The evolution of Open Finance in the EU: legislation inches forward, fraud comes into focus, and payments continue to be at the center

May 22, 2024

1. INTRODUCTION

The digital transformation of financial services in the European Union **(EU)** is progressing rapidly, driven by changing consumer expectations, technological advancements, and regulatory initiatives.

Recent developments in the European Parliament bring the transition from open banking to open finance into sharp relief, including important boundary issues. The outcome of some of the key negotiating points, including around proposed new measures to mitigate fraud, may ultimately affect the roll-out of open finance globally due to what is oft referred to as the "Brussels effect".

The IIF has long advocated for a transition from open banking to not just open finance, but to open data, to ensure the free flow of data in both directions (both in and out of the financial industry) to best serve the consumer if such policies are deemed favorable by policymakers and legislators. We are cognizant of the costs to financial institutions of both implementation and the need to ensure a level playing field while supporting competitive markets.[1] For this reason, we have advocated for reciprocity of access between the financial sector and other sectors, including the technology sector, that hold information that may be valuable for more accurate credit scoring and improved tailoring of financial services to consumer needs.[2]

2. BACKGROUND

In June 2023 the European Commission released its financial data access and payments package against the backdrop of rapid increases in electronic payments, more complex payments ecosystems, and more sophisticated forms of fraud. The package comprises proposals for a revised Payment Services Directive **(PSD3)**, a new Payment Services Regulation **(PSR)**, and a proposed Financial Data Access Regulation **(FIDA)**. It is being considered by the European Parliament and Council at present.

The current Payment Services Directive or PSD2, which the PSD3 and PSR will replace, embodies the EU's open banking initiative and is narrowly focused on the sharing of payments information. The FIDA is intended to establish clear rights and obligations to manage customer data sharing in the financial sector beyond payment accounts and is expected by policymakers to lead to more innovative financial products and services for users and to stimulate competition in the financial sector.

Other payments initiatives in the EU include the Instant Payments Regulation, which recently entered into force on April 8, 2024. We covered the IPR in a member-only Briefing Note, where we noted the timetable. Payment service providers (**PSPs**) will have 9 months from the date of entry into force (so, by January 8, 2025) to be ready to receive instant credit transfers in euro and 18 months (so, by October 8, 2025) to be ready to send them.

3. PSD3/PSR DEVELOPMENTS

3.1 The European Parliament Votes

On April 23, 2024, the European Parliament took a significant step forward in shaping the future of open finance in the EU by **adopting its positions on PSD3 and PSR**. The Parliament voted overwhelmingly in favor of a first reading of both texts,

[1] For example, see IIF – Deloitte (2023), The ecosystem imperative - Moving from Open Banking to Open Data (iif.com)
[2] For example, see IIF (2018), Reciprocity in Customer Data Sharing Frameworks (iif.com)

with PSD3 receiving 484 votes for, 8 against, and 118 abstentions, and PSR garnering 511 votes for, 22 against, and 75 abstentions.

Some of the most important changes the Parliament voted to introduce (mainly to the PSR) include:

- Enhanced consumer protection through fraud prevention, liability clarification, accessibility requirements, and mandatory participation in alternative dispute resolution **(ADR)**.
- Promotion of competition and innovation by enabling new payment services, applying risk-based strong customer authentication (**SCA**), and ensuring interoperability.
- Increased transparency and user control via clear fee information, data sharing opt-out, and consistent permissioning dashboards across both PSR and FIDA.
- Improved fraud data sharing and unique identifier verification through a dedicated EBA IT platform.
- Clarification of the regulation's scope, including interactions with electronic money tokens and specific issues like location-based discrimination and direct debit refunds.

The Parliament's changes are heavily focused on fraud prevention and detection (see **box**). This is an issue that has been rising on political agendas globally, and about which the IIF recently made a submission in response to a formal consultation of the Basel Committee on Banking Supervision. The IIF continues to convene forums that will allow members to discuss this issue in depth.

The Parliament's proposed amendments concerning fraud

- Protect users against social engineering fraud where fraudsters manipulate them into initiating payments or sharing credentials.
- Clarify conditions for authorized vs unauthorized transactions, as new 'spoofing' fraud blurs the lines.
- Payment providers should combat 'spoofing' fraud through prevention and technical safeguards, working with telecom providers who may be jointly liable.
- Online platforms contributing to fraud should be liable if they are informed but fail to remove fraudulent content.
- The EBA should create an IT platform for payment providers to exchange fraud data.
- Payment providers should block suspected fraudulent orders or recover funds based on strong evidence or police reports.
- Telecom providers should educate customers on identifying and reporting online scams.
- Fraud statistics should include reimbursed transactions and reasons for reimbursement refusals.
- Member States should invest in payment fraud education.

