I-7

Open Finance and Innovation: Exploring Opportunities and Addressing Challenges

Liliana Fratini Passi, Biancamaria Raganelli
CBI Scpa - University of Rome Tor Vergata

Abstract

This chapter examines the evolution of Open Banking and Open Finance in the European financial sector, highlighting how technological innovation, digital transformation, and data sharing are reshaping the industry. It analyses the regulatory framework, including PSD2, PSD3, the Payment Services Regulation, and the proposed Financial Data Access Regulation (FIDA), which aims to balance innovation, competition, consumer protection, and security.

The authors emphasize the role of collaborative platforms, APIs, and Financial Data Sharing Schemes in enabling third-party access to financial data while safeguarding privacy and cybersecurity. They argue that while Open Finance offers significant opportunities for personalised services, increased efficiency, and cross-border integration, it also raises complex challenges regarding compliance, regulatory harmonisation, and operational risks. The success of these open models depends on a coordinated European approach that reconciles innovation, security, and market stability, thereby fostering a competitive yet trustworthy financial ecosystem.

Keywords: Open Banking, Open Finance, financial data access, PSD2, PSD3, Financial Data Access Regulation, digital finance, financial innovation, cybersecurity, regulatory harmonization, APIs.

1. The technological revolution and its implications on financial services

The technological innovation in recent years has triggered an evolutionary process with significant repercussions across multiple sectors. In the financial services industry, technological acceleration has enabled the development of new products and services while profoundly transforming the operations of market participants. Traditional actors—most notably banks—and new entrants such as FinTech firms have been compelled to confront unprecedented challenges and to rethink their operating models. In particular, they have increasingly adopted "open" business models based on the sharing of customer data and the interoperability of an open and competitive ecosystem. This transformation has generated both new opportunities and novel regulatory concerns, while intensifying competition in the provision of financial services.

Within this context, the concept of Open Banking refers to the ability of third parties, subject to customer consent, to access data and information relating to payment accounts held with banks to provide innovative services and applications. Open Finance, as an extension of Open Banking, envisages an even broader sharing of financial data among market participants and represents a significant opportunity for consumers and businesses alike. By enabling access to more comprehensive datasets, Open Finance facilitates the design and provision of products and services that are better tailored to the specific needs and expectations of users, thereby supporting more accurate and sophisticated models of service delivery.

This evolution marks a departure from the traditional model in which data was generated, processed, and exploited exclusively within a single banking intermediary. The boundaries of the system have expanded through an increase in both access points and the range of actors entitled—within the limits set by the applicable regulatory framework—to access, use, and reprocess payment account data in order to offer new services. In this environment, regulation plays a crucial role in ensuring the stability of the ecosystem, by providing clear guidance that enables all stakeholders to operate in conditions of security, reliability, and efficiency. Correspondingly, regulatory and supervisory authorities are required to recalibrate their approaches, pursuing a dual objective: on the one hand, fostering innovation and the market offering of new services; on the other, adapting traditional supervisory and oversight methodologies to the specific risks associated with novel infrastructures and technologically complex systems.

The technological revolution in finance has also produced significant social implications affecting many aspects of individuals' daily lives and raising complex economic and legal issues. These include, inter alia, cybersecurity and exposure to cyber-attacks, risks of fraud and market abuse, and challenges related to transparency and information asymmetries. While digital finance offers substantial benefits, it may also complicate the pursuit of core regulatory objectives such as financial stability, consumer protection, market integrity, fair competition, and systemic security, thereby introducing new categories of risk that regulators and supervisors must identify, monitor, and mitigate. This scenario requires robust regulatory frameworks and collaboration between financial institutions, technology providers, and supervisory authorities to ensure innovation does not compromise security, fairness, and consumer trust.

In Italy, following the implementation of the regulatory framework introduced by the PSD2 Directive, the interfaces developed by payment service providers to facilitate third-party access are predominantly based on technical system solutions that operate as single points of access for multiple intermediaries.

In response, the Supervisory Authority has developed a control framework that reflects the highly innovative features of the market. This includes the systematic collection of statistical data aimed at monitoring the efficiency, reliability, security, and regulatory compliance of such system solutions, and at developing indicators capable of assessing the evolution and resilience of the national payments ecosystem.

Finally, a number of sensitive issues emerge that cannot be adequately addressed from a purely domestic perspective. As recently emphasized by the Supervisory Authority, improving the efficiency of cross-border payments requires enhanced international cooperation and the joint analysis of innovative technical solutions, as well as the alignment of policy objectives across jurisdictions. This represents a complex challenge, one that necessarily calls for coordinated action by both public authorities and private stakeholders at the transnational level.

