The world is how we shape it

sopra steria

OPEN FINANCE IN EUROPE:

one year on, where do we really stand?

Adoption, use cases, and regulatory progress

Authors

Mung Ki WOO

Chief Operating Officer,
Financial Services Sopra Steria
mung-ki.woo2@soprasteria.com

Marine LECOMTE

Head of Offers & Innovations,
Financial Services Sopra Steria
marine.lecomte@soprasteria.com

Introduction

Open Banking: From promise to reality

In 2018, the promise of Open Banking in Europe rested on a hypothesis: once PSD2 came into force, it would trigger rapid adoption and a wave of innovation across the ecosystem around data sharing and payment initiation. Today, the picture appears more nuanced. Open Banking is progressing, yes. Tangible use cases are emerging, yes. But the potential remains largely under-exploited in many countries, and Europe is still fragmented between highly advanced ecosystems and others that are still in an experimental phase or held back by technical hurdles, trust issues, or regulatory interpretation.

The years ahead could, however, profoundly transform the banking landscape. The imminent arrival of new regulatory obligations (PSR and PSD3) on the PSD2 scope (payment accounts) will reshape the European market by harmonising requirements around transparency, security standards, and the mechanism for permission management.

FIDA will further disrupt the banking ecosystem by extending the principle of Open Banking, which already allows third-party providers (TPPs), with the customer's consent, to access payment account data to offer account information services or payment initiation to all financial products, thereby expanding the possibilities for innovation.

A year ago, we analysed these three forthcoming texts to shed fresh light on their impacts and on the different scenarios (notably around FIDA schemes) for banks. Indeed, for financial institutions, the question is no longer merely compliance: it is about anticipating developments, accelerating their transformation, and clarifying the position they intend to occupy within the ecosystem, particularly in relation to fintechs already present in the market.

In this new edition of the white paper on Open Finance, we enrich and update our 2024 analysis around three main parts:

- **A market view,** following studies conducted with aggregators and market analyses: where Open Banking adoption in Europe really stands, for which use cases, and what obstacles persist;
- **An update on the upcoming regulatory impacts (PSD3, and above all PSR)** on the scope of payment accounts, notably in light of a new version of the regulation published in June 2025 by the Council of the EU, with a focus on the Permission Dashboard;
- **A projection into the future with the latest news on FIDA,** after a tumultuous year that almost led to its cancellation, and a look ahead to the transition to Open Finance

Part 1

State of play of Open Banking in Europe: between acceleration and under-adoption

1.1 Real adoption: progress, but uneven

The available data show that Open Banking is gaining traction, but in a very heterogeneous way depending on the territories. In mature markets such as the United Kingdom, growth is steady and sustained, and Open Banking now reaches 20% adoption by end customers and small businesses, with 31M Open Banking payments generated in March 2025[1] (OBL Impact Report).

Overall, a study conducted by the University of Cambridge highlighted adoption that remains fragmented by country, due to Open Banking rollouts often marked by disparities in API technical quality, cultural differences around data sharing, and varying levels of consumer[2] trust. A finding that Sopra Steria was able to confirm thanks to a study conducted in France and Italy, respectively with the aggregators Powens and Fabrick.

1- https://www.openbanking.org.uk/insights/obl-impact-report-7-open-banking-delivers-real-world-impact-as-adoption-accelerates-year-on-year/
2- https://www.jbs.cam.ac.uk/wp-content/uploads/2024/11/2024-ccaf-the-global-state-of-open-banking-and-open-finance.pdf

1.2 Two contrasting models: France vs Italy

As a reminder, Open Banking services consist of:

AIS

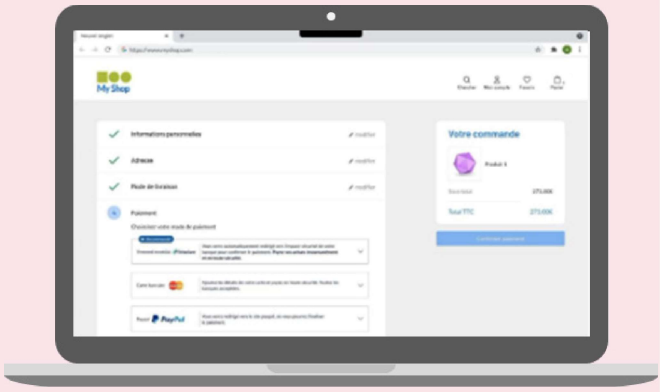
(Account Information Service)

This service allows, with the user's explicit consent, access to information relating to their payment accounts (balance, transaction history, descriptions, etc.) held with one or more banks. The objective is to offer the user a unified and consolidated view of their finances via tools or services enabling account aggregation, budget management, simplified accounting, etc.

PIS

(Payment Initiation Service)

This service allows a third-party provider to initiate a bank transfer from the user's account, always with their explicit authorization, without going through their bank's usual interface. It is particularly useful for offering direct payments using the bank transfer as a payment rail alternative to card schemes, thereby enabling fast, low-cost payments, notably in e-commerce or automated billing services.



