STUDY

Requested by the ECON Committee

European Parliament

Open Finance

What can an enabling framework look like?

Policy Department for Economic, Scientific and Quality of Life Policies
Directorate-General for Internal Policies
Authors: Alexander LEHMANN and J. Scott MARCUS

PE 754.188 – October 2023

EN

Open Finance

What can an enabling framework look like?

Abstract

This study assesses the potential benefits, costs and risks of data sharing in the EU financial sector and implications for consumers, enterprises and the financial sector itself. We examine the coherence of a proposed regulation on financial data access with the broader EU data legislation and recommend a number of changes and modifications.

This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies at the request of the Committee on Economic and Monetary Affairs (ECON).

This document was requested by the European Parliament's committee on Economic and Monetary Affairs.

AUTHORS
Alexander LEHMANN
J. Scott MARCUS

ADMINISTRATOR RESPONSIBLE
Christian SCHEINERT

EDITORIAL ASSISTANT
Marleen LEMMENS

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for email alert updates, please write to:
Policy Department for Economic, Scientific and Quality of Life Policies
European Parliament
L-2929 - Luxembourg
Email: Poldep-Economy-Science@ep.europa.eu

Manuscript completed: October 2023
Date of publication: October 2023
© European Union, 2023

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT
The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.
Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.
For citation purposes, the publication should be referenced as: Lehmann, A. and J.S. Marcus, 2023, *Open Finance - What can an enabling framework look like?*, Publication for the Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, European Parliament, Luxembourg.
© Cover image used under licence from Adobe Stock.

CONTENTS

LIST OF BOXES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AFME	Association of European Financial Markets
AI	Artificial intelligence
AISP	Account information service provider
API	Applications processing interface
APIX	API Exchange (in Singapore)
APP	Authorized push payment
CBDC	Central bank digital currency
CDR	Consumer Data Right
CJEU	Court of Justice of the European Union
CMU	Capital Markets Union
DMA	Digital Markets Act
DORA	Digital operational resilience act
DSA	Digital Services Act
EBA	European Banking Authority
ECB	European Central Bank
EDPB	European Data Protection Board
EEA	European Economic Area
eIDAS	Electronic identification and trust services
EIOPA	European Insurance and Occupational Pensions Authority
ENSISA	European Union Agency for Cybersecurity
EP	European Parliament
ESAP	European Single Accesss Point
ESG	Environmental, social and governance

ESMA	European Securities and Markets Authority
EU	European Union
FCA	Financial Conduct Authority
FCA	Financial Conduct Authority
FIDA	Financial Data Access
FISP	Financial information service provider
GDP	Gross domestic product
GDPR	General Data Protection Regulation
IBAN	International bank account number
ICT	Information and communication technology
IT	Information technology
MiFID	Markets in financial instruments Directive
MIT	Merchant-initiated transaction
MOTO	Mail order or telephone order
MSME	Micro, small and medium-sized enterprises
NCA	National competent authority
OECD	Organisation for Economic Cooperation and Development
PISPs	Payment Initiation Service Provider
PSD	Payment Services Directive
PSR	Payment Services Regulation
SCA	Strong Customer Authentication
SME	Small and medium-sized enterprise
TCA	Trade and Cooperation Agreement (UK-EU).
TPP	Third Party Provider

UK	United Kingdom
US	United States

EXECUTIVE SUMMARY

Background

The digital economy could be a key growth driver in Europe. In the financial sector, digital technologies, new actors and their innovative business models, and changing consumer behaviour have already accelerated structural change. In the process, finance is becoming more decentralised and numerous non-bank forms of credit have emerged. This could raise consumer welfare as innovative and more customized financial products are offered and competition intensifies.

Access to data and a sound regulatory framework for data sharing will be key in this process. The EU now endeavours to progress from its model of *Open Banking*, which mandated data sharing in the payments system, to *Open Finance,* which is to apply to a wider set of financial sector actors and data types. The overarching objectives are to increase competition in the offering of a wide range of financial services, to provide greater consumer choice, and to facilitate market entry of new and innovative financial service providers.

A key instrument in doing so is the *Financial Data Access Regulation,* which was proposed by the EU Commission in June 2023. This regulation, also known as *FIDA,* represents an important step in financial liberalisation and could be an impetus to digital finance in Europe. In principle this is a sensible step in the ongoing programme of rulemaking aimed at making the EU financial sector more innovative and integrated, while strengthening competition. At the same time, the regulation poses a number of questions on data privacy and data governance, financial stability and the associated financial market supervision, which we address in this study.

We do this by assessing FIDA in the context of the overall EU legal *acquis*. The regulation was intended to work in concert with a broad range of existing EU *laws and regulations*, including the GDPR, DORA, and the proposed revised legislation for the payments system.

Crucially, the shift from Open Banking to Open Finance will be informed by the experience, both good and bad, with the existing Payment Services Directive 2 (PSD2), which enabled entry of third-party providers into the payments system and their access to data. This has, however, had mixed success. The take-up of services that depend on PSD2 has been far less than hoped for, and uptake of digital financial services varies widely among EU Member States. The lack of consistent standards and *application programming interfaces (APIs)* has been a major impediment to the effectiveness of PSD2 to date.

Financial regulation now also needs to address new questions around the dominance of certain digital service providers, data privacy, operational resilience and cybersecurity.

Aim

Concretely, a robust Open Finance system for the EU must provide for (1) obligations on a wide range of incumbent data holder financial institutions to provide data and in some cases interoperability with an even wider range of incumbent and new data user service providers; (2) standards that make interoperability and portability efficient, secure, respectful of consumer privacy, and cost-effective, including for cross-border operation; and (3) a compensation model that provides the right incentives to all parties.

Implications for social welfare

Consumers are likely to benefit from the future EU open finance regime due to greater financial access, lower search costs, and product differentiation. However, these gains may be limited due to inadequate digital access and also due to consumer behavioural biases, which are evident for instance in limited switching between products or the persistent choice of a single provider.

In EU countries with poor financial literacy, there is a risk of mis-selling of financial services by data users to poorly informed consumers. In these countries, the effectiveness of permission dashboards, which are envisaged as a key tool for consumers wishing to exercise control over data use, would be quite limited. By contrast, we anticipate that financial exclusion and discrimination against certain consumers would not be significant problems in the early phases of Open Finance.

As regards non-personal corporate data, only firms' creditworthiness indicators have been included in the proposed FIDA regulation. The open finance regime could result in more suitable products and a greater variety of products being offered by outside providers in the future, including, for instance, more suitable risk sharing features for SMEs.

The future Open Finance framework will only indirectly benefit the *Capital Markets Union (CMU)* project to the extent retail investors are better informed about their financial position or where data facilitate the communication by brokers. Such data may also relate to the sustainability preferences of retail investors, which at present need to be assessed through a relatively costly process of questionnaires and client interaction.