2. The "open" ecosystems and the parties involved

The progressive sharing and utilisation of customer authorised financial data by banks with third-party providers has fostered the development of innovative financial services, including real-time payments, enhanced account transparency, and targeted marketing opportunities, enabling both individuals and businesses to exercise greater control over their financial position (Bank for International Settlements, BIS, 2021).

The evolution from Open Banking to Open Finance extends these dynamics beyond payment data, granting third-party providers access to a broader spectrum of financial information—savings, mortgages, pensions, insurance, investments, and securities—thus enabling the design of personalised data-driven financial products tailored to consumer needs (Bank of Italy, 2023). Open Finance, together with Central Bank digital currencies and private-sector cryptocurrencies, is expected to reshape competitive dynamics in the international financial sector.

Empirical evidence highlights the rapid expansion of the European fintech ecosystem. In Italy, 377 Account Servicing Payment Service Providers (ASPSPs) and 85 active Third-Party Providers (TPPs) operate in the Open Banking space, with the majority integrating Personal Finance Management solutions (Bank of Italy, 2023). Across Europe, start-ups securing at least USD 1 million in funding have increased by 81% since 2020, raising USD 35 billion collectively over the past five years (European FinTech Report, 2022). In 2022, the number of registered TPPs providing services beyond account access grew by 12% offering primarily Account Information Services (AIS) and Payment Initiation Services (PIS), alongside emerging solutions in investment, credit, insurance, statistical analytics, and cybersecurity.

The United Kingdom remains the European hub for fintech, hosting 38% of start-ups, followed by France and Germany (11% and 9%, respectively) (European FinTech Report, 2022). Italy, by contrast, exhibits moderate adoption rates of digital banking (approximately 50%) and limited engagement with Open Banking and Open Finance services, attributable to low awareness and investment (Bank of Italy, 2023). Nevertheless, API calls have tripled since 2020, reflecting growing utilisation, particularly for AIS and PIS functionalities. Investment in value-added services beyond PSD2 compliance has begun to increase, signalling an emerging shift in commercial offerings by Italian banks.

The expansion of Open Banking and Open Finance underscores the need for regulatory frameworks that balance innovation with market stability, consumer protection, and cybersecurity. National authorities, including supervisory bodies, must recalibrate oversight to accommodate these new technological realities while fostering competition and efficiency in an increasingly interconnected and data-driven financial ecosystem (European Banking Authority, 2021).

3. Collaborative initiatives

Promoting innovation through collaborative initiatives has become a decisive factor in facilitating the adoption of new financial products and services by both enterprises and consumers. Multistakeholder groups operating within the pan-European area play a central role in developing "open" models, supporting the creation of innovative services and ensuring seamless interoperability among market actors. For example, within the European Payments Council—a non-profit international association composed of 77 Payment Service Providers (PSPs) or PSP associations established to support and promote the integration and development of European payments—a scheme known as SPAA (SEPA Payment Account Access) is under development. SPAA, through a framework of rules, best practices, and technical standards, enables the exchange of payment account data and facilitates the initiation of transactions via value-added Application Programming Interface (API) services.

According to data from the *Global Open Finance Report*, published by CBI in collaboration with PwC Italy in 2023, the API offering technically, an API is a method used by two software systems (applications) to exchange data between EU market actors remains strongly focused on Account *Information* services (AIS) and Payment Initiation services (PIS), which are mandatory under PSD2 and represent 55% of monitored APIs. *Open Finance* APIs are consolidating, particularly for investment services, which represent 10% of the total, while those relating to, for example, Loans and Insurance are still lagging; the analysis highlights how market operators focus on "Statistics & Information" (11%) and "Security" (8%) APIs, suggesting the strengthening and enrichment of their "Open" offering with the inclusion of accessory services alongside core ones offered mainly by traditional banks.

In Italy, the market is predominantly concentrated around account information services, with 85% of respondents (+55% relative to 2021) including commercial offers linked to account aggregation. A smaller proportion of operators have developed Personal Finance Management (PFM) or Business Finance Management (BFM) solutions. Growth has also been observed in new value-added services, such as "Check IBAN," which now exceeds 60% adoption.