France

The French ecosystem has seen the emergence of visible use cases, mainly around the **Account Information Service (AIS).** Adoption is estimated at around 10% on average (according to figures from Powens). The dominant uses revolve around the following services:

Automated loyalty and cashback (e.g. Joko, Paylead), offering frictionless journeys for personalized rewards;

Wealth management and savings with aggregators like Finary or financial assistants such as Bitstack, enabling a consolidated view and support for decision-making;

Connected accounting on the business accounts side (Pennylane, Agicap, Libeo), which leverages the reconciliation of banking data to simplify companies' financial workflows.

Furthermore, an analysis of the **FinTech 100 2025** ranking, produced by Truffle Capital, France Innovation, BPCE and Sopra Steria, reveals that more than 40% of fintechs participating in this ranking now use Open Banking APIs, whether to improve their services or as the core of their value proposition. By comparison, they were only 20% in 2022, which shows a clear increase in adoption within the French ecosystem.

Conversely, **payment initiation services (PIS) remain relatively modest.** Persistent technical obstacles, most notably a lack of standardization and less-than-optimal API reliability, translate into high failure rates: a 2024 Frame study reports up to 44% failure on certain user journeys, undermining trust among partners and end users. However, major use cases are beginning to emerge around PIS, notably the DGFIP, which intends to use it to enable individuals to pay their local liabilities (school canteen, nursery, parking, waste tax, etc.). The market is vast, with more than **72,000** public entities concerned, i.e., around **26 million** transactions annually. For the French government, it is also an opportunity to offer a sovereign alternative.

Italy

In Italy, adoption initially followed a different path compared to France: while AIS drove early Open Banking uptake, as in most markets, it remained heavily B2B-oriented, largely used by SMBs through ERP and accounting systems. Since 2022, however, PIS has taken over as the main growth engine, supported by players such as Fabrick, whose year-on-year transaction growth has been remarkable: **+303.2%** between 2022 and 2023, then **+49.6%** between 2023 and 2024, corresponding to a 2022–2024 CAGR of around **160%**. Moreover, although the overall value of PIS (also called Pay by Bank) transactions continues to rise sharply, **growing from €465 million in S1 2022 to around €1.3 billion in S1 2024**, the **number of transactions has slightly declined** over the same period (from **636k in S2 2022 to 598k in S1 2024**).

Users are initiating fewer but larger payments, suggesting a shift from early micro-tests to more deliberate, high-value use cases, particularly in professional or trust-based contexts. The steady rise in average transaction value supports this trend and indicates that new PIS usage patterns are now taking shape in the Italian market.

1.3 The causes of European fragmentation

In both cases, there is growing dynamism in the use of open banking. However, differences in usage should be noted, and the gap between these two countries highlights several factors driving heterogeneity in Europe:

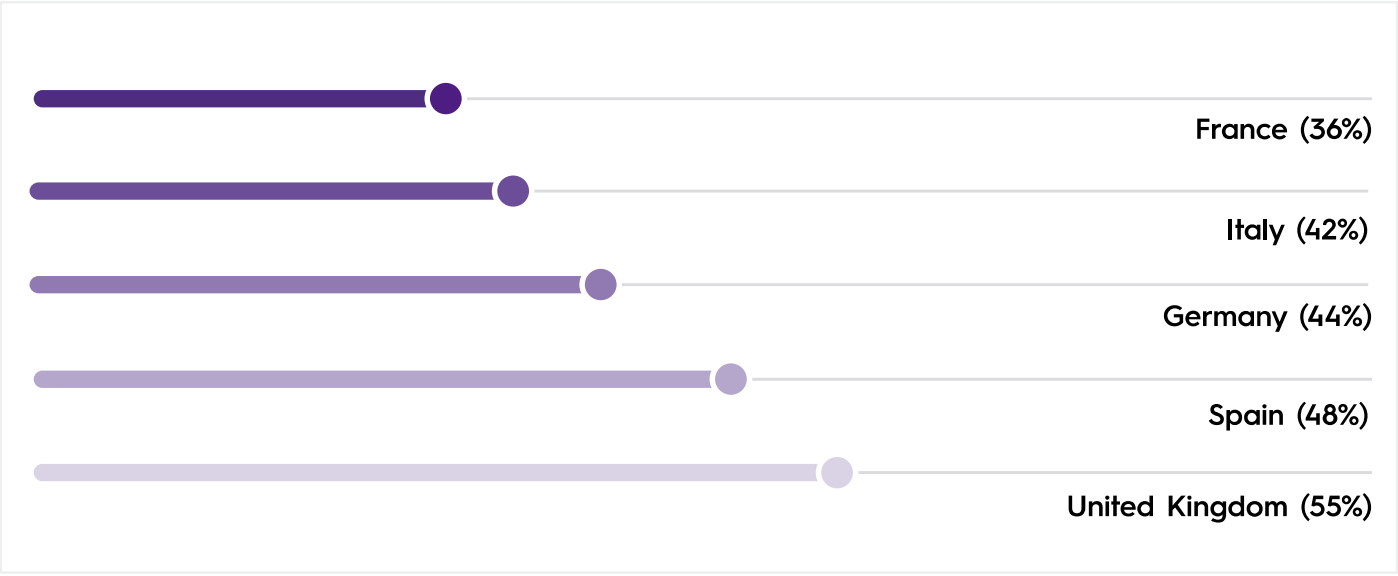
1. API quality and technical reliability:

Underperforming or unstable interfaces complicate user journeys and limit adoption as observed in France for PIS. The new PSR regulation aims to remove these obstacles by imposing transparency, performance, and the elimination of unjustified blockages.