Overall, data sharing under FIDA will accelerate structural change in the EU financial sector through the adoption of digital technologies and business models. This will lead to further gains in the market share of non-bank lenders at the expense of established banks, whose margins may shrink as IT investment weighs on profitability. Within the banking sector larger banks with sufficient investment in digital technology may gain and also act as data users, while banks that are smaller or have not sufficiently invested in IT may be more at risk. This will present additional challenges in both macro-prudential (systemic) and institution-specific supervision.

Implications for digital infrastructure

The Commission has been promoting the use of cross-border use of identity and authentication services since 2014 and sought to use an enhanced version of its electronic identification standard (eIDAS) as part of the strong customer authentication (SCA). Financial service providers have made substantial investments in alternative systems, so it is unlikely that eIDAS-based SCA will have a major impact on Open Banking.

The concentrated market for cloud services has raised numerous concerns. Most EU firms use services from just three service providers, all of which are based in the United States. The concerns over limited interoperability among these cloud service providers, and high switching costs, are potentially mitigated by the proposed (and politically agreed) Data Act. Whether the lack of a first-tier EU-based cloud service provider poses a problem for online financial services in the long term remains to be seen.

SCA has been a major success for PSD2 and has reduced fraud significantly. However, there are known gaps. The proposed PSR seeks to oblige a broader range of financial services providers to implement SCA, and to reduce fraud that is perpetrated by means of "social engineering".

Finally, the lack of skilled experts in financial services ICT will pose challenges in implementing FIDA, including in public supervisory functions.

International aspects and interoperability

Most OECD countries promote the expansion of data sharing provisions in payments and banking. Only a few countries cover non-financial data, such as utilities.

- The UK stands out for having a dedicated supervisory structure, and for seeking to promote SME credit through data sharing.
- Australia has consistently promoted the benefits of consumer data sharing and has made consumer data rights more transparent. Dedicated programmes and fiscal spending underpin the digital agenda, with a dedicated website setting out benefits to consumers.
- Experience in Singapore underlines the benefits of an organic, market-driven approach to open banking, and also wide-ranging inclusion of consumers' financial and government data in consolidated accounts.

There are useful lessons to be learned from these and other jurisdictions. Yet, EU interoperability or portability of data formats, exchange protocols and access rights for such third countries is not a realistic ambition, in light of diverging privacy and data rights standards. The UK with its very innovative digital finance sector should however become a closer partner.

Key recommendations

Our overall assessment is that the proposed FIDA and revised payment services legislation, together with the pre-existing *acquis* such as GDPR or DORA, will define a reliable *Open Finance* framework within the EU. The Commission has done a competent job of analysing both the strengths and the weaknesses of the existing Open Banking framework implemented by PSD2 and has crafted sensible measures to expand it.

There are three key areas that warrant further elaboration over the course of the FIDA trilogue.

Firstly, we see a need to strengthen the resources and possibly the mandates of EU-level supervisors (EBA, EIOPA and ESMA) to reflect the expansion of the regulatory perimeter and the new demands of Open Finance.

Secondly, the regulation relies to a significant extent on financial data sharing schemes as an ambitious and somewhat novel industry-led initiative. The private sector is tasked to fix what is in essence an inherent market failure preventing wider data sharing. We see important strengths in the proposal; however, a major concern is the lack of clarity when data holders and data users do not agree on which standards and which maximum compensation should govern.

Finally, some inevitable divisions within the single market will need to be bridged. We also see a significant risk as regards data transfers to non-EU/EEA countries, for instance if an adverse court ruling were to strike down a GDPR adequacy decision applying to major trading partners such as the UK or the US. This is a GDPR issue – the firms cannot fix this, nor can FIDA.

FIDA would represent an important boost to the Union's digital economy. In the longer term, it will be necessary to fully integrate data sharing in the payments system (PSR and PSD3) with FIDA, capitalising on the scale and scope of data sharing.

Many additional detailed recommendations are listed in Chapter 9 of the report.

1. INTRODUCTION

1.1. Background and motivation

The European economy is increasingly shifting towards data-driven business models based on the generation, sharing and processing of data. Consumers are rapidly gaining near universal access to digital infrastructure, and innovations in cloud computing or artificial intelligence have accelerated the trend towards the digital economy. Finance, with its pervasive links to all sectors of the economy and to most consumers, has been part of this trend for some time. The sector can be a source of data that spurs innovation elsewhere but will itself depend on robust data sharing arrangements between different types of financial firms.

The potential of digital finance has already been partially realised in the payments system. The EU's Payment Services Directive (PSD) has defined an innovative framework of licencing new providers and data access rights. As consumer lending products, retail investment, occupational pensions, insurance and SME finance are also going digital, new products and providers will depend on data about customers and their past financial services use. *Open finance* describes an environment in which such providers gain access to a customer's data, with prior consent, to design, offer and monitor alternative financial products. It extends *Open Banking* and the associated payments data sharing regime but falls short of an *open data* regime in which non-financial sectors would share and in turn draw on financial data.

The European Union has been at the forefront in defining comprehensive legislation for the data economy and digital finance. Rulemaking has been framed by a number of strategies and, most notably, produced legislation on consumers' privacy rights (GDPR), on the obligations of technology firms, and on cybersecurity and digital operational resilience (see Chapter 5 and Section 6.4). The Payments Services Directive (PSD2) of 2015 already defined the rights of data access in the EU payments market, and thus ensured the rights of consumers.

The benefits of Open Finance will stem from a number of factors: greater access by consumers and SMEs to financial products which are more suitable; cost efficiencies within financial services firms, crucially in monitoring clients; and more streamlined interactions with regulators. A number of countries outside the EU, such as Australia, demonstrate how finance can better support consumers and SMEs in such an environment. But there are important policy trade-offs: data users may discriminate against certain types of consumers, or possibly exclude them from certain products. This might aggravate some of the traditional behavioural biases or might manipulate consumer choice. The use and processing of data is also subject to economies of scale which can inhibit competition as dominant market positions become entrenched.

The Union's digital finance legislation is as yet incomplete. It will need to be designed, and continually adapted, in the light of evolving technology and business models, and it should facilitate greater international openness. Key pieces of the EU digital legislation were drafted without the specific requirements of finance in mind, and financial data legislation will in turn need to reflect the broader European data policy and privacy rights established in other recent legislation.

In the transition to digital business models, the EU financial sector will have to overcome a number of rigidities and barriers within the single market. Banks have traditionally been the main holders of data. While some banks struggle with outdated technology and a lack of skilled engineers, others have rapidly moved into digital business models, including through data sharing arrangements with outside fintech providers. National discretion in implementing data sharing arrangements presents barriers to cross-border financial firms, as has long been evident in the challenges facing implementation of the

capital markets union. New financial service providers are emerging not only in the fintech field, but also in the form of online platforms, technology companies and other disintermediated payment providers. These market entrants are as yet not fully within the purview of regulation and of the supervisory authorities.

