# ISPA Position Paper on the Payment Services Regulation

## What is the Payment Services Regulation?

In June 2023, the European Commission (EC) Directorate-General for Financial Stability, Financial Services and Capital Markets Union (FISMA) proposed a Payments Package including a new Payment Services Regulation (PSR).

In April 2024, the European Parliament's report on PSR (Article 59) expanded financial liability to electronic communications services providers (ECSPs) and online platforms, requiring them to "compensate" Payment Service Providers (PSPs) for payments made to victims if they fail to remove "fraudulent or illegal content" once it has been notified by a PSP. The liability of ECSPs and online platforms could be unlimited (no maximum cap on a consumer claim). Even if an ECSP or online platform takes down fraudulent or illegal content, users could still claim in their local court that it is liable.

Other obligations for ECSPs include incident management and fraud mitigation obligations (e.g. educational measures, guidelines for identifying and preventing fraud, and fraud reporting mechanisms). PSR also would impose information-sharing obligations among ECSPs, online platforms, and PSPs.

## Concerns with the European Parliament amendments

Holding ECSPs and online platforms liable and requiring a refund based on (too) broadly defined obligations will undermine effective cooperation to combat fraud and scams due to legal wrangling and blame shifting. This is counterproductive to resolving the core of the problem at hand: reducing the prevalence of fraud and scams.

The wording of the obligations, as proposed by the European Parliament, is not sufficiently thought through. This may refer to filtering, scanning, checking or blocking traffic, or (other) traffic management measures. Such measures have long been the subject of regulation (Net Neutrality Regulation, e-Privacy Directive) to which ECSPs are bound and which are at odds with the proposed obligations. Article 59 paragraph 5 of the proposal imposes an obligation that ECSPs cannot possibly fulfill for technical reasons ("to remove the fraudulent or illegal content which might be linked to the domain of online platforms"). The different legal context of ECSPs and online platforms should be considered.

Similarly, the definitions in the proposal on authorization highlight the intent of the payer. This is detached from procedural or objective benchmarks, rather than taking existing taxonomy's into account. The European Central Bank fraud taxonomy, for example, separates an unauthorized transaction as a payment initiated by a fraudster and scams, where a payer was manipulated to initiate a transaction.

Additionally, the bank sector should investigate further possibilities to introduce restrictions in payment flexibility for its customers to limit potential fraud and increase the protection of their customers against fraud.

Finally, the PSR should align with intermediary liability principles for intermediary services (including online platforms) under the Digital Services Act (DSA). The DSA provides that online platforms should not be liable for content they host if they do not have actual knowledge or awareness of its illegality, and, upon obtaining such knowledge or awareness, act expeditiously to remove or to disable access to the illegal content. The DSA additionally provides for specific information that a third party notification of illegal content should contain to enable the online platform to assess the presence of illegality and take action. Any requirements included in the PSR should not undermine this well-established conditional liability regime.

Fraud is a complex phenomenon that is evolving rapidly. The international and open nature of electronic communications networks makes it difficult to trace the network of the telecom operator used by the fraudulent party. While we understand that the liability approach intends to incentivize players in the fraud chain to target specific types of scams, we do not believe that this will lead to less fraud occurring and instead, could lead to a series of unintended consequences that ultimately will negatively impact customers.

**A better approach**

For more far-reaching measures to combat fraud, legal resources must be expanded, including to use and exchange relevant (personal) data between relevant parties to combat fraud while respecting the essence of e-privacy. The European Parliament's amendment does not contribute to this in any way and is even a step in the wrong direction.

The e-Privacy Directive is clearly outdated. Its revision has been ongoing for years, but it seems the draft e-Privacy Regulation might not be adopted after all. ECSPs need more flexibility and legal certainty to increase their capacities to combat fraud, which is essential to address the increasing capabilities of fraudsters, especially with the rise of artificial intelligence (incl. generative AI tools). ECSPs should be enabled with sufficient legal certainty to process and share telecommunication data (if needed) to efficiently fight fraud and adapt its efforts in that regard, while taking sufficient measures to protect individuals' right to privacy and data protection.

Anti-fraud measures must be designed based on an in-depth analysis of each type of fraud at both technical and legal levels and of the different parties in the chain. Experience shows that measures have limited effectiveness; unfortunately, there is no silver bullet. As soon as a certain type of fraud is tackled, the fraudster quickly adapts (waterbed effect). Remedies should be developed in collaboration so that they are targeted, flexible, feasible, effective, in short, efficient. The European Parliament's proposals do not take this into account. PSR is also incompatible with encryption, requiring content to be removed from encrypted communication channels.

ECSPs only play a secondary, indirect role by enabling communication between the parties to payment services. Furthermore, PSPs receive all the income from the use of their services, so transferring the financial liability for fraud from PSPs to operators would be disproportionate.

The fraud problem cannot be solved by passing on liability and has an adverse effect on the cooperation between banks, online platforms and ECSPs that focuses on shared responsibility.

Combating fraud benefits from voluntary cooperation between banks, online platforms and ECSPs at operational level, where relevant (personal) data can be exchanged. The ECSPs argue for an expansion of the legal means to do this better. Such a collaboration between the bank sector and ECSPs is for instance already in place in Belgium under the lead of the Belgian national electronic communications regulator and should be continued to counter the evolution in the fraud scenarios.

In addition, the Belgian telecom law imposes ECSPs to take the relevant, proportionate, preventive, and curative measures considering the most recent technical possibilities. These measures have shown to be efficient and sufficient as incentive for ECSPs to take their responsibility in combating fraud. Such horizontal measure is relevant for all sectors, including the bank sector.

By implementing measures to prevent fraud on the ECSPs' own network, the banking sector will indirectly benefit as their customers will be less likely to be targeted by fraudulent calls/messages impersonating their banks. However, such obligation should not be interpreted as already creating a liability towards the banking sector or any other sector.

Based on this legal framework, additional legal requirements were defined to avoid CLI spoofing in Belgium for international calls to Belgium with Belgian numbers for implementation by end of 2024. In this way the impersonation fraud will be mitigated as far as technically possible.

For these reasons, ISPA believes the proposal should consider the points in this letter so that the common goal of reducing fraud victims can be reached.