2. Trust and perception of data sharing:

In some countries, consumers do not perceive that the regulatory framework protects them and are reluctant to share their banking data, which slows development.

According to the **Digital Banking Experience 2025** study (Forrester & Sopra Steria), European consumers' sense of security regarding the online use of their financial data varies greatly: 55% in the UK versus 36% in France, with Spain (48%), Germany (44%) and Italy (42%) in between.



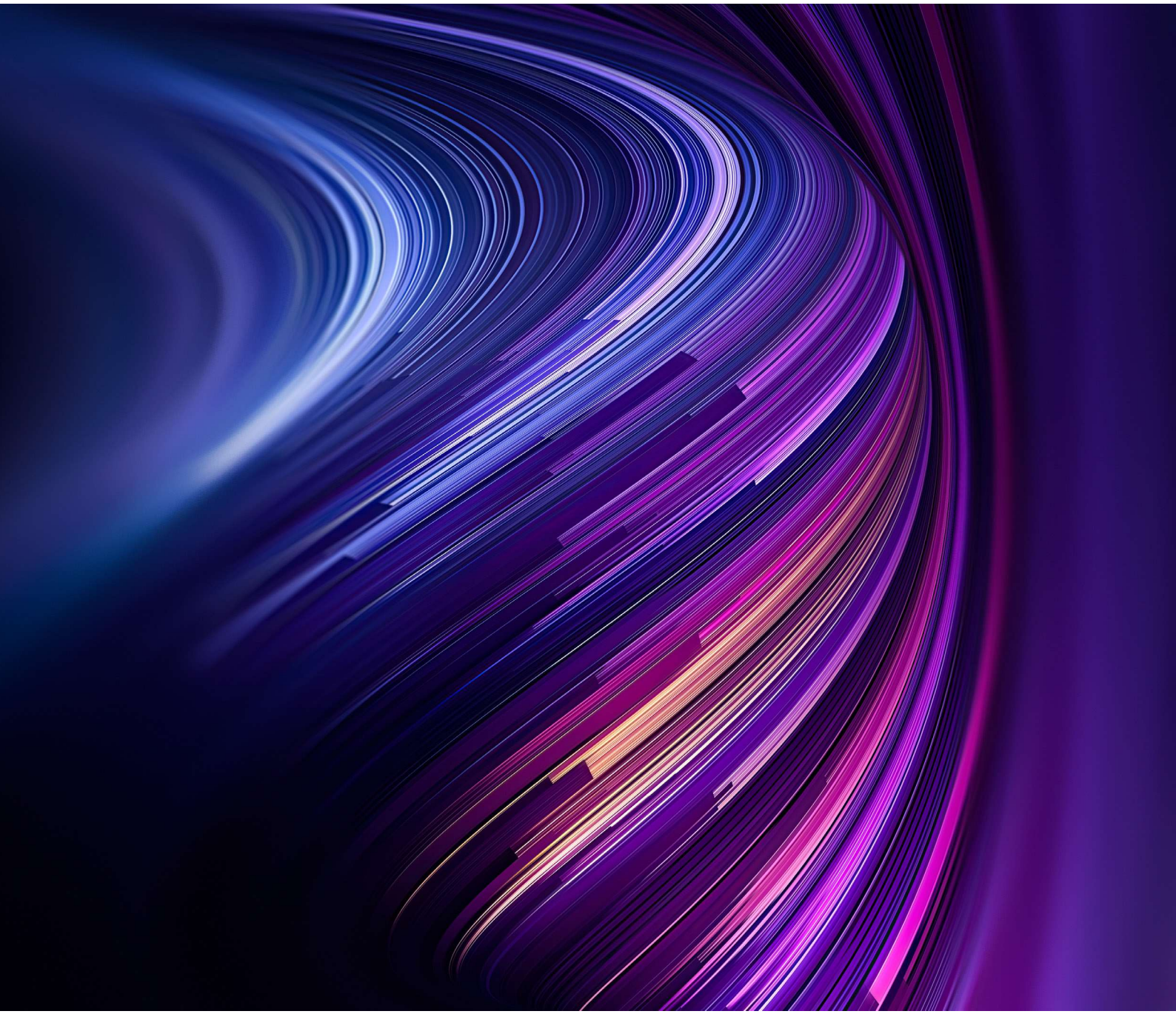
Moreover, the type of actors also strongly influences perceptions: for example, in France, 56% trust their main bank, but only 20% trust third-party financial players, a gap that is much narrower in the United Kingdom (with more than 40% stating they are inclined to share their financial data with third parties), a sign of greater openness to innovation.

Strengthening the clarity of consent and control over data appears essential to bridge this trust deficit; this is also a pillar to which PSR is committed.

3. Divergent regulatory approaches and heterogeneous implementation:

PSD2 was a directive, meaning transposable into national law, which created heterogeneity in the way it was implemented in domestic legislation. PSR, a regulation that applies uniformly across Europe, will also partly address this point.