A wider data sharing in the financial sector is held back by a lack of trust on the part of consumers, and by disincentives for consumers to consent to data access. Other barriers to data sharing might seem to be merely technical, such as incompatible data formats and access protocols. These barriers reflect deeper incentive problems as individual data holders cannot capture the wider benefit to consumer welfare of the data they control and no model for compensation of data use has emerged. As in other areas of the data economy, strong network externalities, first mover advantages, and persistence of consumer behaviour reduce market contestability.

The EU Commission tabled its proposal for a regulation on financial data access in June 2023 ('FIDA' in European Commission, 2023a).[1] On the basis of this proposal, the scope of data designated for mandatory sharing arrangements, and of financial services actors eligible to request or share such data, is significantly expanded. The EU's financial data economy would now comprise retail credit, insurance, retail investment and SME finance, among others (we largely use the terminology and definitions from that regulation, and list the key terms in Box 1).

At the same time, the Commission proposed a revision to legislation governing the payments system in the form of a revised directive and a new regulation (the PSR). This sector remains subject to a distinct regime, even though the Commission acknowledges that the integration of Open Banking and the remainder of Open Finance would be desirable.

FIDA could be a 'big bang' moment of liberalisation for digital finance in Europe, but the regulation now needs to undergo careful scrutiny. Product innovation and the market entry of new providers could meet tangible needs of consumers and SMEs. Gaps in access to finance and barriers in the single market for financial services may disappear over time. Equally, the regulation will raise the bar for established financial services firms acting as data holders and having to adopt consistent protocols and format for data sharing. Regulators will have to tackle the likely effects on stability and competition in the financial system, and to safeguard consumer privacy and data rights.

1.2. Objectives of this study

This study has the two broad objectives: firstly, to assess the gains and risks from applying the principles of data sharing to a wider set of financial sector actors and data; and, secondly, to study how the existing EU data governance framework and principles of the PSD2 can be applied to those actors.

We will examine open finance in terms of both economic costs and benefits, and also in terms of legislative implications and coherence with the broader EU data governance. In doing so, we will comment on and assess the EU Commission's open finance proposal, assessing the economic rationale for its present design and certain gaps in its provisions. However, the study is not designed as a commentary on a specific piece of legislation, but rather seeks to sketch out a desirable framework for open finance, bearing in mind the above trade-offs.

1 COM(2023) 360 final.

1.3. Outline

The next two Sections provide context in an effort to judge the significance of the financial data economy. In Section 2 we review how digital technology has reshaped the EU financial system, and the implications for the further widening of the perimeter of EU financial regulation. In Section 3, we study the role of data and of a potential framework for data access and sharing in delivering the potential gains from digital finance. We identify underlying economic disincentives, rather than technical issues, as the root cause of inadequate data sharing.

Section 4 then studies in detail the potential economic benefits that could result from open finance for consumers and MSMEs, and potential costs and risks in realising these gains. This section also studies the implications of an open finance regime for the structure of the EU financial market, including the EU Capital Markets Union, sustainable finance, and some financial stability considerations.

The following two sections then study the implications of FIDA for data governance in the EU. Section 5 examines the policy considerations in designing a robust legislative and regulatory framework for open finance that accommodates personal privacy. We show that FIDA and PSR are essentially consistent with Europe's key data privacy act, the GDPR. Nevertheless, there is a risk of disruptions to data sharing arrangements with users in third countries. Section 6 then studies technical aspects surrounding data infrastructure and IT resources that will arise with the implementation of the open finance regime. The expansion of the types of data designated for exchange, and of the type of data users and data holders engaged in it, will vastly expand the demands on the industry. The need to define sufficiently usable data exchange formats (in the form of the so-called application processing interfaces, or APIs) could in principle be handled within the proposed data sharing schemes, which are to be run as collective arrangements by the industry. Yet, the need for skilled IT staff and cloud services will weigh on the industry's resources.

Finally, Section 7 looks at experience with open finance in jurisdictions outside the EU, including in Australia, Singapore and the UK. While many lessons can be learned, often privacy rights and financial sector structure are very different from those in the EU. Finally, Section 8 concludes, identifying gaps in the existing framework and in the proposed regulation, and sketching out how open finance legislation could be more coherent, including across sectors.

Box 1: Definitions and terminology

In this study, we assess the general requirements for open finance, the as yet unregulated environment of access to and use of customer data in finance, and whenever appropriate refer to the specific EU legislative proposal as the FIDA Regulation (or also as 'Open Finance'). We generally refer to 'Open Banking' as the body of EU legislation, namely the framework established under the revised Payment Services Directive (PSD2) mandating financial institutions to share, at the request of a customer, payment account data with licensed Third Party Providers of payment-related services (EU Commission, 2023).

FIDA will regulate a complex web of data sharing between multiple types of financial actors and alongside the GDPR will address the privacy and data rights of consumers and enterprises. Debating the regulation will need to rely on consistent terminology. The regulation defines new terms in addition to those in the PSD, and some are slightly different from earlier reports, such as that by the Expert Group on the EU financial data space (EU Commission, 2022b). Without prejudice to FIDA, we reproduce below the key terms that will be used throughout our study. In addition, we refer the reader to Art. 3 of the regulation for a full list of definitions.

The key actors in financial data sharing will be:

- Customers. Individual or enterprise who uses financial products and services.
- Consumers. Individual who is acting on his or her personal finances (as opposed to business).
- SMEs. Small and medium-sized enterprise, as defined in EU regulations by size and turnover.
- Data users. Entities seeking and obtaining access to customer data under the regulation. This includes, though is not limited to, entities currently subsumed as so-called third party providers, which are actors in the payment system empowered by the PSD. Financial information service provider (FISP) are data users which have been authorised under the regulation to access customer data.
- Data holders. A financial institution that collects, stores and processes data. Often, though not necessarily, an established financial institution, such as a bank, insurance firm or investment firm. Account information service providers under the PSD2 are specifically excluded.

FIDA defines in Art. 2 an exhaustive list of entities that can act as data holders or users under the regulation, most notably of course banks, insurance and investment firms, though also a range of fintech firms.

Source: Authors' own elaborations.

