FS Consulting Blog

By PwC Deutschland | 30. Juni 2023

A First Look at Implications of PSD3, PSR, and FIDA for Open Banking & Finance in the European Union

The years since the introduction of the second Payment Services Directive (PSD2) have seen steady change in the European retail payment services market.

Backdrop for the Proposals

The years since the introduction of the second Payment Services Directive (PSD2) have seen steady change in the European retail payment services market. Long-term trends, such as the increased adoption of digital payment methods, entrance of new market actors and proliferation of service offerings, have continually tested the bounds and exposed the deficiencies of the current regulatory framework.

A thorough review of the impacts of PSD2 and the second Electronic Money Directive (EMD2) has resulted in the newly minted third Payment Service Directive (PSD3) and and the associated Payment Service Regulation (PSR). These proposals, which both incorporate some aspects of and supersede the prior legislation, attempt to acknowledge this new market landscape, address identified shortcomings of their predecessors, and further strengthen current regulatory mechanisms.

The Financial Data Access (FIDA) Regulation was also published to begin the construction of a comprehensive framework for financial data access that encompasses a broader array of financial services beyond what is handled in PSD3 and PSR. FIDA is applicable to various entities, including credit institutions, payment institutions, investment firms, and insurance undertakings. It also covers an extensive scope of customer data related to a variety of financial products. FIDA obliges market participants to both equip customers with dashboards for financial data access permissions and devise common scheme standards for customer data access and exchange. It also introduces a compensation approach for data holders for their upkeep of infrastructure.

Overview of Major Changes in the PSD3 and PSR Proposals

Four goals are explicitly listed in the proposals: to strengthen user protection and confidence in payments, to improve the competitiveness of open banking, to harmonize enforcement and implementation across EU Member States, and to improve access to payment systems and bank accounts for non-bank payment service providers (PSPs).

A wide-ranging “package of preferred options” is laid down to achieve these goals, the rough contours of which can be sketched as follows: improving the application of Strong Customer Authentication (SCA), shifting of liability to PSPs commensurate with their increased role and competencies and requiring the creation of both dedicated data access interfaces and “permissions dashboards” for payment service users (PSUs).

(1) SCA Requirements

In the interest of the open banking (OB) ecosystem, electronic payment security is of critical importance, and several measures are taken to address current regulatory shortcomings.

Language surrounding SCA requirements for Merchant Initiated Transactions (MITs) and Mail Orders or Telephone Orders (MOTOs) has been clarified. In the case of MITs, SCA is required during the initial setup of a payment mandate, but not during any subsequent payments. For MOTOs, only non-digital payment

initiations (e.g., paper-based payment orders, mail orders, or telephone orders) are exempted from SCA requirements.

For direct debits, an SCA requirement has been introduced for cases in which a payment mandate is placed through a remote channel (i.e., over the internet) with the direct involvement of a PSP. This narrowing of SCA exemptions helps homogenize regulations of MITs and direct debits with an eye towards strengthened PSU protection during payee-initiated transactions.

An additional point of interest within discussions on SCA are proposed accessibility requirements for persons with disabilities or with low digital skills. The proposals mandate that the performance of no SCA process be solely dependent upon a single authentication method or technology, although it is unclear how these measures are to be best translated into practice.

In acknowledgement of their increasing necessity in carrying out payment services, technical service providers (TSPs) are also addressed. Although generally excluded from SCA requirements, when operating in conjunction with PSPs, TSPs should become liable for any failure to support SCA. Additionally, TSPs should be required to enter into formal outsourcing agreements with PSPs should they provide or verify SCA services to them.

(2) Shifting Liabilities in the Interest of User Confidence

Another recurring theme in the proposals is the notion of using PSP liability—especially in the event of error or fraud—as a mechanism for increasing both security and user confidence.

To help prevent errors during the input of user data during the transfer of funds, PSPs should implement systems capable of identifying potential discrepancies and notifying users of potential consequences thereof. Should these verification services malfunction or otherwise fail to notify the PSU of potential discrepancies in entered payment information, the payment service provider is liable.

In the case of fraudulent transactions, PSUs are entitled to immediate refund from their PSP, excepting cases of fraudulent action on the part of the PSU. As such, existing mechanisms for identifying unauthorized transactions and processing refunds must be strengthened.

The increasingly common instances of social engineering or “spoofing” are also addressed. Given the imbalance of resources and influence between PSPs and their users, the onus of protecting against such cases—and thus liability for such events—is clearly placed on PSPs, and systems should thus be developed to effectively monitor, combat, and process such claims.

(3) APIs and Dashboards

In the interest of data security, open banking services providers should be allowed access to payment accounts and their associated data via dedicated interfaces provided by account servicing payment service providers (ASPSP). These dedicated interfaces should generally be the sole point of contact for open banking services providers.

As the keystone in the proposed OB framework, these interfaces should conform to stringent technical, performance, and functionality requirements. Critically, interfaces should also generally handle requests in an origin-agnostic manner and thus preclude the possibility of discrimination against open banking services providers.

To increase consumer trust in OB, PSUs should also remain in control and easily retain an overview of their data, specifically, any access permissions granted to open banking services providers. To this end, ASPSP can offer PSUs specially designed dashboards. These dashboards should provide users the ability to withdraw and re-establish previously granted permissions. It is also required for both open banking services providers and ASPSPs to inform one another of any newly granted or withdrawn permissions, which should be then reflected on the dashboard.

Impact and Growth Potential

These sweeping changes introduced by PSD3 and PSR will no doubt cause the need for changes in the OB ecosystem.

The challenges posed by the above-discussed changes can be directly addressed by the introduction of new technical mechanisms and the refinement of existing systems. Specifically tailored APIs and dedicated dashboards, which must largely be designed and built from scratch, are the elements of these proposals that will pose some of the greatest challenges for PSPs.

These proposals have thoroughly assessed the current needs, trends, and deficiencies of the payments landscape. The OB market has significant room for further expansion, including new business models; investments into compliance will further boost user confidence and market innovation. Traditional banks and open banking services providers should quickly and proactively define their stances relative to these proposals so that they are optimally positioned in this rapidly developing ecosystem.

The proposals can be found online here:

PSD3: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0366

PSR: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0367

FIDA: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0360

Get ongoing updates on the topic via regulatory horizon scanning in our research application, PwC Plus. Read more about the opportunities and offerings here.

To further PwC Blogs

Schlagwörter

Compliance, Digitalisierung, Fonds, Framework, Retail Banking, Zahlungsdienste / Payment Services, Zahlungsverkehr, financial liabilities

Kontakt

Maximilian Harmsen

München

maximilian.harmsen@pwc.com