As a matter of fact, this fragmentation has been identified by the European regulator, which now seeks to remove the major obstacles highlighted through a new regulatory package, PSD3 and PSR.



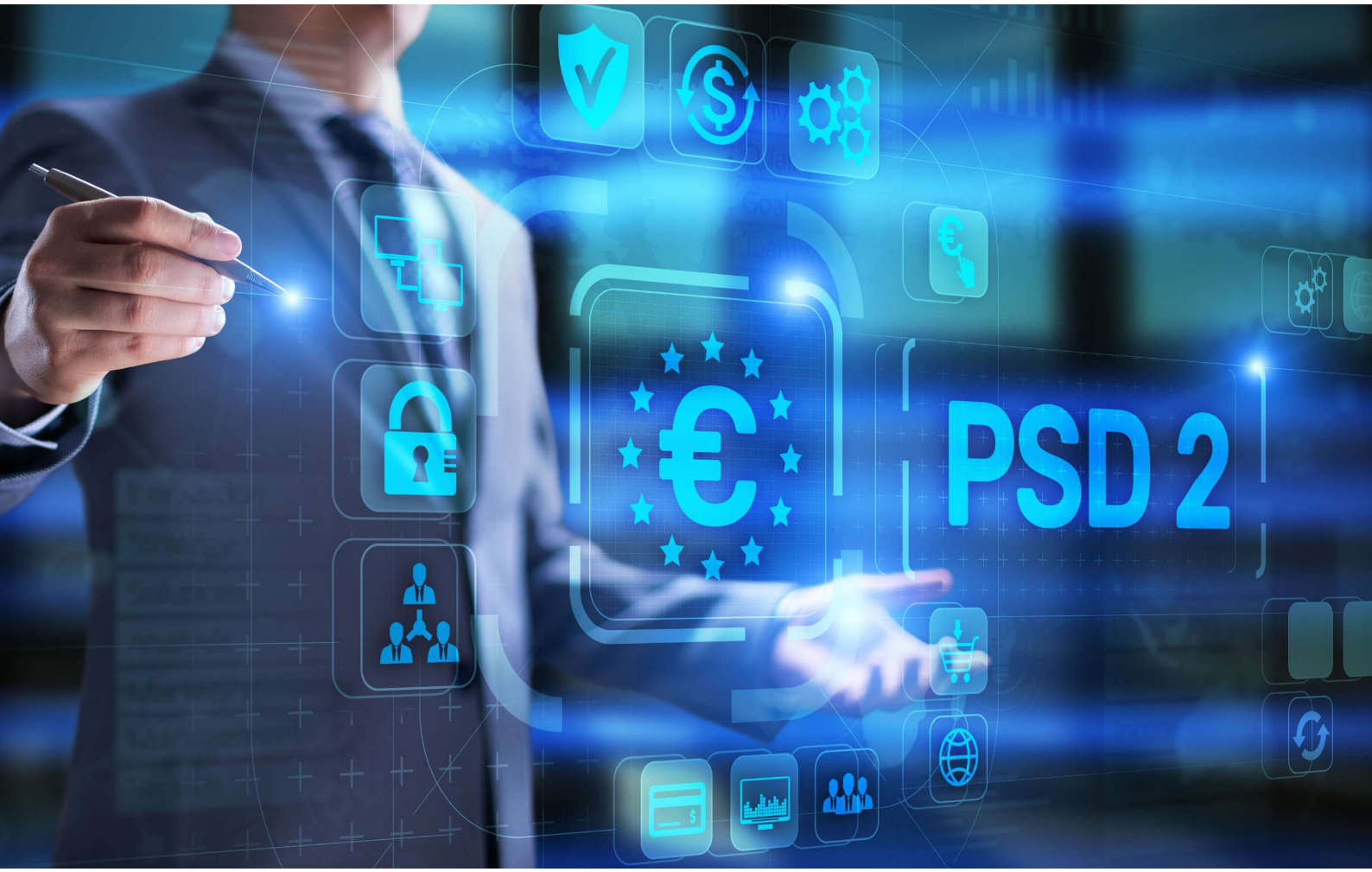
Part 2

PSD3 and PSR: a new structuring framework for Open Banking

The combination of **PSD3** (Payment Services Directive 3) and **PSR** (Payment Services Regulation) constitutes a normative overhaul: PSD3 clarifies and adjusts certain aspects of provider authorisation, while PSR more deeply restructures how Open Banking operates at the operational and technical levels, and in terms of trust and enforcement.

2.1 From fragmentation to harmonisation: the ambition of PSR

As we noted in our first white paper, PSR addresses weaknesses identified in the application of PSD2: disparities in interpretation and local applications (regulatory arbitrage), insufficient user protection and consideration of new fraud and security risks, as well as a lack of robust mechanisms to guarantee fair and high-performing access to data. In other words, PSD2 opened access to data, but actual usage showed that clear and binding rules were missing to ensure proper functioning. PSR responds by introducing a stricter deployment framework, with penalties that can reach up to 10% of global turnover in the event of breaches on major points, an unprecedented level.



2.2 The four major impacts of PSR

The latest version of PSR, proposed by the Council in June 2025 to support trilogue discussions, highlights four structuring transformation pillars.