2. TECHNOLOGY AND THE NEW CHALLENGES FOR FINANCIAL REGULATION

KEY FINDINGS

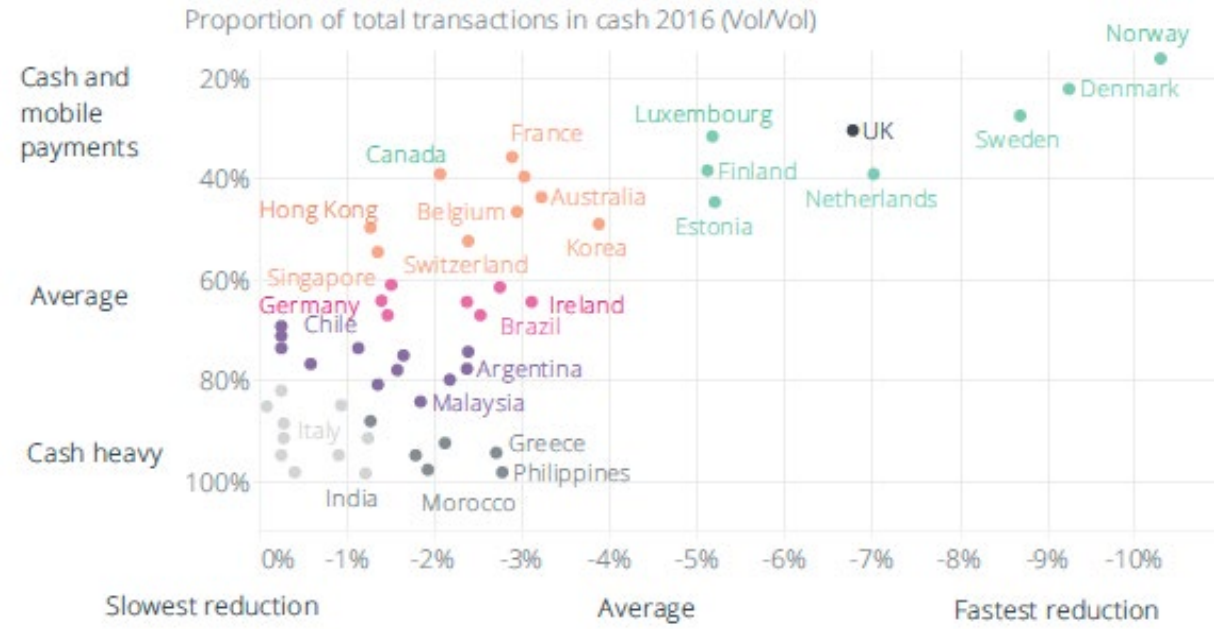
- Digital technologies, the related financial sector business models and changing consumer behaviour have accelerated structural change in the EU financial sector and have led to a decentralisation of finance.
- The adoption of digital finance technologies and business models raises consumer welfare, given greater product variety and efficiency of new financial service providers.
- Given the emergence of digital finance technologies, financial regulation now needs to address new questions around the dominance of certain digital service providers, data privacy, operational resilience and cybersecurity.
- The perimeter of EU financial regulation has already been broadened to encompass third party providers in the payments system. PSD2 also defined a regulatory framework for the sharing of payments-related data.
- Uptake of digital financial services has nevertheless been more limited than expected, and varies greatly among EU Member States.
- One key lesson of PSD2 has been that incentives for developing application process interfaces (APIs) need to be well-defined.

2.1. Digital innovation and business models in finance

Over recent years, a number of new technologies and business models have emerged which are rapidly reshaping the EU financial sector:

- Electronic payments have steadily displaced cash in everyday purchases, as online commerce and the mobile phone became widely accessible. The 27 EU economies show widely different shares of mobile payment use. Some countries have reduced the rate of cash use rapidly coming from an already high level of electronic payment penetration, while others hold on to the continuing use of cash (Figure 1). This variation in the adoption of digital finance across EU Member States is likely to persist, given the still different policies and digital infrastructure, but also given differences in consumer preferences and behaviour.

Figure 1: Shares of cash and mobile payments



Source: Bank of England (2019a) Future of Finance Report.

- In several EU countries, banks have also set up account-to-account payment systems, such as iDeal in Sweden[2], obviating the need for intermediaries, such as credit or debit card companies. This technology offers greater choice and convenience to consumers and reduces transaction costs. Payment data therefore accumulate outside the established financial payment providers and could serve in designing and promoting new products, or in monitoring existing clients.
- Large technology companies, such as Alipay in China or Apple and its Apple Pay service, are increasingly entering financial services. These firms utilise data generated by existing e-commerce and social media activities to offer financial services which are easily accessible and customised. Activities of these firms have been mainly in payment services so far but are also beginning to cover insurance and wealth management. Network economies of scale favour the accumulation of customer data which could lead to dominant market positions.[3] The different data access options available to big tech firms (which are subject to GDPR) and banks (which are also required to share data under PSD2) has created certain asymmetries and concerns over a 'level playing field'.
- Cloud computing enables financial firms to store and process data at much lower costs than would be the case with in-house data centres. Third-party providers often host financial businesses, offering data applications and analytics. This is already utilised by banks and other established financial firms and reduces entry barriers for new and smaller service providers. While cloud services raise efficiency, there are also concerns over cybersecurity and market concentration within three dominant providers, all of which are headquartered in the US.

[2] Bank of England (2019a).
[3] Carstens et al. (2021).

- Finally, central bank digital currencies (CBDCs) are set to transform digital finance. In the view of the ECB, the dominance of a few large non-EU firms in online payments puts customers' data privacy at risk and threatens the EU's strategic autonomy. The case for CBDCs is still debated, but there could be important benefits in cross-border payments.[4]

All of the above technological trends have brought new actors into the EU's financial sector. Fintechs, which deliver financial services primarily on the back of utilising and analysing large data, and technology firms will increasingly challenge established incumbents in core financial activities, such as lending and payments. Consumer welfare may be raised due to greater product variety and lower cost services. Data sharing rights will be central in ensuring a 'level playing field'.

2.2. The shifting perimeter of EU financial regulation

The financial system performs essential functions in the EU economy, such as the allocation of capital, the identification of valuable investment projects and related support to entrepreneurs, and the management of risks to which households and enterprises are exposed. Regulators are in essence focused on the stability and the efficient performance of specific financial activities, such as bank lending, deposit taking, insurance or bond and equity issuance or central clearing etc. These activities have traditionally been combined within and performed by certain types of financial sector firms, for instance banks and their funding and lending activities. These entities with their legal identity and financial accounts can be constrained and are normally the object of regulation and financial supervision.[5]

The financial sector, and some of the digital technologies which we highlighted above remains highly fluid, and technology has already led to a separation of activities across different types of entities. Innovations, such as machine learning, the processing of 'big data', and artificial intelligence (AI) have accelerated this trend further. Financial activities are shaped by the evolving technology and are performed by different entities. Consumer behaviour, new types of financial projects, and the digital sharing of and access to financial data have accelerated this trend. The brokerage sector, for instance, has undergone rapid changes as the internet has made a wider range of financial instruments and portfolio investment tools accessible to an increasingly engaged investor class.