Overall, many of the changes proposed by the Parliament, which later need to be considered in trilogue discussions with the Council and the European Commission, appear to be positive, particularly the notion that telecom providers and social media platforms should share responsibility for losses.

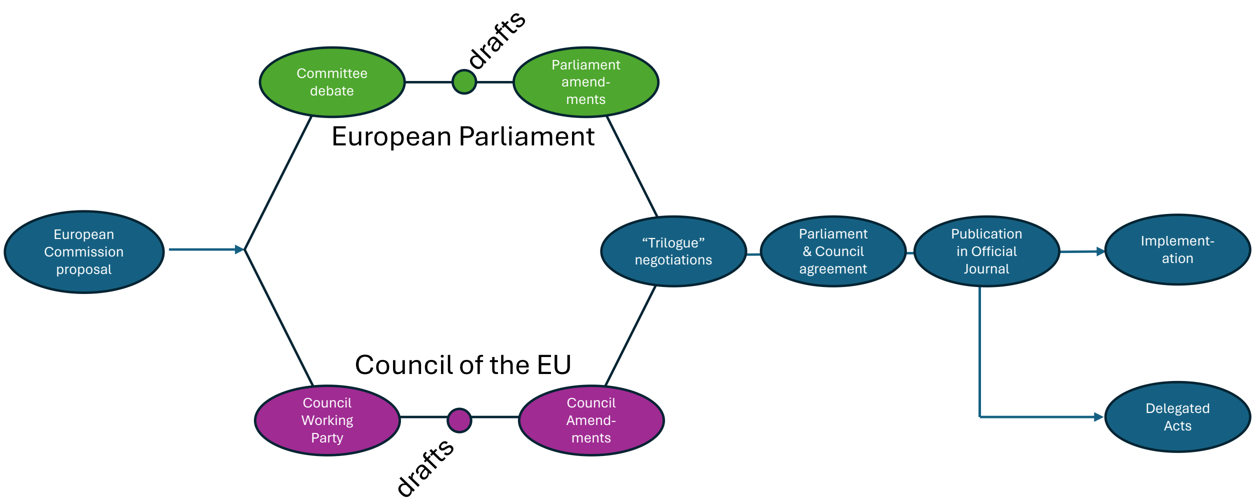
However, moves to extend the category of unauthorized payments to any transaction where the payment service user does not authenticate a given transaction "freely and with full knowledge of all relevant facts" may be concerning.[3] This would appear to make transactions that have been fraudulently procured but have been authorized by the customer, count as unauthorized for liability purposes. As stated in the IIF's February 16, 2024 submission to the Basel Committee on Banking Supervision, moves

[3] Proposed Article 3(34a).

to allocate liability to financial institutions away from customers for authorized payments fraud will reduce client incentives to take appropriate care, and will encourage first-person fraud. Separately, it may also be problematic that in Article 88 PSR, the obligation to provide non-smartphone based SCA solutions is not limited to vulnerable customers who do not have access to app-based solutions.

The next steps in the legislative process (see also **graph**) will be taken up by the new Parliament following the European elections in June 2024. Finalized versions of PSD3 and PSR had been expected by late 2024, with potential implementation around 2026, but these timelines may be subject to change.

Graph: EU Legislative Process



Source: Adapted from European Free Trade Association, Shaping EU Policies (efta.int)

3.2 The European Banking Authority weighs in

On April 29, 2024, only a few days after the European Parliament's vote, the European Banking Authority published a wide-ranging opinion on fraud in payments, setting out some provocative findings, and making a series of specific suggestions for further amendments to the PSD3/PSR texts.

The EBA's key findings include:

- SCA as required under PSD2 has been successful in mitigating fraud overall, with low fraud rates for credit transfers (0.0008% of value) and direct debits (0.0020%) in 2022. However, fraud levels are higher for some specific payment types, geographies and circumstances;[4]
- new complex fraud types have emerged, including manipulation of the payer/authorized push payment fraud, mixed social engineering and technical scams, and compromise of the enrolment process for second SCA factors;

[4] For example, instant payments have ~10x higher fraud rates than traditional credit transfers; merchant-initiated transactions (13.1% of remote card payments) and mail order/telephone order transactions had fraud rates over 0.1%; and cross-border transaction fraud rates are ~9x higher than domestic for both cards and credit transfers.

- liability for fraud losses varies significantly between payment instruments, with 79% borne by payment service users for credit transfers.

The EBA went on to recommend a number of changes to the PSD3/PSR text, while also noting the Parliament's amendments:

- clarify that the two SCA factors must be from different categories;
- require PSPs to allow users to set transaction limits;
- mandate transaction monitoring (**TM**) be performed pre-execution for instant payments; apply TM to all electronic channels; require payee PSP screening; require data sharing between PSPs to enhance TM;
- strengthen device enrolment process security;
- require PSPs to have a fraud risk management framework including risk assessments, monitoring, and updating of security measures;
- clarify liability rules - SCA alone should not prove authorization; consider transactions unauthorized if user unaware of IBAN/name mismatch; define gross negligence;
- increase supervision of PSP fraud management practices; and
- consider an EU-wide platform for secure sharing of fraud data between PSPs.