1. Permission Dashboard (Articles 43 & 49)

This is the trust and governance breakthrough. Users must have a dashboard integrated into their banking interface, easy to access, allowing them to see in real time:

- The providers to whom they have granted access, for which account, for which purpose, with which categories of data, and over what period;
- The ability to withdraw or reinstate access within 48 hours, and a two-year history of expired or revoked permissions.

We emphasised this as early as 2024, and this dashboard will require profound changes for banks, with a need to rethink both the back ends (granular permission management, traceability, real-time notifications when a permission status changes) and the client front end (transparency, non-manipulation, a ban on dark patterns that encourage withdrawing or keeping permissions in an opaque way). Anticipating these changes will be key in order to ensure effective compliance and the smoothest possible customer experience.

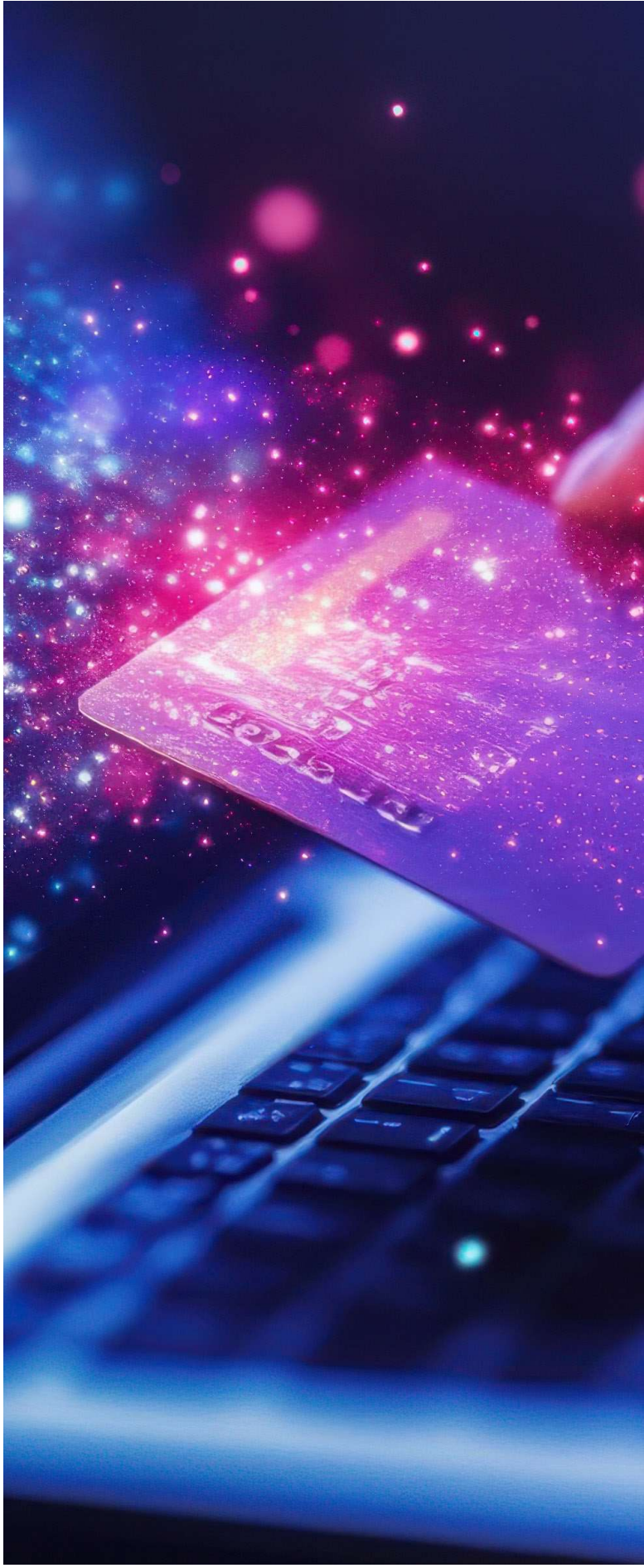
2. Regulatory APIs (Articles 35 to 42 and 44)

PSR requires the immediate removal of 10 unjustified obstacles ("prohibited obstacles") listed in Article 44, while strengthening the harmonisation of interfaces dedicated to Open Banking, as well as performance, availability, and data-parity requirements (the same scope of information must be accessible via API as is available to the end user on the banking interface).

Among the major obstacles, we can cite in particular:

- Unjustified limitations on the number of API calls or recurring unavailability; PSR *requires that API performance be equivalent to that of a standard user journey in the bank's interface;*
- Forced disconnections or unjustified session expirations; PSR *requires financial institutions to fully respect the duration of consent, with continuous and stable data synchronisation.*

The overall objective is clear: to enable third-party providers (TPPs) to access users' bank accounts under reliable, fair, and non-discriminatory conditions, mirroring the access available to users directly via their banking app.



3. Strengthening the fight against fraud (Articles 82 to 84)

In France, wire transfer fraud reached **168 million euros** in the first half of 2024, up **7.6%** despite a relatively low fraud rate **(0.0011%).** This increase is explained by a **29%** rise in the volume of fraudulent transactions, **47%** of which rely on manipulation of the payer (fake advisers, IBAN substitution) and **45%** on the misappropriation of banking credentials.