Among platform solutions, CBI Globe—developed in 2019 by CBI S.c.p.a., a Benefit Corporation since 2023—has emerged as a leading international Open Banking and Open Finance ecosystem, significantly streamlining connectivity among European PSPs via API. This infrastructure has enabled the development of advanced fintech services addressing the evolving needs of corporate and retail clients, including Check IBAN, CBI GO, Name Check (Verification of Payee, VoP), and the Invoice Control Database service (Safe Trade), which has been admitted to the Bank of Italy's Regulatory Sandbox. In 2023, CBI Globe, adopted by approximately 80% of the Italian financial industry, recorded nearly 800 million API invocations (+150% compared to 2022) executed by over 500 PSPs across Europe.

Collaborative innovation is an ongoing process. It is essential to broaden the perspective by expanding the range of actors operating on platform functionalities, allowing PSPs to strengthen their commercial position with businesses and end customers, while leveraging strategic partnerships with EU stakeholders. Examples include the "Cross-Border Check

IBAN," which allows real-time verification of the association between IBANs and VAT numbers, thereby reducing fraud risk; "Name Check" (VoP), which verifies the correspondence between IBANs and beneficiary names in compliance with the Regulation on Instant Payments; and Safe Trade, which aggregates multi-bank, multi-channel invoice data to enhance financial sector stability and mitigate risks associated with fraudulent credit disbursement. Furthermore, Smart Onboarding (CBI GO) enables corporates to retrieve end-user information in real time through telematic interaction with the user's bank.

To support the transition toward increasingly open financial models, it is essential to maintain an appropriate balance between innovation and security. Robust infrastructure, such as the CBI Hub Cloud, facilitates the migration of multi-bank payment and collection transactions—currently managing interactions between Italian companies and public administrations—onto dedicated cloud technology. This architecture enables credit institutions to offer corporate and retail clients, as well as public administrations, more advanced and real-time transactional and Open Finance services, thereby enhancing efficiency, security, and integration across the national payments market.

Hopefully, this will lead to a European and global vision capable of crossing traditional State borders and extending regulatory and supervisory framework beyond the confines of domestic legal systems. For banking intermediaries, this creates an opportunity to capitalise on a significant wealth of experience, fostering collaboration to enhance competition and transform the dynamics of a highly competitive environment into sustainable long-term success. However, it is desirable that the ambition extends beyond the boundaries of banking activity in the strict sense and encompasses the entire financial market as a broader macro-system, in which various types of intermediaries operate, ensuring adequate services and protections for customers.

Recent studies provide quantitative support for the trends described above. According to the Bank of International Settlements (BIS, 2022), the sharing and exploitation of payment account data by banks withauthorised third parties enables greater financial control for both individuals and businesses, while also creating new opportunities for real-time payments and enhanced transparency. The Global Open Finance Report (2023) confirms that 55% of EU APIs continue to focus on Account Information Services (AIS) and Payment Initiation Services (PIS), with investments and ancillary functionalities such as statistics, security, and information services expanding steadily.

In Italy, the Bank of Italy (2023) reports 377 Account Servicing Payment Service Providers (ASPSPs) and 85 active Third Party Providers (TPPs), 39 of which are domestic, most integrating Personal Finance Management solutions. API calls in Italy have tripled since 2020, reaching 51 million, demonstrating a rapid increase in usage despite moderate adoption of Open Banking and Open Finance services among end-users. Funding data further illustrate the rise of innovative start-ups: European fintechs raising at least USD 1 million grew by 81% from 2020 to 2022, totalling USD 35 billion over five years, highlighting a significant shift in the competitive landscape of financial services.

These quantitative insights underscore the strategic importance of continuing to develop robust and secure Open Banking and Open Finance infrastructures, supporting both market expansion and consumer protection within a rapidly evolving European financial ecosystem.

4. Ready for regulation?

More than forty countries worldwide have implemented initiatives in the fields of Open Banking and Open Finance, albeit following diverse regulatory approaches. Europe, through Directive 2015/2366 on payment services (PSD2), was a forerunner in establishing initial regulatory frameworks for the sector. The directive aims to enhance the protection of payment service users, increase transparency and security, and foster efficiency and innovation in a market that, due to its rapid expansion, often lacked adequate regulatory safeguards. PSD2 seeks to promote greater competition in the payments market and ensure wider accessibility to customer account information. In Italy, the integration of the 2007 PSD1 regulations and the transposition of PSD2 was satisfied by the Legislative Decree no. 218/2017. Moreover, building upon the principles introduced by PSD2, the upcoming PSD3 and the Payment Services Regulation (PSR) aim to further enhance consumer protection, strengthen cybersecurity measures, and harmonise rules across the EU to address new technological and market development.

