EPIF Position on TSPs: Roles and Responsibilities

Purpose of this Document

This document lays out the EPIF recommendation on TSPs and SCA and it provides a detailed breakdown of the different types of TSP models used in SCA implementations. It aims to clarify the roles and responsibilities of each model. Given the rapidly evolving payments landscape, it is critical for upcoming regulations, primarily PSD3/PSR, to acknowledge and embrace this diversity and adopt an inclusive approach that fosters safe and secure innovation while ensuring safety, security and compliance in payment authentication. We note that this document represents EPIF views based on our own review and assessment of the operating models of TSP services as available through publicly available sources and further based on our own categorisation of involvement levels in the SCA process. We do not intend to advocate for any particular level of supervision of services mentioned in this document but aim to illustrate different operating models that exist for TSPs contributing to the payment landscape.

EPIF Recommendation

EPIF supports the proposed deletion of Article 87 of the PSR. We agree that Article 58 addresses issues related to liability for technical service providers and payment scheme operators regarding strong customer authentication (SCA), rendering Article 87 redundant. We also note that the outsourcing and audit aspects of Article 87 are duplicative of DORA and the EBA guidelines on outsourcing. Furthermore, given the proposed deletion of Article 87, **we believe Recital 119 should also be removed to maintain consistency and avoid potential confusion**. We believe this approach simplifies the regulation and provides greater clarity for all stakeholders.

We kindly recommend the following draft for A58: "*Technical service providers and operators of payment schemes that either provide services to the payee, or to the payment service provider of the payee or of the payer, shall be liable for direct financial damage caused to the payee, to the payment service provider of the payee or of the payer for, and proportionate to, their failure, within the remit of their contractual relationship, and not exceeding the amount of the transaction in question to provide and verify the elements of strong customer authentication."*

Moreover, we call for the **deletion of the Article 89.1 (d)** that mandates the EBA to develop Regulatory Technical standards (RTS) for outsourcing agreements between TSPs and PSPs, limiting the negotiating flexibility of such arrangements. As noted above, these agreements already must follow the EBA guidelines on outsourcing and TSPs already fall (either directly or indirectly) under the supervision of DORA and the ECB's PISA framework. Further barriers would significantly impact the provision of technology services in the payments sector.

Involvement and Commercial Models: From Free Services to Liability-Driven Costs

As you'll be able to read more about below, the TSP ecosystem is extremely diverse. There are TSPs with very limited involvement in the SCA process, such as those providing off the shelf technology and enabling access to third-party methods. In other cases, the TSP actually carries out the SCA on behalf of the PSP and **verifies the SCA.** This should be understood as a stand-alone commercial service. Different TSP models vary in their level of involvement and the scope of services they offer in supporting compliance with SCA requirements. This broad ecosystem is important to allow PSPs to choose the model that works best for their unique operating model. **Any requirements in the PSR should also take into account existing contractual arrangements between PSPs and TSPs.**

It is also important to understand that TSPs typically do not have contractual relationships with the end-users but instead enter into agreements with PSPs, and within their contractual relationship, they provide a technical service to

those PSPs that account for the relevant risks through their overall commercial model (e.g. via their pricing structure and insurance products). The liability provision set out in the Commission draft proposal raises a number of concerns (e.g. by exposing TSPs to any indirect and consequential damages, thereby introducing unprecedented and unlimited liability for all entities involved in the operational implementation of strong customer authentication.

TSP Models Spectrum - Role in the SCA

Access to technology
Low involvement

Full SCA verification / execution
High involvement

Limited Enabler	Multi-Method Integrator	Routing Gateway	SCA as a Service Platform	Risk-Based Orchestrator	Full-Service Handler	All-In-One Authentication Provider

TSP Models for SCA Enablement: Roles

TSP Model	Differentiations in SCA Role
Limited Enabler: Provides access to off the shelf technology (e.g., biometrics) for issuers / PSPs to use in authentication but does not handle verification or processing. ***Level of involvement: Low***	- Typically no involvement in flow of funds or settlement - Issuers or PSPs perform and verify SCA.
Multi-Method Integrator: Aggregates multiple authentication services but leaves the final SCA decision to the issuer or PSP. ***Level of involvement: Low***	- Combines multiple authentication methods into one interface. - Issuers or PSPs perform and verify SCA.
Routing Gateway: Routes SCA requests to relevant services based on compliance requirements, without executing SCA. ***Level of involvement: Medium***	- Ensures requests are sent to appropriate services. - Focuses on compliance across regions.
SCA-as-a-Service Platform: Provides a fully managed, subscription-based service for SCA compliance and authentication. ***Level of involvement: Medium***	- Handles all aspects of SCA compliance. - Provides ongoing updates to meet regulatory changes.

Risk-Based Orchestrator: Coordinates identity verification and SCA decisions based on risk assessments and multiple identity inputs. ***Level of involvement: Medium***	- Manages identity and risk signals to trigger SCA dynamically. - Ensures minimal user friction by adapting to risk levels.
Full-Service Handler: Manages the entire SCA process, from transaction initiation to final authentication, on behalf of the issuer or PSP. ***Level of involvement: High***	- Takes over the entire SCA process, including handling exceptions. - Provides the SCA result to the issuer or PSP.
All-In-One Authentication Provider: Delivers both identity verification and SCA, providing a comprehensive solution for authentication and fraud prevention. ***Level of involvement: High***	- Manages identity verification and SCA end-to-end. - Integrates advanced fraud detection techniques.