To minimise these risks and the amounts at stake, PSR aims to impose a **more harmonised and effective anti-fraud framework at the European level,** marking a break with the current fragmented approaches.

As soon as it enters into force, payment service providers will have to transmit standardised fraud data to national authorities, according to a common format defined by the EBA (Art. 82), which will reinforce existing reporting obligations to authorities. The regulation also introduces a framework for **information sharing between PSPs,** limited to cases of reasonable suspicion and accompanied by strict safeguards (for example, anonymisation and a maximum retention period of five years), in order to optimise the circulation of information and better combat repeat fraudsters (Art. 83a). To support this coordination, the Commission will set up a European platform bringing together authorities and private players to analyse trends, share best practices, and issue recommendations (Art. 83b). Moreover, technical measures are expected in order to effectively reduce fraud through strengthened prevention and detection.

On the preventive side, in addition to information exchanges encouraged between players, including cross-sector exchanges with telecom operators to combat spoofing and identity theft (Art. 59a), PSR emphasises information and training mechanisms. PSPs must therefore proactively alert their customers to new scams via appropriate channels, provide annual training to their teams, and particularly target vulnerable groups (Art. 84).

Regarding detection, PSR imposes the obligation of real-time monitoring of transactions. On the payer side, the control must take place before execution, and on the beneficiary side, upon receipt without delaying the credit (Art. 83). This monitoring will serve to trigger strong customer authentication (SCA), justify exemptions on the basis of risk, and detect fraud, including for payments initiated by third parties (PISPs). If the mechanism is absent or deemed insufficient, liability will lie directly with the PSP, which will have to prove its compliance.

4. Customer protection (notably Articles 51, 56, 59)

PSR places the user at the heart of its reform, with reinforced requirements in terms of transparency, readability, and control. For example, it will now be mandatory for each user to be able to directly manage their payment limits, by day, by transaction, or by instrument, with any increase subject to a security delay and strong authentication, a real circuit breaker against the fraudulent takeover of an account (Art. 51).

It also reaffirms the obligation for the PSP to carry out **Verification of Payee (VoP),** which will came into force as of October 2025 under the Instant Payments Regulation (IPR). In practical terms, the payer's bank must systematically verify the name/IBAN match and alert in real time in the event of a discrepancy. This verification will always be active. The user will have the possibility, when faced with an alert, to confirm or cancel the operation. And if, despite everything, the verification is not applied and an error occurs, the customer must be reimbursed immediately. Only then will the different providers determine their respective liabilities (Arts. 57 and 50).

Also, in general, the rules on reimbursement are strengthened. By way of illustration, in the event of an unauthorised transaction, the rule becomes clear: rapid reimbursement, at the latest on the next business day, except in cases of fraud or gross negligence by the customer duly proven. The burden of proof lies with the PSP (and with the PISP for its part), not with the customer (Arts. 55–56).

In addition, the payer's liability is capped in cases of loss, theft, or impersonation (excluding fraud or gross negligence) and drops to zero if strong customer authentication (SCA) was required but absent or wrongly exempted by the PSP (Arts. 58 and 60).

In short, PSR must now assume the role of a genuine **pro-consumer shield,** and it aligns with the approach already promoted in the United Kingdom with the liability shift introduced in 2024, where responsibility in the event of fraud is transferred to providers in the absence of sufficient protective measures.

2.3 In summary: PSR, a transformation, not a mere adjustment

Ultimately, the impact of PSR will be anything but marginal. With a compliance deadline set at only 24 months after the regulation is adopted, institutions will have to undertake profound transformations in the customer relationship (more transparency, more user control), in technical architectures (back ends, APIs, real-time monitoring), and in internal processes (consent management, information sharing, reimbursement within 24 hours). Penalties of up to 10% of global turnover underline that the financial stakes are substantial. Beyond simple regulatory compliance, PSR aims to establish a fully secure framework for European Open Banking, capable of eliminating obstacles, restoring user trust, and encouraging active participation in an open and resilient digital ecosystem.

It is therefore essential for banking institutions to prepare for this transformation and to anticipate it through a fine-grained analysis and understanding of the text, in order to guarantee effective and complete compliance within the allotted time.

Part 3

FIDA: The future of Open Finance takes shape

3.1 The shift from Open Banking to Open Finance

As we introduced as early as 2024, FIDA (Financial Data Access Regulation) is the forthcoming European regulation that aims to extend data access and sharing beyond payment accounts to savings, investments, credit, insurance, pensions, and crypto-assets. This broader scope corresponds precisely to the concept of **Open Finance**. According to the initial discussions, sharing would be based on user-granted permissions, via a dashboard equivalent to that in PSR, within a market framework organised by sharing schemes (FDSS, or Financial Data Sharing Schemes) that would define technical standards, governance, SLAs, and compensation mechanisms.

The objective? Accelerate innovation while protecting trust and security.

After a period of uncertainty and rumours of the text being cancelled in February, FIDA ultimately continued its legislative path from March 2025. The latest trilogue in June 2025 (a three-way negotiation between Parliament, Council, and Commission to finalise a text) has not yet led to a compromise, but it was able to assess simplification proposals presented in three "non-papers", aimed at further aligning regulators and financial institutions, which view the text primarily as a significant financial burden.

