Subject: Joint Industry Letter for Effective and Efficient Fraud Prevention in Europe

Brussels, 10 June 2024: As representatives of the digital payments and technology sectors, we would like to express our appreciation for the ongoing work on the EU Payments Package.

Part of the Payments Package addresses an issue that has gained increased relevance in the digital economy: fraud. As the EBA Opinion on new types of payment fraud (April 2024) finds[1], whilst Strong Customer Authentication has been successful in mitigating fraud based on stealing customer's credentials, new security measures are necessary as increasingly sophisticated types of frauds have been surfacing.

The EU Commission' draft proposal for the Payments Services Regulation (PSR) already includes provisions to prevent and mitigate fraud risks, such as verification of payee for all credit transfers and data sharing among payment service providers (PSPs) for fraud detection and prevention.

Yet, ***we believe certain improvements are needed to reach the objective that the industry, policymakers, and consumers share: reduce frauds.*** Below we articulate our policy recommendations, which we believe would make Europe less prone to scams. Later in this letter, we also address the most controversial PSR draft provisions on the topic, such as fraud liability, authorised/unauthorised fraud definition and gross negligence.

* * *

1. POLICY RECOMMENDATIONS

1.1. Tackling the whole fraud chain

We recommend a holistic and systemic approach in addressing fraud. We are prepared to elaborate joint-industry codes of conduct and support the establishment of a cross-industry, EU-wide task force to coordinate efforts between industry and regulators in the fight against fraud.

Tackling fraud in the digital ecosystem requires a dynamic approach that spans across all actors involved. A comprehensive solution must address each link in the fraud chain to be effective: not only payments services providers (or PSPs), but also telecommunication companies and online platforms. We, as an industry, are prepared to work with legislators to develop fit-for-purpose measures to fight fraud, as the current proposal falls short of addressing the challenge in its entirety. While the PSR draft includes requirements on electronic communications service providers to cooperate with PSPs to fight against fraud[2], there is no provision involving telecommunications providers to work towards the same objective. Also, the PSR draft fails to reference online platforms efforts to remove fraudulent content: the Digital Services Act (DSA) should be cross-referenced in the PSR, as it aims to ensure a safe, predictable and trusted online environment. In particular, the DSA allows the Commission to initiate drafting of codes of conduct, including setting out

[1] EBA Opinion on new types of payment fraud

[2] PSR, Article 59(5)

commitments to adopt specific risk mitigation measures. We would suggest expanding this practice to payment fraud prevention, e.g., by introducing *Do Not Originate Lists* and *Sender ID Registers* commitments for telecommunication companies, along with the use of advanced machine learning technology/AI systems to proactively remove fraudulent content on online platforms. To ensure optimal coordination across industries, we would recommend setting a dedicated taskforce of EU regulators including payments, technology and telecommunication sectors. For instance, in the payments sector, the Euro Retail Payments Board has created a Working Group on Fraud, which can play a key role for joint-industry efforts.

1.2. Extended Data Sharing

We recommend extending the ability to establish voluntary data sharing arrangements for the transaction monitoring purposes to include electronic communications service providers, online platforms, technical services providers, and competent authorities under the existing data sharing frameworks.

We support the provisions of the draft PSR allowing PSPs to voluntarily enter information sharing arrangements, to better detect fraudulent payment transactions and protect their customers. However, information sharing of personal identifiers alone is not enough: the list should be extended to at least name, organisation number, modus operandi and other relevant transaction information to the extent it is available. Also, fraud prevention efforts would benefit from information being provided to PSPs by all participants of the ecosystem - such as electronic communications service providers, and online platforms and would require clear data sharing rules, and possibly lead to the setting-up of a platform where the exchange takes place. The PSR adoption allows for a unique opportunity to support collaborative efforts and shape the process. Involvement of both European and national competent authorities is needed to swiftly address new fraud patterns and the threats private and public entities face.

1.3. Educational Campaigns

We recommend collaboration between industry and public sectors to enhance financial literacy and prevent fraud by effective information campaigns.

Education plays a crucial role in preventing fraud by raising public awareness about the emerging types of scams and the everchanging tactics used by fraudsters. By helping consumers and businesses to recognize and respond to fraudulent activities, these campaigns empower vulnerable individuals and businesses to protect themselves proactively. Education on safe online practices and accessible information on the importance of secure transactions can significantly reduce the likelihood of becoming fraud victims. An academic study - published in the Journal of Economic Behaviour & Organisation[3] - shows that concise, online educational interventions can significantly reduce susceptibility to investment fraud.

1.4. Verification of Payee

[3] https://www.sciencedirect.com/science/article/abs/pii/S0167268122001238

We fully support the European Payments Council's work on establishing the SEPA Verification of Payee scheme. The scheme should be open to all PSPs, easy to use and future-proof.