Given the evolving technology, the task of regulators, which is to ensure the stability of the system and its continued support to the growth of the EU economy, is becoming more complex. They will increasingly need to go beyond their purview of entities that are traditionally seen to be within the financial sector, and address financial activities performed in other sectors in order to ensure a certain 'level playing field'. For instance, online retailers now regularly extend credit to consumers, and suppliers in the industrial sector extend trade credit, in each case performing a role that is akin to that of corporate lending by a bank. A key question for regulators is to what extent similar activities outside the financial sector can be subject to the same regulation that is applied to financial firms, and how the perimeter of regulation will be widened to ensure a level playing field. Entities that have to date been considered to lie outside the financial sector will also require rights and privileges that were so far available only to financial services firms and will need to be subject to certain safeguards. One such right is that of access to data.

4 Demertzis and Martins (2023).

5 Borio et al. (2022).

2.3. The lessons from the payments system

One specific objective for regulators has been that the payment system remains safe, universally accessible and cost-efficient as digital technologies and new providers proliferate. The payment system is prone to market failures, given the strong network externalities, and given the behaviour of consumers who may not easily switch payment providers.

Banks traditionally utilise economies of scope between their deposit taking activities and the provision of payment services. Third-party providers, such as fintechs, now offer more accessible and more tailored services and challenge banks as the established payment providers, although they depend on data access to do so.

A regulatory framework that governs access to and sharing of customer payments data was largely delivered by payments services directive (PSD2). The revised directive has been applied in Member States since January 2018, and has transformed the European payments landscape. Broadly speaking, there were five main aims:

- To create an environment which helps innovative payment services to reach a broader market;
- To further level the playing field for payment service providers by including new players;
- To increase the efficiency, transparency and choice of payment instruments for payment service users;
- To enhance protection for European consumers and businesses;
- To facilitate the provision of card, internet and mobile payment services across-borders within the EU by ensuring a single market for payments.[6]

To this end, PSD2 defined obligations for data sharing together with rights of data access for data holders and data users, governed by the rights of customers. PSD2 imposed an obligation on banks and other data holders to facilitate access to payments data for Account Information Service Providers (AISPs), which essentially act as data intermediaries and analysts, and for Payment Initiation Service Providers (PISPs), which help consumers make online credit transfers and inform the merchant immediately of the payment initiation. Crucially, banks were required to share payment data for free at the request of a customer.

Data users have 'read and write' privileges, i.e., they can not only draw down customer data but can also modify data, for instance when they initiate a payment on behalf of a customer. This represented an important innovation in EU data governance. Comparable arrangements have been implemented in only very few other jurisdictions.

The directive was the EU's first experience with user-controlled real time data access. The implementation of PSD2 therefore holds a number of lessons for the design of an open finance regime in the EU, which will cover a wider scope of financial data and additional market participants.

According to the study on PSD2 done on behalf of the EU Commission, (European Commission, 2023c), it appears the initial objectives of the Commission have been at least partially delivered:[7]

[6] CEPR and IESE (2022).

[7] European Commission (2023c).

- New business models and technology have emerged, including contactless cards, mobile wallets, and instant payments, underpinning the move from cash-based to digital payments in the EU payments market.
- Stronger systems of customer authentication have reduced fraud and helped to protect consumers better.
- Fintechs and technology firms have played a larger role in offering payment solutions, and this has strengthened competition and product innovation. The number of Account Information Service Providers and Payment Initiation Service Providers has grown significantly.[8] However, the majority of PSD2 licenses have been obtained by firms that were already operating before the implementation of the directive (Polasik et al., 2020).

Equally, the PSD2 evaluation points to a number of gaps and challenges in establishing data sharing on a wider scale:

- The costs of developing APIs, which are needed to make data more broadly accessible, cannot be charged to data users and are therefore passed on to customers. Industry statements suggest this has acted as a disincentive of innovation and development (EFR, 2022).
- The consumer awareness and uptake of innovative payment solutions remains limited overall. In some Member States, only about 1 per cent of transactions are conducted through payment initiation services.[9]
- Cross-border payments remain still quite slow and costly as there are technical issues in the initiation of payments.
- Licensing of entities appears to have been slow, and national competent authorities (NCAs) have applied the directive inconsistently. An additional technical standard issued by the EBA has complicated implementation further as it reopened issues around execution risk, according to industry feedback.

***Recommendation** 1. Given the ongoing trend towards decentralised finance and the emergence of new types of fintechs, EU regulators should continue to broaden the perimeter of financial regulation, in particular to govern data access rights outside the payment system.*

***Recommendation 2.** The experience of PSD2 should be reflected in future regulation on financial data access rights. Specifically, the PSD2 experience underlines the need for incentives for API development and consumer trust that fosters wider adoption of digital finance models and the related scale economies.*

[8] A register maintained by the European Banking Authority (EBA) listed over 400 TPPs that have been authorised outside the banking system, and over 100 AISPs, most of which have licenses to operate across all EU markets.

[9] European Financial Services Roundtable (2022).

3. DATA SHARING IN THE FINANCIAL SYSTEM

KEY FINDINGS

- The benefits of the digital economy for productivity depend on scale economies in data use (larger datasets), and network effects (number of users adopting a similar standard).
- Data use is therefore subject to positive externalities, as the social value of data use exceeds the private value.
- Financial markets also suffer from information barriers between lenders and borrowers, and between data holders and potential data users.
- Data are normally tightly controlled by individual data owners or shared in groups with limited access rights for outsiders, exhibiting the characteristics of a 'club good'.
- In the credit market, data are traditionally collated and processed by private credit bureaus. The market share and role of credit bureaus has already been eroded by fintechs and other technology firms such as alternative providers of data and credit analysis, as governed by PSD2. FIDA would further challenge that position.
- Under the proposed new Regulation on Financial Data Access, financial data sharing schemes will be a new type of private sector collective arrangement designed to develop common standards and entitle data holders to compensation. This encourages industry-led development of standards (APIs), though dominant positions by banks in certain EU countries may limit the inclusiveness of such schemes.

3.1. Data in the digital economy

Digital technology – the representation of information in bits rather than physical media – has wide-ranging implications for the structure of the European economy as the costs of storage, transmission and analysis of data are drastically reduced. Finance has for some time been part of this wider digital and data-driven transformation of advanced economies. As search costs approach zero, consumers' options in finding a suitable financial product are enlarged, and a match to consumer preferences, for instance on sustainability, is more likely. Equally, the costs for a service provider of tracking information about a prospective or current customer are lower. Targeting customers with specific products, or even customised products, and discriminating prices between customers, has become vastly easier (Goldfarb and Tucker, 2019).