Definition box: (Non-paper)

A non-paper is an informal note (Member State, Commission, or coalition) that steers the legislative debate: drafting options, timing or scope variants, governance principles. These documents do not bind the legislator, but they can strongly influence trilogue compromises.

3.2 Major simplification proposals under review according to the "non-papers"

1. Data scope

Should the entirety of financial data be opened, at the risk of handling a large volume of information (sometimes of limited usefulness), that would increase costs and slow deployment, or should priority be given to high value-added use cases?

A graduated approach is favoured in the non-papers. The idea is to identify the most promising use cases upfront and prioritise them. However, assessing demand for these use cases is largely an open question today, since this is a new market with consumer habits still to be created.

As of now, there is mainly discussion of excluding large enterprises from the scope and focusing on retail customers and small businesses, as well as limiting the historical depth of data made available (for example, between 2 and 5 years).

2. Monetisation:

What economic model for consent-based data sharing would incentivise banks without "killing" innovation in the fintech ecosystem?

At this stage, two avenues are being studied: an initially favoured path around "reasonable compensation" for institutions (no margin), and a model put forward in the latest version of FIDA (December 2024), involving the possible introduction of a margin for financial institutions.

3. Sharing schemes (FDSS):

What responsibilities should schemes have, and what governance should be put in place to operate them?

Definition box: (FDSS)

A sectoral scheme that organises access to and sharing of data (governance rules, API standards, security, compensation model, responsibilities, reporting).

A scheme is not a new actor or a central platform. It is a framework (rulebook): a set of common rules that independent participants adhere to (data holders and data users). The FDSS does not host data: each participant exposes or consumes data via its own APIs. A scheme operator (often an association or consortium) can facilitate the framework and perform compliance checks, but remains a facilitator, not a data collector.

As early as 2024, we highlighted that schemes would be central to how FIDA operates, with several potential scenarios for their operation and governance, and with players such as Visa and Mastercard potentially positioning themselves by leveraging their experience with payment schemes.

The non-papers do not yet clarify who will operate these schemes; they focus more on specifying how they are constructed. In line with demand-led prioritisation of use cases, schemes would be formed only around priority products and would have at least one year to define initial technical and governance standards. If no scheme were to emerge, the Commission could then set a minimal baseline by delegated act, as a last resort, in order to ensure the launch of FIDA.

In all cases, whether schemes are introduced and defined by market actors or directly by European institutions, the EUDI Wallet (the European digital identity wallet that allows citizens to store and use their official credentials online) would be recommended to provide homogeneous authentication by end users, at least for individuals, and possibly for businesses. Other concrete deployment modalities for the schemes are not mentioned at this stage.

4. Role of gatekeepers:

Should they be excluded from acting as operators of data-sharing schemes (FDSS) and more broadly from their ability to consume or exploit Europeans' financial data in order to safeguard European sovereignty, or should they be considered for inclusion, as envisaged in the version of FIDA commented on by the European Council at the end of 2024?

Definition box – (Gatekeeper)

In the Digital Markets Act, a gatekeeper is a very large platform designated by the European Commission because it controls one or more core platform services (for example, mobile OS, search engine, messaging, social network). Owing to a massive user base and unparalleled volumes of behavioural and transactional data, they have a significant natural advantage that can threaten competition (network effects, lock-in, information asymmetry) if it is not strictly regulated. This is a central issue when discussing data access and sharing under FIDA.

The non-papers are unanimous and advocate the need to exclude these gatekeepers entirely in order to avoid unfair non-European competition. The leveraging effects of BigTechs are indeed a major issue (data access plus distribution), creating negotiating imbalances and risks for sovereignty. FIDA aims to foster innovation, while preventing dominant positions of foreign players from controlling European financial data.