Unlike some other jurisdictions, the European legislator adopted a prescriptive approach, mandating that all payment service providers managing customer accounts allow third-party access for payment initiation or for processing aggregated account information. The objective was to foster competition in a payments market historically concentrated around a limited set of products and operators—such as card-based services—while recognizing the emergence of technologically advanced services beyond traditional payments. These services, now widespread, required formal regulation to ensure consumer protection and promote sectoral development. In this way, PSD2 simultaneously encourages innovation, competition, and safeguards in a sector that tends naturally toward oligopolistic structures.

However, the system introduces new operational complexities. It overlays an additional layer of service offerings and compulsory interaction between authorised third parties and account-holding payment service providers onto the pre-existing architecture, in the absence of universally agreed operational procedures or consolidated standards. Banks are obliged to honour access requests from authorised third parties unless objective grounds, such as fraud risk, justify refusal.

Internationally, different approaches can be observed. In Canada, Brazil, and South Africa, authorities adopt a prescriptive model, issuing regulatory or technological frameworks for specific categories of participants. In contrast, countries such as the Philippines employ a "facilitator" approach, where central banks issue guidelines to encourage collaboration among actors and support financial inclusion. Finally, a market-driven model exists in which industry players themselves define standards and services, without direct regulatory intervention.

In Europe, the EU Commission has worked on broadening the provisions contained in the Payment Services Directive (PSD2) in the *Open Banking* sector, moving toward Open Finance by launching important initiatives including the *Digital Finance Package* - a set of legislative measures defining how the EU can support digital transformation and innovation in the financial sector. These measure include significant actions in areas such as *Digital Identity, Open Finance*, Crypto-assets, *Digital Resilience, Blockchain*, and consumer protection.

The *Digital Finance Package* aims to make financial services more digital fostering responsible innovation and competition among different competitors in the European Union. The strategy seeks to ensure a level playing field among financial service providers, whether traditional banks or fintechs, based onthe principle of *"same activity, same risks, same rules.*

Consequently, financial services are increasingly migrating into digital environments characterized by fragmented ecosystems, with digital service providers often operating under temporary derogations permitted by sectoral regulation. Digital finance introduces challenges for safeguarding financial stability, consumer protection, market integrity, fair competition, and security, raising issues that require coordinated attention from regulators at national, European, and global levels, encompassing legislators as well as independent supervisory authorities. In this context, it is desirable that European reflection converges toward a centralised regulatory and supervisory perspective capable of ensuring uniformity of approach while reconciling top-down design with appropriate bottom-up stakeholder dialogue.

Digital finance can make safeguarding financial stability, consumer protection, market integrity, fair competition, and security more challenging, bringing new issues to the attention of regulators at multiple levels (national, European, and global) and of different types (legislators, independent regulatory and supervisory authorities). It is desirable that, at least in Europe, reflection be directed toward a centralised regulatory and supervisory approach that ensure uniformity, reconciling top-down design with adequate bottom up dialogue.

With the aim of enabling the design of services within a broader European vision of an "open asset sharing economy," the European Commission published the proposal for the Third Payment Services Directive (PSD3) and the accompanying Payment Services Regulation (PSR) in June 2023. This marked the beginning of the legislative process. It is important to note that the PSD3 is not yet in force. After formal adoption, it will need to be transposed into national laws, which is expected to occur by 2027–2028, following a similar timeline to PSD2.

European regulation of account access services is structured on several levels: PSD2 and its national transposition sources; the RTS (Regulatory Technical Standards) and other secondary implementing rules defined by the EBA (European Banking Authority); and interpretations provided by both the Commission and the EBA through the "Questions and Answers" tool. The core innovations lies in the sharing of the customer's information assets: a new model that differs sharply from the traditional one based on a bilateral bank-customer relationship.

The second Payment Services Directive (2015/2366/EU) introduced this framework enabling new open banking service models whereby a customer of a payment service provider - where an online account is held (so-called *Account Servicing Payment System Provider* – ASPSP) can use an authorised third party (so-called *Third-Party Provider* – TPP). The TPP may operate as a *Payment Initiation Services Provider* (PISP), initiating payments from the online account an *Account Information Services Provider* (AISP), providing consolidated information on online accounts held across multiple payment service providers (ASPSPs). Alongside the directive, the framework includes national transposition measures, RTS and other secondary rules defined by the EBA, as well as interpretations provided by the Commission and EBA.