The productivity effects of data use benefit from economies of scale (due to the volume of data) and network effects, which are due the number of users adopting a similar standard. Data, when combined with analytics, generates additional information that is valuable to both the original data holder and for data users, boosting productivity and innovation. This data-driven innovation has been given additional potential through the increased use of artificial intelligence and machine learning. The gains from the digital transformation and related innovation arise to both the supply side and to consumers. Large firms are especially likely to increasingly make decisions based on 'big' data sets, leading to greater productivity and output when compared to traditional investment processes. Matching products and services to consumer preferences as they become evident in online markets appears to benefit smaller suppliers in particular (CEPR and IESE, 2022).

Economies of scale and network effects in data use represent positive externalities: the social value of data exceeds the value attributed to data by an individual data holder. For this reason, a market equilibrium is not socially optimal, and the data holder will under-invest in the maintenance and provision of data. Data sharing arrangements, whether in private arrangements or imposed through regulation, essentially seek to broaden data use and overcome this market failure.

3.2. The financial data ecosystem

Financial markets are inherently plagued by information barriers, which distort competition and constitute a further market failure. Asymmetric information arises first and foremost between borrowers and lenders and may lead to adverse selection, credit rationing and moral hazard problems. Information barriers are primarily a problem in credit and insurance markets. Capital markets in principle do not depend on intermediaries of capital, and information sharing between issuers and investors is relatively efficient, including for corporate financial accounts data, credit quality scoring and ratings. Data platforms are now more widely accessible to retail investors and have further raised the efficiency of capital allocations.

In credit markets, a key economic function of banks is to overcome information barriers by screening high-value from low-value projects and monitoring the efforts borrowers make in servicing their loans. Banks inherently enjoy an information advantage over other potential lenders by observing their clients' cash flows, balances and loan performance. Overcoming this imbalance between information accessible to data holders such as banks and potential data users is a further objective of data sharing arrangements.

Despite banks' central role in processing and analysing customer data, it is not clear that banks utilise data efficiently. For instance, digital innovation activity, as evident in patents filed by the largest US banks, seems low (CEPR and IESE, 2022). Effective data usage requires complementary physical inputs, such as data storage and processing capacity, and also specific skills, in particular in IT and modern applications such as machine learning and AI.[10] On both physical IT infrastructure and related skills, banks in the EU fall short of the capacity of their peers in other markets.

In their effort to collate, process and analyse customer information banks typically draw on private sector credit bureaus, which traditionally serve as intermediaries and, to some extent, as repositories of customer data, bridging information barriers between borrowers and lenders.[11] Credit bureaus collate information on customers' basic personal information and also credit quality data, such credit histories or utility payment records. In essence, they are databases and data portals for borrower information, supported by technology and legal solutions. This sector has already undergone rapid change and now typically offers automated lending solutions, database management and 'one-stop-shop' access to a wider set of relevant data sources (World Bank, 2019 and Stournaras, 2019). Even though credit bureaus as private information providers are essential for efficiency in the credit market, the coverage and depth of information varies widely between EU states. This is in part due to the different levels of support by local banks, which often use alternative institutions.

Payment providers, fintechs and large technology firms now increasingly challenge the traditional and symbiotic role of banks and credit bureaus in accessing and processing financial data. These new

[10] The EU data survey (IDC & Lisbon Council, 2022) shows that only 8 per cent of European data professionals work in finance.

[11] Unlike credit bureaus, credit registries are typically publicly owned and designed to support supervision and the monitoring of loans made by regulated financial institutions. In the euro area this sector has been transformed through the establishment of the Analytical Credit Dataset ('AnaCredit') which imposed new reporting requirements for lenders and also credit bureaus who began reporting in 2018. This has to some extent helped with the harmonisation of definitions, indicators and reporting obligations.

market entrants not only draw on a more data-driven organisational culture but also have access to a variety of sources of additional non-financial information, for instance online purchasing and payment histories, which can be utilised in offering and pricing financial services, utilising the network effects in the industry.

The gains from digital finance will therefore depend on suitable mechanisms that can govern the access to and sharing of data across different types of data users and sectors, primarily of credit quality information. As we will show in the next section, the wider use of data could also have significant benefits for the funding of entrepreneurs and improve access to credit for individuals.

Recommendation 3. *The new EU Open Finance regime should foster network and scale economies resulting from a wider data sharing as much as possible. Scale effects need to be assessed in the light of anti-competitive effects and potential market dominance of certain data users, such as large technology firms.*

3.3. The scope of relevant data

The EU's Open Finance framework is set to significantly expand the scope of financial data that are subject to mandatory data sharing arrangements, going beyond payments data covered in the PSD2 so far.

The scope of additional financial sector data that could be included in the new regulation on data sharing is potentially vast. From the perspective of third-party providers seeking to offer additional consumer finance products on the basis of customer data, there will be an interest in balance sheet data and risk exposures of potential clients. They may be interested in asset data (savings and credit accounts and securities holdings) but also need to judge retirement income and risk coverage. There may also be interested in secondary data about a borrower, such as creditworthiness assessments in the form of risk scores and ratings, which a data holder, such as a bank, has computed. For SMEs and corporate clients, there is similarly a need to judge the balance sheet. Intangible assets, such as patents or other trade secrets, play a significant role in a creditworthiness assessment.

At the same time, some data categories may have only marginal benefits compared to the costs that arise from defining data formats and infrastructure. Moreover, the Commission does not cover certain data in the regulation as it sees a risk that certain individuals will be excluded from the financial market (a risk that seems overstated, as we will demonstrate below).[12]

In its proposal, the Commission designates certain data categories for mandatory sharing arrangements, subject to customer consent. This is based on value added and innovative potential, and only data categories that do not risk exclusion of customers are included. Specifically, Art. 2 of the proposed Regulation includes personal data covering:

- Liabilities, such as loans, mortgage-related data;
- financial assets, such as savings, real estate investments in financial instruments and insurance products, including investor profile data;
- insurance-related data, such as non-life insurance, occupational pensions and personal saving plans.

In the area of corporate data, only creditworthiness data are included once they have been collected as part of a loan application or request for a credit rating.

[12] Commission Regulation, recital 18.

At the same time, a number of important financial data and indicators are omitted. Some of these could have a higher potential of value added and innovation than the Commission seems to acknowledge. Among personal data, creditworthiness assessments, life insurance and health insurance and public pension rights are excluded. Public pensions rights account for the bulk of retirement income and could be an important consideration in the assessment of individuals' credit risk. In the area of non-personal (corporate) data, ratings on non-financial indicators could also be considered, specifically on environmental, social and governance (ESG) performance, and on a company's use of intangible assets.

As we review in Section 7 below, other jurisdictions, such as Australia, have also provided for the gradual introduction of non-financial data categories in data sharing arrangements. The regular settlement of utility bills, such as payments to energy and telecoms firms, is an important indicator of personal creditworthiness.

