaction. A reduction of the negligence degree is required especially if PSP can prove that relevant awareness and cautionary warnings have been issued for the customer to avoid certain behaviours. Clarification is required for legal security reasons. EBA could issue RTS for this purpose.

- According to PSD2, in case of unauthorized transactions, the banks must refund the client immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction. However, 24 hours are not enough to carry out accurate analysis of the event and liability, especially regarding the issue of gross negligence of the user. We consider it appropriate to extend the deadline for refunding, aligned with the delays for complaints handling (15 business days), while ensuring that the refund has the end of the business day following the dispute as value date.
- Transactions initiated through third party providers (TPPs) lack rich information for the ASPSPs in the fraud prevention process, compared to the elements they have when the user initiates a transaction directly through the ASPAP interface (i.e. related to navigation, IP, device…). SCA being the only security measure in ASPSPs' hands makes the transaction safe, but it is not enough from fraud prevention perspective. Therefore, TPPs should be obliged to apply the same or equivalent preventive measures as ASPSPs and be responsible of their own thoroughness in fraud prevention. Therefore, they should also face their liability accordingly. As a consequence, since the amount of information with regards to the online sessions as well as transactional data are limited for ASPSPs, the transactional fraud decline rates through TPP access should not be obliged to be similar to direct access.
- Legal tools should be provided for PSPs (both the payer's PSP and the payee's PSP) to suspend the provision of payment services when they detect suspicious behaviors of fraud. That includes the initiation of payments, even instant payments, and the obligation to make funds immediately available to the payee.
- From a technical perspective, PSPs are only able to see the device used for the insert and for the authorization of the transaction. Therefore, we see the limit of liability of PSPs, if no new or different device than the customer device is used for the transaction. If there is a new device, however, the PSP should have the possibility to block the transaction and to clarify it with the customer. We would like to avoid a discussion about "unusual behaviour or transaction" of the customer and the definition thereof.
- Finally, it would be helpful if institutions were explicitly allowed to temporarily lower disposition limits when suspicious activity is observed, provided that the customer is informed. This would allow the amount of loss to be reduced in the case of actual fraud without blocking the customer's account completely and would thus be a less severe measure in cases of uncertainty.