

A cross-sectoral approach to fraud prevention: PSR policy recommendations

November | 2024

EXECUTIVE SUMMARY

Tackling the growing trend of payment fraud is critical to protecting consumers and ensuring continued confidence in the payments system. This is especially important as the financial services sector becomes more digital, and the types and methods of fraud become more complex and sophisticated. It is therefore important that policymakers look to take a “whole of sector” approach to the prevention of fraud, considering the majority of new payment fraud originates online. And while the draft Payment Services Regulation (PSR) attempts to address these challenges through better information sharing and cross-sectoral collaboration, automatic refunds could have the opposite effect on consumer behavior and fraud attempts. To resolve this dilemma, we believe that policymakers should look at further ways to boost fraud prevention, while strengthening the protections around automatic refunds to avoid risks of moral hazard. Specifically, we would recommend the following adjustments to the initial proposal:

- Include a requirement on all electronic communication providers to verify with national competent authorities (NCAs) that ads promoting financial services companies or products are authorized.
- Require telecom operators to prevent scam text messages or calls by implementing advanced security technologies and protocols, similar to certain Member State requirements.
- Ensure that the definition of authorisation leads to legal certainty, irrevocability, and predictability for payment transactions.
- Examine a shared liability regime based on levy contributions from electronic communication providers

Introduction

To further harmonise the payment services landscape within the EU, the European Commission (EC) has proposed turning many elements of the Payment Services Directive (PSD) into a Regulation. This is a very positive development which seeks to reduce fragmentation and build on the strong foundations already laid out in the Directive. Alongside this, a key part of proposal aims to address the growing rate of payment fraud, through a number of targeted measures. Recognizing that fraud is not solely an issue for the financial sector, the draft proposal puts forward a number of policy measures to tackle this. The two main measures (which we support) relate to the sharing of fraud information within the financial services sector and the requirement on electronic communication providers to

“cooperate closely” with payment service providers in the fight against fraud. At the same time, the proposal also introduces a new requirement for payment service providers to refund customers for impersonation fraud so long as gross negligence has not been identified and where the victim has informed police authorities.

Since the proposal was published, discussions within the European Parliament (EP) and EU Council have also resulted in new issues and proposals being put forward for consideration. In the main, these have looked at potentially (1) extending the liability provisions beyond purely impersonation fraud (2) developing a shared liability regime by including electronic communication providers within the scope of the Regulation and (3) examining whether a “subjective” reading of authorized transactions should be considered in the context of refunds – potentially broadening the scope of what transactions payment service providers would be liable to reimburse.

The intention of this paper is to provide some perspectives on the PSR as the discussions have evolved, with a view to providing recommendations that can help overcome some of the challenges identified. We of course endorse the wider industry position by the European Banking Federation (EBF) and the European Credit Sector Associations (ECSAs), which cover many of the issues laid down in this paper, although our solutions may differ somewhat.

What are the challenges with the proposals?

Given the impact fraud can have on consumers it is understandable that policymakers have sought to address gaps through legislative action. And while progress has been made during the discussions, we believe greater attention needs to be placed on fraud prevention more broadly. As things stand, the current proposals will not address the underlying drivers of fraud if the focus remains largely on bank reimbursement. In our view, the main challenges with the current proposals can be summarized as follows:

- **Liability of impersonation fraud:** By incorporating near automatic liability requirements into the Regulation, this has the potential of reducing customers awareness of fraud attempts, while introducing significant moral hazard into the financial system – especially if the types of fraud under consideration go beyond bank impersonation. At the same time, it could lead to an increase in “friendly fraud” where the customer claims to be exposed to fraud, but in reality, is in collusion with the fraudster. This can in turn lead to an increased exploitation of young people and other vulnerable customers for the purpose of money laundering. Reduced attention to online risks could also spill over on all types of digital services and make payment service users more vulnerable to cyber risks. Incentives for other stakeholders (telecom and social media / online platforms) to collaborate with banks are also reduced when the full financial burden is carried by banks. Additionally, our members have experienced difficulties with getting advertisements taken down on social media sites when they are not related to their own brand, highlighting the challenges with extending liability requirements beyond bank impersonation.
- **Absence of mandatory requirements on telecommunication & electronic communication providers:** While it is welcome that the draft PSR puts forward the

proposal that other parties within the fraud chain should “cooperate closely” in the prevention of fraud, without specific requirements on these sectors – especially in the absence of liability – it will be challenging to establish a well-functioning cross industry collaborative approach.

- **Establishing a shared liability regime:** The banking sector fully supports proposals that require other sectors – like electronic communication providers – to share liability in respect to payment fraud. With the majority of payment fraud originating online, we believe this makes sense. How such a regime could operate effectively is, however unclear. Often payment fraud is only identified days, weeks or months after it has occurred, with the original fraud advertisement having been removed/altered in the interim. This makes it very difficult for customers to validate the origins of a fraud without evidence of the original scam. The net result is that trying to apportion liability between parties will be very challenging, which is likely to result in payment service providers being required to reimburse customers.
- **Authorization Vs authentication:** The current policy discussion linking authorization with intent – and especially the amendment proposed by the European Parliament – would create legal uncertainty and fragmentation in EU payments regulation, undermining the well-established liability framework between payment service providers and payment service users. Identifying a legally sound definition of authorisation is a complex and delicate task, but it is extremely important to ensure that the definition leads to legal certainty, irrevocability, and predictability for payment transactions, including transactions executed by consumers, SMEs, corporates and governments, while not negatively impacting the payments market and ensuring proper functioning of the payment system. More broadly, we believe such a legal approach would present challenges to Ireland’s common law system where judicial decisions play a key role. Further consideration on this latter point is required, in our view.