***Recommendation 4**. The scope of data covered by the Regulation could include additional categories, such as public pension rights which are an important indicator in personal creditworthiness assessments. SMEs and other enterprises could also benefit from using the future data sharing schemes for non-financial indicators such as ESG ratings. Even though non-financial data, such as utility payments, are not covered in the FIDA currently, this should be an option in the long term.*

3.4. Open Finance and barriers to data sharing

Reaping the benefits of the digital economy will depend on effective mechanisms for accessing, sharing, analysing and processing of data. The various new digital technologies reviewed in the previous section and the growth of data in non-financial sectors also underline the need for provisions for the access to data that cover the financial sector broadly defined, possibly at some point also including non-financial data.

At the same time, the positive externalities from data use explains the incentive problems and ostensible barriers to data sharing. In principle, data access can be tightly controlled only by the data holder or data owner and in fact very few data are fully public. Data can be used by many potential users without limiting the use by others (they are 'non-rival'), though at the same time others can be excluded from access. Most commonly, data are shared freely within a group of users, though limited outside that group. These are the properties of a so-called 'club good' (CEPR and IESE, 2022). This explains why the typical network effects of using a single standard across the industry are not utilised, as we will explain in more detail in Section 6.

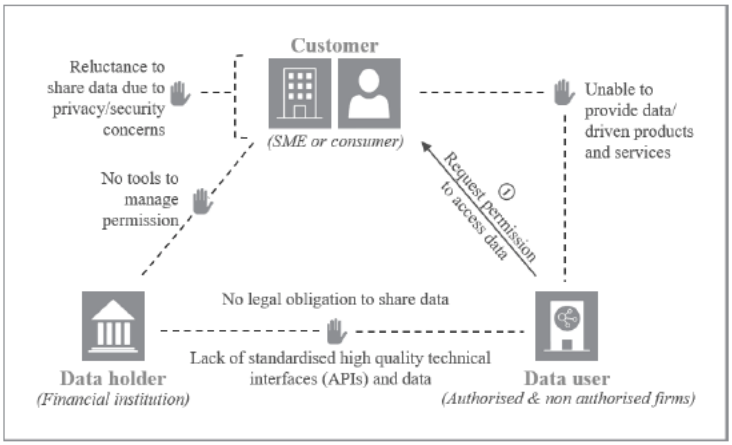
Open banking in the EU context is well defined and refers to the sharing of payment account data with other providers, based on the data owner's consent, and regulated in the EU in the form of PSD2. Open finance is a more recent concept and envisages a framework that governs the access to and use of customer data in all areas of finance, also comprising SME and consumer loans, insurance, pensions and asset management.[13]

The EU's Open Finance framework will regulate the interaction between three key groups of stakeholders: the customer, or data owner, who may want to give access to data to obtain suitable financial products and services, the data holder where such data are housed (typically a bank or other regulated financial institution) and a third party providers or data users who upon accessing customer data could provide additional financial products or services (EU Commission, 2023, see also definitions

[13] Open finance is an opportunity that will "allow consumers and SMEs to access and share their data with third party providers who can then use that data to develop innovative products and services with meet their needs today and in the future" (Mills, 2019).

used by the European Expert Group in: European Commission, 2022b). These interactions are still beset by multiple obstacles (Figure 2).

Figure 2: Stakeholders in the financial system and barriers to data sharing



Source: DG Fisma, Open Finance Regulation Impact Assessment.

Obstacles to data sharing are in large part rooted in the absence of economic incentives: even though the re-use of a dataset by other financial services actors could raise consumer welfare and foster other benefits within the financial system as a whole (due to the returns to the scale of data use), the individual data user attaches a value to the dataset that is below this social value. The various barriers identified in the FIDA impact assessment (European Commission, 2023b) are largely a reflection of this underlying disincentive:

- Given consumer uncertainty over the privacy and security of their shared financial data, consumers tend to be reluctant to share their data. The Commission's survey points to a lack of trust in data governance frameworks, also given the fact that consumers as yet lack tools to control the further use of their data. Terms for data re-use and data sharing would need to be agreed with the consumer (data owner) in the first instance, and be implemented by the data holder, such as a bank who would also need to monitor, and if need be, discipline, other users. This context is particularly problematic given the greater incidence of cybersecurity risks.
- A further problem is the absence of a data sharing obligation. Few consumers have exercised their right under the GDPR to transfer their data to other financial services firms ('data portability'). The concentration of data repositories among banks represents a distortion to competition which may prevent contractual solutions to data sharing.
- In part as a reflection of inadequate incentives for data owners, there is no standard format for transferring interoperable customer data, nor for the way in which they may be shared through accessible common interfaces (APIs) (see Section 6.1). The ongoing lack of a widely recognised digital identity compounds this problem.

3.5. Financial data sharing schemes

Under the new Regulation on Financial Data Access, the Commission proposes an obligation on data holders to share certain types of data at the request of an outside data user, who acts with permission from the customer.[14] Only by acting within the so-called financial data sharing schemes, in which both

[14] These data users will need to be authorised as financial information service providers (FISP) in their respective jurisdictions.

data owners and data users will be need to become members, will data holders be entitled to demand compensation (Art. 5.2 and Title IV and Recitals 25-27 of the Regulation).

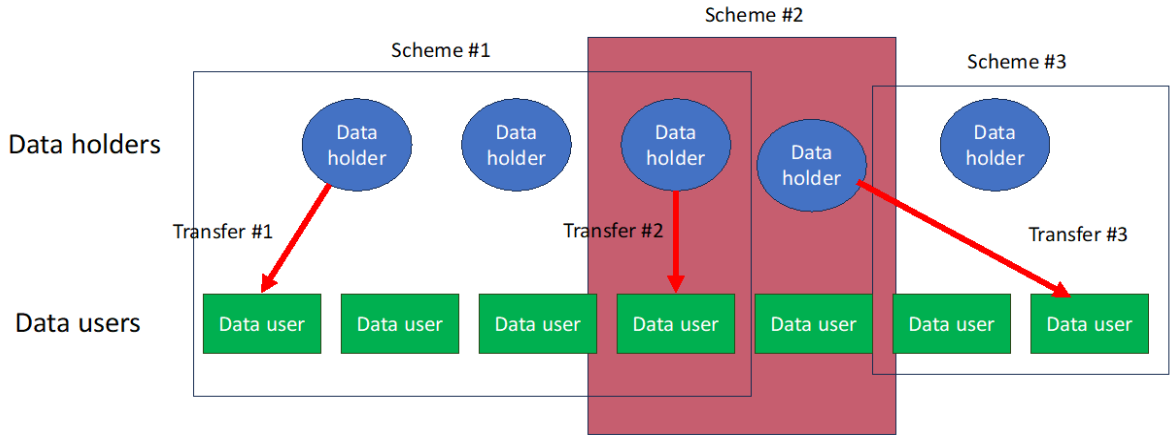
Data sharing schemes will be a novel type of private sector collective arrangement in the financial sector and could in principle overcome many of the above barriers and incentive problems in the market for financial data. In essence, they are designed to break open the restrictive 'club good' nature of data.