This is a complex set of rules, originating from different regulatory sources and various types: the provisions contained in the directive are joined by those elaborated by the European Banking Authority, one of the three Financial Supervisory Authorities connected to national authorities through a multi-level network model. .

Implementing regulations are set out in the "Regulatory Technical Standards (RTS)", prepared by the EBA and adopted by the European Commission. In the Delegated Regulation of November 27, 2017, the European Commission detailed all technical standards for customer authentication and communication. .

Thus, the need emerged to balance the conflicting interests of banks, third parties, and their respective users, interests that cannot be resolved through spontaneous market discipline or structured forms of self-regulation. In the absence of a direct contractual relationship, the rights and obligations characterizing the relationship between the third party and the bank are regulated (Articles 64 to 67 of PSD2). Services offered to customers must comply with these provisions and the relevant contracts must conform accordingly.

Specific provisions define the liability regime usually borne by the bank in the case of operations carried out with the intermediation of a third party. These address proper authentication and execution of payments, management of user consent, and the allocation of liability in the case of unauthorisedoperations.

Other regulatory provisions concern the operational interaction between the bank and the third party: second-level rules established by the EBA establish technical requirements for mutual identification and secure communication, access methods via specific interfaces, and measures to ensure continuity of communication channels. The proper functioning of the entire system depends on the correct and uniform application of "regulatory standards". Through its guidelines and opinions, the EBA has clarified detailed aspects and reduced the scope for interpretation.

The regulation, transposed in Italy with the Legislative Decree of December 15, 2017, modified the Consolidated Banking Act (TUB in the Italian acronym). Efforts were made to converge on common technical standards for implementing dedicated interfaces, leading to the adoption of the "NextGenPSD2 Framework" standard. Subsequently, the national banking system organized itself to define «system» application solutions for creating these dedicated interfaces. As a result, a central role was assumed by the previously mentioned "system platforms," which support both banks and third parties.

On June 28, 2023, the European Commission published a proposal for the adoption of a regulation aimed at defining a harmonised regulatory framework regarding access to financial data: the so-called *"Financial Data Access"* or «FIDA».

It aims to promote the creation of a so-called *Open Finance* system, which allows the sharing of user data among subjects operating in the banking, investment services, insurance, payment, and financial sectors, starting from the rules of the PSD2 directive, but guaranteeing high standards of security and confidentiality by operators. It therefore intends to promote the development of financial products personalised based on customer needs and facilitate the creation of innovative business models based on access to user data, ensuring that data usage occurs only with user consent. This system could bring Europe closer to countries like Brazil, Hong Kong, and Australia, allowing for the development of Open Finance.

The European Commission's *European Data Strategy* ***aligns*** with the fundamental approach of the proposed *Data Act* of February 23, 2023. The FIDA regulation proposal fits into a group of proposals or reform measures applicable to financial services and user data management at the European level: the new Payment Services Regulation (PSR) and the new Payment Services and Electronic Money Directive (PSD3). Together these form a single "*Financial Data Access and Payments Package*" which establishes the regulatory framework for *Open Finance* and *Open Banking*.

The FIDA regulation should apply to all subjects subject to supervision under Union law, with some limited exceptions regarding below-threshold managers and insurance intermediaries qualifying as SMEs.

It should regulate the sharing of customer data (so-called "*customer data*") of a personal nature ("*personal data*") or non-personal nature ("*non-personal data*"), provided by customers themselves or generated by customer interaction with the intermediary and collected, stored, or otherwise processed by an intermediary in the context of their ordinary activity with customers.

Numerous types of data are involved, including loans, mortgages, savings, investments, pensions, non-life insurance, creditworthiness, pension products, and financial suitability and appropriateness assessments. More precisely, access is provided for data regarding: mortgage credit, loans, and accounts (except for payment accounts under PSD2); savings, investments in financial instruments, insurance-based investment products (IBIPs), crypto-assets, real estate and other financial assets, as well as economic benefits deriving from such assets, including data collected to perform suitability and appropriateness assessments; pension products; non-life insurance products (except for products covering health and sickness risks), including information collected to perform the consistency assessment ("*demands and needs test*") and appropriateness/suitability of the insurance product; and data forming part of the creditworthiness assessment of a company collected in the context of a loan application or *rating request*.