The Instant Payments Regulation[4] mandates PSPs to provide verification of payee (also, VoP) services to customers making a SEPA instant or regular credit transfer. Matching the name and unique identifier (intended as going beyond IBAN only) of the payee is an important step in making bank transfers safer by reducing fraud and misdirected payments and building consumers' trust incentivizing adoption of these types of payments.

2. INDUSTRY CONSIDERATIONS ON THE PSR FRAUD PROVISIONS

The industry sector considers that liability allocation for authorised payment fraud is not a silver bullet to address the ever-changing threat and increased levels of impersonation fraud or scams. Below are our considerations on the alternative options that we propose to adopt during the PSR discussions to tackle the issue.

2.1 Fraud Liability

We warn against automatic fraud liability allocation for impersonation scams.

Art. 59 of the PSR establishes PSPs liability for impersonation scams. While we understand this approach intends to incentivize PSPs to better address scams, evidence from other jurisdictions suggest that this could lead to a series of unintended consequences, including moral hazard and eventually increase fraud.

The **UK** - which has been battling against Authorised Push Payments (or APP) for years - introduced the Contingent Reimbursement Model Code in 2019. Since then, the UK saw a 64% increase in APP Fraud by 2021; the Payment Services Regulator's recent APP Fraud Performance Data report finds that the firms with the highest reimbursement rate also had the highest rate of issuing fraud by value in the sector.[5] **Australia** choose to fight fraud by introducing mandatory industry codes[6]. The Chief of Financial Crime Risk at the National Australia Bank called the mandatory reimbursement regime a "*honeypot for organised crime*".[7] Mandating liability for all APP fraud/scams is a bonanza for fraudsters and fails to address the issue, which requires effective law enforcement and implementation of robust fraud prevention measures by ALL the actors in the chain (*see policy recommendation 1.1 above*).

2.2. Definition of Authorised and Unauthorised Fraud

[4] IPR Article 5c

[5] https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/, Metric A: percentage of reported APP fraud losses refunded by value + Metric B: Value of APP fraud sent per £ million of transactions.

[6] https://treasury.gov.au/sites/default/files/2023-11/c2023-464732-cp.pdf

[7] https://www.afr.com/companies/financial-services/refunding-scam-victims-creates-honeypot-for-organised-crime-nab-20230918-p5e5k9

We support a payment authorisation definition based on the authorization to execute a transaction without referring to subjective elements.

The industry is alarmed at the possibility to introduce in the PSR the subjective definition of payment transaction authorization, which would refer to the "*intent*" of the payer. Given the apparent legal and practical difficulties on how PSPs are supposed to detect the "*intent*" of the payer, this definition will only lead to increased litigation and lower consumer trust. In fact, we expect this approach to produce inconsistent customer outcomes and legal uncertainty across the EEA, as PSPs may interpret the payer's intent differently. We would strongly recommend to align with the European Central Bank fraud taxonomy instead, which identifies an payment transaction initiated by a fraudster and scams, and where a payer was manipulated to initiate a transaction as unauthorised.

2.3. Gross Negligence

We support including a non-exhaustive list of gross negligence examples in the PSR.

Including a non-exhaustive list of gross negligence examples at Level 1 legislation would provide clarity to both PSPs and consumers, and reduce arbitrary national approaches and litigation. We understand that the EU Council is considering the possible list of such examples, similar to the one used by the Bank of Lithuania in their fraud prevention guidelines[8], which we support. Should the original Commission draft on liability for authorised fraud be retained, we would then recommend adding (to either Article 59 or Recital 82), at least a specific example of gross negligence, such as :

> *"where the PSP has proactively flagged the risk of a transaction being fraudulent to the payment user, and the payment user has nevertheless proceeded to authorise such transaction".*

According to data presented by one of our industry members, users react to fraud warnings only in 50% of cases.

2.4. Unconditional refund right for MITs

We recommend to the EU Council to exclude unconditional refund rights for MITs.

The EU Parliament text proposes to exclude MIT (e.g., subscriptions, bill payments, and digital economy use-cases) from the unconditional ('no question asked') refund right currently set out for SEPA Direct Debit transactions. The European Parliament also helpfully proposes that the MIT exclusion applies to refund transactions initiated by the merchant.

2.5. Behavioural and environmental characteristics are valid SCA factors for inherence

We recommend the Council to recognise behavioural and environmental characteristics as valid factors of authentication.

The EU Parliament rightfully proposes that (1) acquirers must provide issuers with the data for transaction monitoring and that (2) environmental and behavioural characteristics are a valid SCA

[8] https://www.lb.lt/uploads/documents/docs/44226_77a36df7cd0c350012778525034c87fa.pdf

factor of 'inherence'. This could help expanding use of EMV 3DS for transaction monitoring purposes and fully aligns with the goal of establishing a future-proof regulatory regime, leveraging technology innovation to improve transactions authentication.

* * *

We continue supporting the EU Council work on the Payments Package and stand ready to continue engaging to ensure the final EU rules will be fit-for purpose and sustain digital growth, healthy competition and high consumer protection.