Of these measures, the most impactful for financial institutions could be the proposal to significantly change the proposal in Article 83 PSR for an EBA-operated data sharing platform to one that is operated by PSPs themselves:

> *The EBA advises the EU co-legislators and the EU Commission to consider further strengthening Art. 83 of the PSR proposal with a requirement to have a single EU-wide platform, **to be maintained and run by PSPs**, for the sharing of fraud data amongst PSPs, in order to fully capture the benefits of the measure. (Emphasis added.)*

While a so-called "consortium approach" to fraud data sharing can maximize the power of machine learning models, such an approach raises important questions about the potential costs, which are so far not estimated.

4. FIDA DEVELOPMENTS

Alongside PSD3 and PSR, the proposed FIDA framework is set to play a crucial role in the EU's journey from open banking to open finance. FIDA aims to give financial customers control over their data, allowing third parties to access a wide range of financial information beyond just payment accounts. This includes data on mortgages, loans, savings, investments, insurance, pensions, and creditworthiness assessments.

Key points of negotiation around FIDA include:

- Scope and types of data covered: Stakeholders are seeking clarification on the specific types of data included within each broad category, as well as the distinction between data provided by customers and data generated through customer interactions.
- Compensation, liability, and security considerations: The framework must address issues related to fair compensation for data holders, allocation of liability, and ensuring the security of shared data.
- Interplay with other regulations: FIDA's interaction with other key regulations, such as the General Data Protection Regulation **(GDPR)** and the EU Data Act, needs to be clearly defined to ensure a coherent and harmonized approach to data sharing.

FIDA was recently voted on at the European Parliament's Economic and Monetary Affairs Committee **(ECON)** on 18 April 2024. Controversially, ECON voted to exclude gatekeepers designated under the Digital Markets Act (**DMA**) from accessing the financial information of consumers. The list of gatekeepers includes most of the global digital giants such as Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft. According to the Parliament's press release, "their exclusion aims to ensure that they could not circumvent the rules in case they owned or control data users."

The next steps will be taken by the new Parliament following the June 2024 elections.

5. IMPACT ON FINANCIAL INSTITUTIONS

While many aspects of the data access and payments package will likely be positive for customer experiences and also for jurisdictions in which explicit competition mandates exist, the implementation of this complex and fast-changing legislation will present several challenges for financial institutions.

> *Most concerningly, the possibility of radical changes to the liability model for authorized push payment (**APP**) fraud should not be ruled out. While the EBA's proposals in this regard would appear more palatable than the Parliament's, the EBA has on the other hand proposed a new, potentially costly data sharing platform to be operated by PSPs, without any cost estimate.*

Meeting the real-time data sharing requirements under FIDA may prove technically challenging and costly for data holders. The industry will need clarification on the interplay between FIDA, PSD3, GDPR, and other relevant regulations to ensure compliance and avoid conflicts.

Establishing fair compensation and liability models will be crucial to incentivize participation in an open data ecosystem. In the limited context of just open finance at this time, the short implementation timelines proposed for these initiatives may pose readiness challenges for industry participants.

However, the industry can leverage existing open banking standards, APIs, and lessons learned to facilitate the transition to the new regulatory environment. The European Commission's report on the application and impact of PSD2 highlighted that while the directive laid the foundations for open banking and open finance in the EU, many of the expected benefits have not yet been fully realized due to issues related to data access, sharing, consent, and API standardization.[5] The report also noted that the majority of banks and banking associations consulted suggested that the costs of PSD2 largely outweighed the benefits to them.[6] As such, continued industry engagement will be essential to influence the development of technical standards and ensure a more balanced and effective implementation of PSD3, PSR, and FIDA.

6. CONCLUSION

The recent European Parliament votes on PSD3 and PSR, along with the ongoing development of FIDA, reflect a significant evolution of the EU's open finance framework. These initiatives aim to increase innovation, enhance competition, and strengthen consumer protection in the financial services sector. However, the requirements introduced by these regulations may prove complex and costly for the industry to implement.

As the legislative process moves forward, continued industry engagement will be crucial to influence the finalization of the regulatory texts and the subsequent development of technical standards. By actively participating in this process, financial institutions can help shape a more balanced and effective open finance ecosystem that benefits all stakeholders.

Despite the challenges posed by PSD3, PSR, and FIDA, these initiatives may also present opportunities for the financial services industry. Pending a further shift towards open data, not just open finance, financial institutions can collaborate with new players in the ecosystem to develop innovative, value-added products and services and improve customer experiences.

---

[5] At p. 153
[6] At p. 155