A new category is envisaged, the *Financial Information Service Providers* (FISP), corresponding to the *Account Information Service Providers* (AISP) under PSD2. These entities, will be able to access customer data subject to authorization issued by the competent Authority of their home Member State. Entities established in third countries may also be authorised to operate as FISPs without establishing a company or branch within the Union territory, provided they appoint a legal representative in one of the Member States from which the FISP intends to access financial data, who will be responsible for *compliance* with the European regulatory framework.

The FIDA Regulation identifies two types of actors: *data holders* and *data users*. Both will be required at the customer's request, to share information through dedicated interfaces (APIs) created in accordance with widely used market standards. The scope of application therefore includes entities acting as *data holders* - any intermediary that collects, stores, or otherwise processes customer financial data – and *data users* - any intermediary or FISP that, based on customer consent, has legitimate access to the latter's financial data.

Data holders must make customer financial data available to the customer themselves and to the *data user*. They are required to: make financial data available without delay, on a continuous basis, and in real-time; use a format based on generally recognized standard models and with quality not inferior to that characterizing the data possessed by the data holder; communicate with the data user ensuring the security and confidentiality of data processing and transmission; request proof of the customer's consent given to the data user; and make a *permission dashboard* available to the customer. They may request payment of compensation for data sharing within the maximum limits identified by so-called Financial Data Sharing Schemes (FDSSs). Compensation cannot be requested if data is made available directly at the customer›s request; furthermore, in case of an access request by SMEs, compensation cannot exceed the costs incurred by the data holder to respond to the request itself.

Data holders must make available to the customer the so-called *permission dashboard*, a specific IT interface used to monitor and manage consents given by the customer to the data user. With the *permission dashboard*, the customer can be provided with an overview of each active consent given to data users and allowed to revoke or re-activate consent, as well as provided with a record of consents revoked or expired within a maximum period of two years.

Data users, on their part, are required: not to process customer data for purposes other than those pertaining to the provision of the service expressly requested by the customer; to respect the confidentiality of trade secrets and intellectual property rights when accessing data; to adopt necessary measures to ensure an adequate level of security regarding the storage, processing, and transmission of non-personal data; and not to process customer data for mere *marketing* purposes.

5. Data management challenges

Data sharing under the proposed framework is expected to occur through Financial Data Sharing Schemes (FDSS). These are self-regulatory bodies composed of data holders, data users, and organisations representing clients and consumers. They are tasked with managing various operational aspects of the legislation, including the definition of technical standards, participant identification procedures, and remuneration models. Each data holder and data user is required to join at least one FDSS and to share customer data in accordance with the rules and procedures established by the scheme. Where no FDSS exists for certain categories of data, the European Commission may adopt delegated acts to regulate the relevant aspects of data sharing.

Data users will also be able to access customer financial data across borders under the freedom to provide services or establish a presence in other Member States. For Financial Information Service Providers (FISPs), cross-border access will require a notification procedure between competent authorities, similar to the passporting mechanisms used in other sectors of the European financial system.

The European Banking Authority (EBA) will maintain a central electronic register containing information on authorised FISPs, FISPs that have notified their intention to access data in other Member States, and established FDSSs.

The Financial Data Access (FIDA) proposal is part of the European Union's broader strategy to create a more integrated, secure, and innovative digital financial ecosystem. It complements initiatives such as the Data Act and the Digital Operational Resilience Act (DORA) and aims to build on the experience of Open Banking by opening the market to innovative operators, enabling the aggregation of information across customers' full range of financial assets, and supporting the provision of value-added advisory services.

It aims to extend the principles of Open Banking established under PSD2 to a wider range of financial data, enabling authorised third-party providers to access not only payment account information but also data related to loans, investments, insurance, pensions, and other financial products. The regulation is designed to allow consumers and businesses to benefit from more personalised financial services, increased transparency, and improved advisory tools, while ensuring that access to data occurs only with the explicit consent of the user.

FIDA establishes a framework for both data holders, such as banks and financial intermediaries, and data users, including financial information service providers, to interact through standardised APIs under defined security, confidentiality, and operational requirements. It also introduces self-regulatory mechanisms through Financial Data Sharing Schemes, which set guidelines on technical standards, remuneration, and operational processes, helping to coordinate the growing complexity of data exchange in a multi-actor environment. The regulation further contemplates cross-border access, allowing authorised providers to operate across the EU under a notification or 'passport' system, facilitating the development of a more integrated European financial market.

