European Payment Institutions Federation aisbl

EPIF Statement on the Authorization of Payment Transactions under the Payment Services Regulation

European payment service providers (PSPs) are committed to combating payment fraud and enhancing transaction security across Europe. Since the introduction of PSD2, we have seen a significant decrease in unauthorised payment transactions, thanks to the introduction of Strong Customer Authentication (SCA) under PSD2, as well as to PSPs' continuing investments in fraud prevention. This continues to be essential for PSPs, in order to maintain consumer trust in electronic payments.

Current discussions at the Council level focus on the emerging issue of authorised push payment fraud (APP fraud) and its interplay with the current definition of authorised payment transactions under Article 55 of the Payment Services Regulation (PSR). One proposed approach to combating increased social engineering fraud is the introduction of a subjective theory to payment transaction authorisation.

We acknowledge Member States' objective to bolster consumer protection, but we would argue that this approach is not the best path to achieving that goal. The subjective theory presents significant challenges and potential unintended consequences. This approach inadvertently introduces quasi-automatic liability for PSPs, effectively setting a precedent for an insurance-like protection that does not tackle the root causes of social engineering fraud. Such measures could destabilise the payment ecosystem rather than fortify it. Therefore, we urge a reconsideration of this approach in favour of maintaining and enhancing objective criteria, ensuring more direct and effective fraud management and system stability.

Recommendations

In order to maintain a well-functioning European payments ecosystem, we suggest taking the following steps to ensure consumer protection while not inadvertently placing the stability of the payments system at risk:

1. **Maintain Objective Authorisation Criteria:** Continue using clear, objective criteria for transaction authorisation to ensure consistency and reliability in payment processing, while also establishing the criteria to investigate and manage social engineering fraud. In addition to maintaining objective criteria, consumer protection measures should be reinforced, such as consumer education and awareness, industry collaboration and up-flow controls. An objective approach combined with all these measures will be more effective in combating social engineering fraud.
2. **Revert Burden of Proof Post-SCA:** Ensure that the burden of proof reverts to the payer when SCA is correctly implemented, aligning liability between the payment service user and the payment service provider more fairly and encouraging ongoing investment in security technologies.
3. **Standardise Definitions of Gross Negligence:** Establish a unified, objective definition of gross negligence by including a non-exhaustive list of criteria to assess gross negligence. This will help reduce inconsistencies and improve legal clarity across jurisdictions.

Operational Challenges and Impact on Security Protocols

The subjective approach to determining transaction authorisation based on payer intent is fraught with operational challenges. PSPs cannot assess as payment service user's (PSU) state of mind when executing a transaction but can merely look at objective criteria, such as the effective use of SCA to determine the intent of a PSU in making a transaction. Asking PSPs to consider the intent of PSUs therefore seems impossible and could undermine the integrity of SCA by making it less effective in proving transaction legitimacy, thereby diminishing PSPs' incentives to invest in or maintain robust security measures.

Legal Uncertainties and Increased Dispute Risks

Adopting the subjective approach would increase legal and operational uncertainties. Transactions could become reversible based on retrospective claims of non-intent by payers, leading to unpredictability in payment processing and an increase in disputes. This scenario necessitates complex resolution mechanisms and could place an undue operational burden on PSPs. We propose that when SCA is properly implemented, as a minimum, the burden of proof should revert to the payer, allowing the PSPs to assess the mechanism of fraud that happened to the PSU, to confirm if the PSU is entitled to a reimbursement.

Economic Impact and Systemic Concerns

The potential for increased operational and legal risks under the subjective approach would likely lead to higher costs for providing payment services, costs which will ultimately be passed on to all users. This approach is also unlikely to lead PSPs to enhance their fraud detection mechanisms since it is virtually impossible for them to assess customer intent in the case of social engineering, where the customer believes they are making a justified transaction in the moment of payment. Clear, objective criteria for transaction authorisation would, therefore, streamline judicial decisions, reduce administrative complexities, and support more consistent and equitable outcomes across Member States.

Additionally, rather than improving the confidence in the payment system, the subjective theory could jeopardise societal awareness against this type of fraud. The automatic liability of PSPs could lower the level of due diligence users exhibit, as they would not face economic consequences in relation to a fraud they suffered. On the contrary, the objective theory would provide more legal certainty while providing users with a way to compensate financial losses they suffer due to social engineering fraud.

Lack of Continuity with the PSD2

Since the introduction of SCA has greatly reduced fraud, the PSR should build on this progress to address gaps, such as those created by social engineering fraud. The objective approach would allow for the reimbursement of payments made due to social engineering scams, if the payer can prove their case and that they have not acted fraudulently or with gross negligence.

The subjective approach offers no advantages over the objective approach in this respect, given that the jurisprudence in several Member States already allows for reimbursement even when the

transaction is authenticated, if it involves social engineering fraud. Moreover, enhancing fraud prevention measures is not necessarily linked to adopting a subjective approach. PSPs naturally strive to reduce fraud and losses, and implementing the objective theory aligns perfectly with these goals, proving to be a solution that avoids unintended consequences while providing consumer protection.