Our solutions

Financial institutions have a clear role to play in preventing fraud, a commitment which the industry takes very seriously through a range of measures both at industry level and within each individual institution. However, it is important to note the first sight a financial provider will have of a scam is when a transaction has already taken place. The payment occurs at the end of what can often be a long engagement between the criminal and the victim. Therefore, the banks cannot combat this crime alone. A fraud prevention strategy needs a centrally led ‘whole of system’ response where social media companies, telecoms, financial services, governments, and law enforcement can collaborate to devise appropriate strategies to better share intelligence, implement protections for consumers and develop barriers to criminals.

To effectively combat fraud, it is crucial to address the source and prevent frauds from reaching consumers in the first place. This is why legislation should concentrate on fraud prevention and mitigation. Some of the measures that could help overcome the challenges outlined above include:

- 1. A requirement on all electronic communication providers to verify with national competent authorities (NCAs) that ads promoting financial services companies or products are authorized.** From our members' experience, the vast majority of payment fraud originates through social media platforms. Despite many interactions identifying known fraud, these are very often not acted upon. While we recognize that the new Digital Services Act (DSA) aims to address illegal content, having a clear mandate requiring online platforms to only publish advertising for financial products and services from companies that are regulated by their competent national authority would greatly assist in fraud prevention. In practice, this would mean that before accepting an advertisement for a financial product or service an online platform would be required to check if the company is regulated to provide these services. Recently, Google Ireland has committed to updating its fraud prevention measures, which could serve as a legislative basis for the wider sector. In essence, it will require Financial Services advertisers to complete verification based on their authorisation from appropriate regulators. Advertisers who are required to complete the process and do not, will not be allowed to show financial services ads, including via third parties.
- 2. Require telecom operators to prevent text messages or calls from appearing to originate from a Payment Service Provider (PSP),** blocking deceptive text messages and spoofed numbers, promptly disabling mobile numbers used for fraudulent activities, and monitoring bulk messages with URLs. Exploring a European Registry of SMS sender aliases to combat spoofing is also a potential avenue. We note several examples of national legislation, such as in Finland (where telecom companies report having prevented tens of millions of fraudulent calls), that are going in this direction. Mandating software providers to technically prevent SMS or phone calls displayed with the same alias as a bank from being grouped together in the same thread should also be required.
- 3. Maintain the current definition of authorization as currently in operation.** It is crucially important that the definition leads to legal certainty, irrevocability, and predictability for all payment transactions. Including a refund right for authorised transactions would bring significant uncertainty into the payment system. In our view, the definition should be grounded in an objective legal approach. Any other solution, like the subjective approach being considered, would only result in further fragmentation across the EU through varying legal interpretations when cases arise, while it would make payment transactions very unpredictable. 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.

4. **Establishing a levy to address shared liability:** As outlined above, trying to apportion shared liability in respect to payment fraud could be operationally challenging, despite its good intentions. As an alternative approach, policymakers could explore creating a levy which electronic communication providers would be subject to based on a “polluter pays principle”.

Annex 1 – Proposed drafting to require electronic communication providers to verify financial services advertisements

1. The following definitions are proposed to be inserted in Article 3 of the Draft Regulation:

“advertisement” means ‘advertisement’ as defined in Article 3, point (r), of EU Regulation 2022/2065;

‘dissemination to the public’ means ‘dissemination to the public’ as defined in Article 3, point (k), of EU Regulation 2022/2065;

‘financial service’ means any service of a banking, credit, insurance, personal pension, investment, crypto asset or payment nature;

“inducement” means persuading or inciting or seeking to persuade or incite a person to avail of a service;

“invitation” means any communication that directly or indirectly invites a person to take an action which will result in his availing of a service whether this step is by means of contacting any person or entity or otherwise;

“marketing communication” means any form of representation made by a trader or recipient of a service in connection with a trade, business or profession in order to promote the supply of a service;

‘online platform’ means ‘online platform’ as defined in Article 3, point (i), of EU Regulation 2022/2065;

‘online search engine ’ means ‘online search engine ’ as defined in Article 3, point (j), of EU Regulation 2022/2065;

‘recipient of a service’ means ‘recipient of a service’ as defined in Article 3, point (b), of EU Regulation 2022/2065;

“trader” means ‘trader’ as defined in Article 3, point (f), of EU Regulation 2022/2065.

2. The following underlined wording is proposed to be inserted in Article 107 of the Draft Regulation:

Article 107

More favourable refund rights and Stricter fraud prevention measures

[Insert new paragraph 3]

3. In order to prevent payment fraud, providers of online platforms or of online search engines that have been designated by the Commission in accordance with Article 33 of EU Regulation 2022/2065 as being very large online platforms and very large online search engines shall not engage in the dissemination to the public in the territory of the Union of any item of information or otherwise for or on behalf of any recipient of a service or trader that would lead an average viewer of that information to believe that the information presented or any element of that information is an advertisement, marketing communication, invitation or inducement for any financial service unless that recipient of the service or trader is authorised or licenced to carry on business as a financial service provider by a competent or supervisory authority of a Member State where that competent or supervisory authority has been designated as such by that Member State under any Directive or Regulation of the Union that relates to financial services.



Banking & Payments Federation Ireland,
Floor 3, One Molesworth Street, Dublin 2, D02 RF29, Ireland.

Tel: +353 1 671 53 11 Email: info@bpfi.ie
www.bpfi.ie

Dublin • Brussels • Frankfurt