The importance of FIDA for payment services lies in its potential to transform the sector by enabling broader data-driven innovation. Payment service providers can develop new value-added services, improve risk management, and enhance fraud detection capabilities by accessing a more comprehensive view of their customers' financial profiles. At the same time, the regulation seeks to maintain trust and security, balancing innovation with the protection of sensitive financial data. By standardising access, clarifying liability, and supporting interoperability, FIDA could strengthen competition, expand the market for fintech operators, and improve the efficiency and quality of payment and financial services across the EU.

Access to financial data, however, introduces greater complexity and sensitivity than access to payment account data. Unlike payment transaction data, financial information may reveal strategically significant details about intermediaries' products, services, and proprietary know-how, particularly in areas such as investment management, collective asset management, and insurance services.

The proposal raises questions about how to balance innovation with the protection of intermediaries' confidential information. It also intersects with broader legal concerns, including consumer protection, cyber resilience, coordination among regulatory authorities, enforcement of uniform rules, supervision of market participants, and the design of effective administrative sanctioning mechanisms.

FDSSs are expected to play a central role in shaping the Open Finance ecosystem, delegating key design tasks to market participants and emphasizing collaboration as essential for effective data exchange. However, entrusting technical rule-making to multiple entities may create challenges, including increased compliance costs, the adoption of divergent standards, and potential distortions or regulatory arbitrage.

The proposal presents both opportunities and uncertainties. It constitutes a significant innovation for market operators, particularly in a sector where the combination of rich financial data and advances in artificial intelligence could substantially enhance service quality. At the same time, several aspects still require clarification, including operator identification, customer authentication, and remuneration frameworks. These issues will need to be carefully addressed before the formal adoption of the regulation.

6. Issues and perspectives

The digitisation of the financial sector has brought significant benefits, enabling the development and delivery of innovative services that are increasingly accessible and offered at lower costs. At the same time, it has introduced new challenges related to data management and increased the overall vulnerability of the system, making it an attractive target for cybercrime.

Technological innovation remains a central pillar of the transition toward more open financial models, yet it also presents substantial risks, particularly regarding the security of shared data. The financial sector is inherently exposed to cyber threats, which are evolving through increasingly sophisticated tools and methods.

While digitisation has driven the development and delivery of innovative , cost-effective services, it has also increased its vulnerability. To remain competitive, banks must therefore strike the right balance between innovation and security, a prerequisite for offering new services.

The market has responded with a range of solutions. Preventive verification tools allow customers to confirm beneficiary account details before initiating payments. Legal entity identifiers, such as the LEI (Legal Entity Identifier) code, enable precise, instant, and automated cross-border identification of payers and payees. Artificial Intelligence (AI) and Machine Learning (ML) techniques help detect fraudulent activities in high-volume transaction environments. Blockchain technology, in turn, enhances the security of information sharing across transaction participants compared to traditional methods.

One key challenge is the fragmentation of regulations across different countries, highlighting the need for greater harmonization. This harmonization should adopt an approach that considers market trends and leverages proprietary tools already developed and successfully tested at the corporate level.

As previously mentioned, In June 2023, the European Commission presented legislative proposals of considerable importance for the digital payments market, which include the third Payment Services Directive (PSD3), the Payment Services Regulation (PSR), the framework for financial data access (FIDA), and a package dedicated to the Digital Euro.

The new regulatory framework prioritizes the protection of competition - a cornerstone of European Law since the signing of the first Treaties - while also safeguarding consumer security and trust. The *Payment Service Regulation*, together with the *Payment Service Directive 3* ***and the*** *Financial*

Data Access Regulation, aims to enhance the payment experience for consumers and businesses, while ensuring data protection and transaction security.

The recently approved Instant Payments Regulation updates and modernizes the 2012 Single Euro Payments Area (SEPA) regulation, to improve the availability of instant payment options in euros. It enables money transfers within ten seconds for consumers and businesses in the EU and EEA countries.

The PSD3 Directive aims to strengthen the regulation of payment institutions in the European Union operating as supervised Payment Service Providers. It introduces new regulations regarding cash withdrawal services, requires the inclusion of a liquidation plan in the authorization application process, and expands mechanisms for safeguarding funds. Furthermore, it seeks to enhance transparency and efficiency in the payments sector by maintaining up-to-date registers of authorised institutions and establishing a framework for cross-border cooperation.

Both the *Payment Service Regulation* and the regulatory proposal on Instant Payments provide for the obligation by payment service providers to implement pre-validation mechanisms to verify the correct association betweena beneficiary's name and the corresponding IBAN These tools are already present and operational in the market.