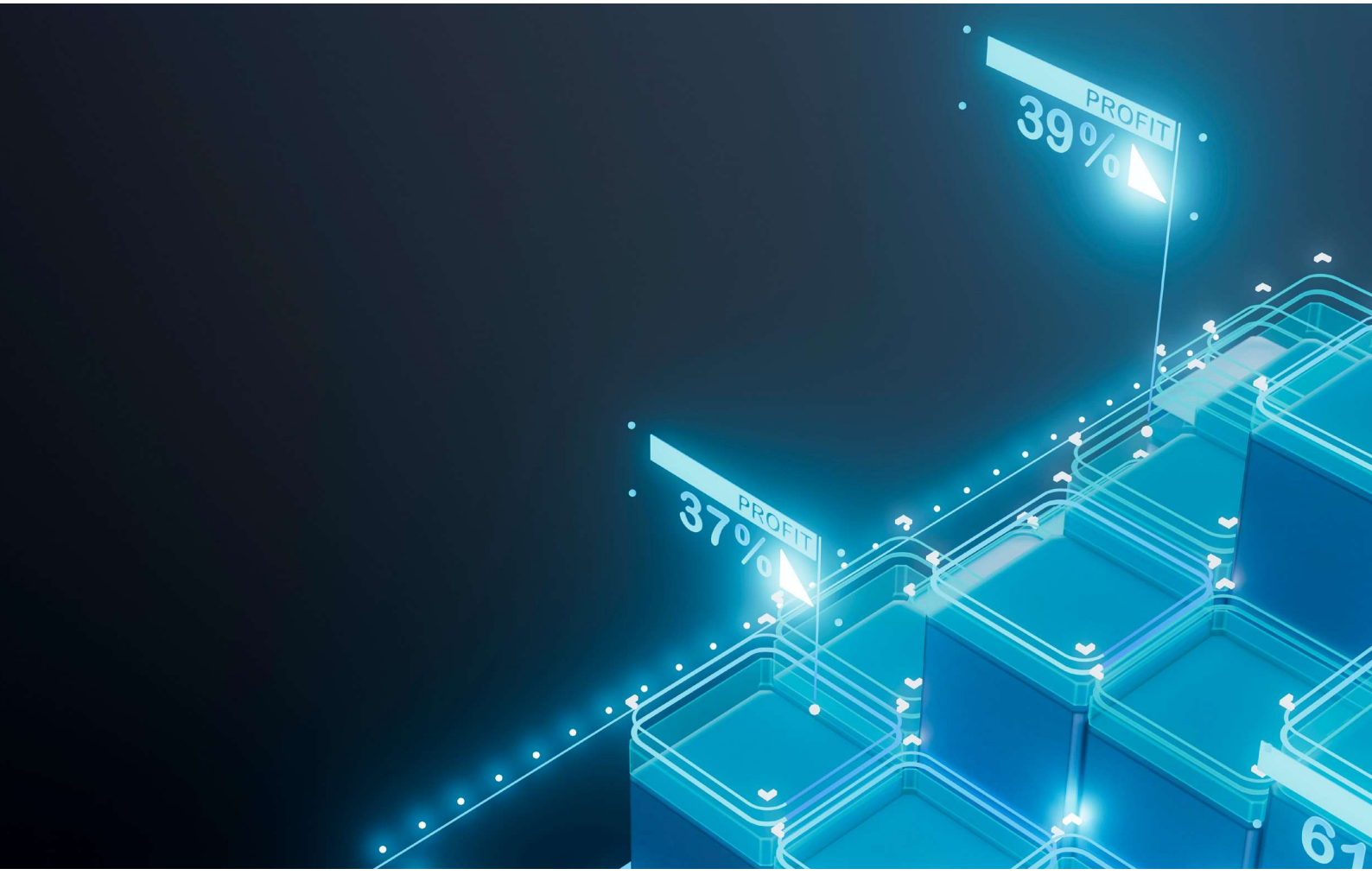
At a minimum, these gatekeepers should be excluded from applying for FISP status (Financial Information Service Provider), the intermediaries that could build services around data originating from FIDA, similar to current AISPs and PISPs under the PSD2 perimeter. Also under consideration is the possibility of excluding BigTechs as data users, namely from the ability to access a customer's financial data via a FISP in order to provide a service or product, with the customer's explicit consent.

These four key questions will be decided during upcoming trilogues starting in September 2025.

3.3 What stakeholders must do now

There are still many uncertainties around FIDA. However, the European institutions seem determined to pass this text. Given the changes introduced, it is essential for financial institutions to start preparing for this big bang by:

- Structuring data governance suited to Open Finance, notably through a mapping of existing data;
- Identifying high value use cases in order to highlight them so that Europe also decides to prioritise them;
- Building technical bridges between Open Banking and Open Finance, notably by unifying consents with permission dashboards that should be common to both regulations (FIDA and PSR) and by industrialising APIs;
- Modelling monetisation scenarios based on estimates of future demand and associated costs;
- Engaging in active monitoring of European trilogues and non-papers.



Conclusion

Seize the opportunity, now!

One year after our first analyses, the conclusion is clear: the forthcoming Open Finance regulations are highly structuring, and their finalisation is fast approaching.
In mid-June, a new version of the PSR was published, with a vote expected before the end of 2025. In parallel, the trilogue on FIDA has resumed, with concrete avenues for simplification and deployment.

The transformations to be undertaken, technical, organisational, and on the customer experience, are profound, and waiting until the last minute is no longer an option. Until now, most banks have limited themselves to opening access to their data, without truly developing services around it. PSR, and even more so FIDA, reshuffle the deck: it is up to institutions to decide whether they simply want to comply, or whether they will finally take advantage of these developments to innovate and deliver new value-added services, such as a consolidated wealth view thanks to the inclusion of more exhaustive financial data, or dynamic insurance services.

The winners will be those who have anticipated, influenced, and defined a clear strategy around this open finance, a European promise initiated in 2018 with PSD2, and one that could be greatly extended with FIDA by 2030.

At Sopra Steria, we support you on this journey, starting now, notably through our PSR Readiness Check: a fast, operational, fact-based assessment even before the vote, to:

- Measure your level of preparedness across the four key PSR pillars defined in this paper;
- Identify technical and organisational gaps;
- Prioritise the structuring workstreams, in particular those exposed to penalties of up to 10% of revenue;
- Build an acceleration roadmap at 6, 12, 18, and 24 months.

Because the future of Open Finance should not simply be endured.

It can be built. Starting today.