In the national context, services such as Name Check and Check IBAN represent important anti-fraud instruments. They align with specific objectives of the UN *Sustainable Development Goals*, as they contribute to cost reduction, improved efficiency, lower environmental impact of financial services, and foster innovation through a collaborative ecosystem among market players[1].

In recognition of the importance of verifying beneficiaries to com-

1 Law no. 132 of September 23, 2025, *Provisions and delegations to the Government regarding artificial intelligence.*

bat fraud, CBI introduced the Check IBAN service in Italy in 2020. This solution enables verification of the correct association between an IBAN code and the corresponding tax code/or VAT number of a payment beneficiary. Initially designed to support, the Public Administration, it was subsequently extended to corporate users, including in its cross-border declination. This service has demonstrated remarkable growth, with annual increases exceeding 120% .

Furthermore, the Name Check service allows for real-time verification of the correspondence between a payment beneficiary's name and the associated IBAN, helping both Corporate and Retail users avoid accidental payments to incorrect account holders and providing an additional layer of protection against fraud and scams.

To extend the Name Check service at the European level and beyond, CBI has activated dialogues with international partners, notably establishing a collaboration with Swift for the use of its *Pre-Validation Account* functionality. This collaboration will allow both operators to expand their respective markets, creating a broader verification network and delivering a higher level of security for financial service users. In particular, Italian banks will be able to perform checks abroad through CBI, implementing a unique solution at both national and cross-border levels.

Significant development opportunities foster collaboration and innovation, allowing third-party developers, fintech start-ups, and other operators to create new financial products and services using shared financial data. This opens new possibilities for innovative offerings aimed at improving the commercial proposition of financial institutions and addressing previously unmet customer needs. However, this also intensifies competition: a more competitive landscape at the European level with new operators, third parties, competing with traditional financial institutions. It is important to note that while this benefits customers, it also exerts pressure on operators' margins.

On the other hand, financial institutions can choose to collaborate with fintech and other technology companies to build integrated ecosystems capable of offering new or more interconnected financial services, potentially impacting revenue streams.

Nevertheless, data security and privacy remain critical concerns, at risk of being overwhelmed by the ongoing technological and cultural shift toward "open data sharing". Intermediaries and operators involved must provide strong assurances to maintain customer trust and prevent violations, ensuring robust cybersecurity and Data Protection measures.

The challenge of balancing innovation, competition, and security is ambitious, particularly from a European perspective, and represents a crucial test for the financial sector in the digital age.

References

[1] Arner, Douglas W.; Buckley, Ross P.; Zetzsche, Dirk A., *Open Banking, Open Data, and Open Finance: Lessons from the European Union*, in *Open Banking* (edited volume), Oxford University Press, March 2022.

[2] Arnal, J.; Andersson, F., *FiDA: Is the EU Prepared to Move from Open Banking to Open Finance?*, *European Credit Research Institute (ECRI) Commentaries*, 2024.

[3] CBI – PwC, *The Global Open Finance Report*, 2023.

[4] Colangelo, G., *Open Banking goes to Washington: Lessons from the EU on regulatory-driven data sharing regimes*, *Computer Law & Security Review*, 2024.

[5] Colangelo, G.; Khandelwal, P., *The many shades of open banking: A comparative analysis of rationales and models*, *Internet Policy Review*, 2025.

[6] EU – European Commission, *Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending regulations (EU)*, 2023.

[7] Grassi, L.; Figini, N.; Fedeli, L., *How does a data strategy enable customer value? The case of FinTechs and traditional banks under the open finance framework*, *Financial Innovation* (Springer), 2022.

[8] Maimeri, F.; Mancini, M., *Open Banking and Open Finance in the European Union*, introduzione a una raccolta di saggi di esperti della Banca d'Italia e del mondo accademico, 2019.

[9] Pellitteri, R.; Parrini, R.; Cafarotti, C.; De Vendictis, B.A., *Mercati, infrastrutture, sistemi di pagamento*, Banca d'Italia, 2023.

[10] Preziuso, M.; Koefer, F.; Ehrenhard, M., *Open banking and inclusive finance in the European Union: perspectives from the Dutch stakeholder ecosystem*, *Financial Innovation* (Springer), 2023.

[11] Raganelli, B.; Fratini Passi, L., *Open Finance e innovazione finanziaria: opportunità, questioni e sfide*, in *Dall'Open Banking all'Open Finance. Profili di diritto dell'economia*, Giappichelli, 2024.