The Commission seems to reflect some of the lessons from the PSD2 implementation. Crucially, models for compensation and data interfaces can be specific to individual types of markets and the schemes will be open to all data users and data holders on non-discriminatory terms. To this end, the Commission defines detailed requirements for the composition, governance and compensation models of the schemes in Art. 10 of the Regulation.

The Commission in essence defers to the industry in defining what would in effect become the key fulcrum in the market for financial data. Experience in the payments area, such as the API standards developed by the so-called Berlin Group, seems to be encouraging and could point to a good faith implementation also for other types of financial data. Data sharing schemes will only play their intended role to the extent that they cover the entire single market and a similarly large number of data holders and users within each sector. Ideally, a single scheme would cover all EU data holders and data users in a certain data type, such as insurance or retail investment data. Of course, it is plausible that multiple such schemes may emerge, which would result in barriers between the data pools of different Member States or make data of the largest data holders less accessible for smaller users.

Figure 3 presents stylised cases of data transfers. These could occur between a data holder and data user who are each member in only one scheme, based on the terms of that scheme (transfer 1). Should both parties be member of several schemes they could elect the scheme that defines the terms (transfer 2), instilling a degree of competition between alternative schemes. In the case of the cross-scheme transfer (case 3) the FIDA's requirement for non-discriminatory treatment will apply.[15]

Figure 3: Membership in financial data sharing schemes



Source: Authors' own elaboration.

[15] FIDA Art. 10.1 (h) ii.

Whether industry initiatives will indeed converge on sufficiently inclusive schemes is open to doubt. Experience with credit bureaus for instance suggests that the dominant positions of banks in certain EU markets limited the scope and inclusiveness of collective information sharing. Equally, the FIDA data schemes might over time become overly fragmented by market, sector, or might allow data holders inordinate influence, discouraging open data exchange. Rival schemes in the same sector may frustrate data exchange or define compensation models that discourage data access. In any case, entities authorised under the PSD (the account information and payment initiation servicers providers) will remain subject to a distinct regime.

Recommendation 5. *To be effective, data sharing schemes will need to be inclusive across different data types and data holders and span the markets of most EU countries. European supervisory authorities should closely guide what is in essence an industry initiative to overcome market failures.*

Recommendation 6. *Payments-related data and other financial data have a similar use and origin but will be covered by two different sets of EU legislation. The ecosystems of data sharing arrangement should be constructed so that the two systems can ultimately be integrated.*

4. THE POTENTIAL OF OPEN FINANCE IN THE EU FINANCIAL SYSTEM

KEY FINDINGS

- Consumers are likely to benefit from the future EU open finance regime due to greater financial access, lower search costs and product differentiation. These gains may however be limited due to inadequate digital access and also due to consumer behavioural biases, evident for instance in limited switching between products or the persistent choice of a single provider.
- In EU countries with poor financial literacy, there is also a risk of mis-selling of financial services by data users to poorly informed consumers. Permission dashboards will be of limited use in exercising data privacy rights.
- Financial exclusion and discrimination against certain consumers are only risks in an environment of abundant data availability in which the consumer's decision to not disclose data is interpreted as signalling inferior credit quality.
- As regards non-personal corporate data, only creditworthiness indicators have been included in the proposed FIDA regulation. The open finance regime could result in more suitable products and a greater variety of products being offered by outside providers, including for instance more suitable risk sharing features.
- The future open finance framework will only indirectly benefit the capital markets union project to the extent retail investors are better informed about their financial position or where data access facilitates the communication by brokers. Such data may also relate to the sustainability preferences of retail investors, which at present need to be assessed through a relatively costly process of questionnaires and client interaction.
- Overall, open data will likely accelerate the gains in market share of non-bank lenders at the expense of established banks, whose margins may shrink as IT costs weigh on profitability.

The Open Finance regime in the EU promises to overcome information barriers and allow frictionless interaction between different financial firms and between financial firms and their customers. Many types of data exchange can be envisaged (as for instance described in Recitals 11-16 of the FIDA regulation) or could emerge in future. This is expected to result in welfare benefits for consumers and enterprises, particularly SMEs, and in greater efficiency in the financial sector itself.

In their study of a potential comprehensive open data regime, covering also non-financial data, McKinsey (2021) estimated potential total gains to the EU of 1-1.5 per cent of GDP, with the bulk arising within financial institutions and MSMEs, and smaller gains for consumers. These estimates can at best give a broad idea of orders of magnitude, given that a very ambitious regime of comprehensive data sharing was assumed, and as the dynamic effects or structural changes in the industry were not considered.

In this section, we examine the three potential beneficiary groups in turn and also point to a number of trade-offs and risks that need to be considered. In this review of the evidence, we also reflect on a

more ambitious model for open finance in which entities and data types covered are more expansive than those targeted in the present FIDA proposal.

4.1. Benefits of Open Finance for consumers

A key benefit for households will lie in improved access to suitable financial products. Gains to consumer welfare are likely where consumers are given the option to draw on a wider range of their financial data in supporting a credit application. Alternative credit channels or providers may open up, or borrowers could consolidate various credit relationships within one provider, economising on transaction costs. Additional benefits may arise through greater convenience and lower costs in searching for alternative financial products.

Non-financial data, such as utility payment histories or even tax and other public sector payments, in principle are also relevant in assessing consumer creditworthiness, although they are of course excluded from the present version of FIDA. Credit extended by fintech firms often relies on machine learning algorithms which will need to access digitalised data from a variety of sources while avoiding biased data (Bazarbasch, 2019). The option to draw on additional consumer finance data could be especially significant for borrowers with an early or poorly documented history of payments and loan servicing (a 'thin file' in the industry parlance (McKinsey, 2021)).

Where fintechs and other third-party providers have access to more reliable and comprehensive cash flow data, which show how consumers manage their finances, this may lead to more favourable decisions compared to traditional credit reports, which are often based only on outstanding liabilities. Moreover, providers are more likely to price products in line with true credit quality of the borrower and offer a greater variety of suitable products, including through loan customisation (e.g., offering specific grace periods or changed repayment profiles). [16]

Compared to a situation of undifferentiated products and pricing where some consumers who are creditworthy but poorly documented cannot access credit at all, an ambitious model for open finance represents an unambiguous welfare gain.

At the same time, consumer finance suffers from multiple behavioural biases which make personal financial decisions complex and challenging (Mills, 2019). One result of these biases is a relative disengagement by many consumers from the financial marketplace, evident for instance in the limited switching between providers of the same product, such as current account services, even though comparable information on alternative providers is widely available. At present, only 12.2 million EU consumers, or about 5 per cent, use open banking, pointing to a lack of trust in data governance and also limited interest in potential additional products.[17]

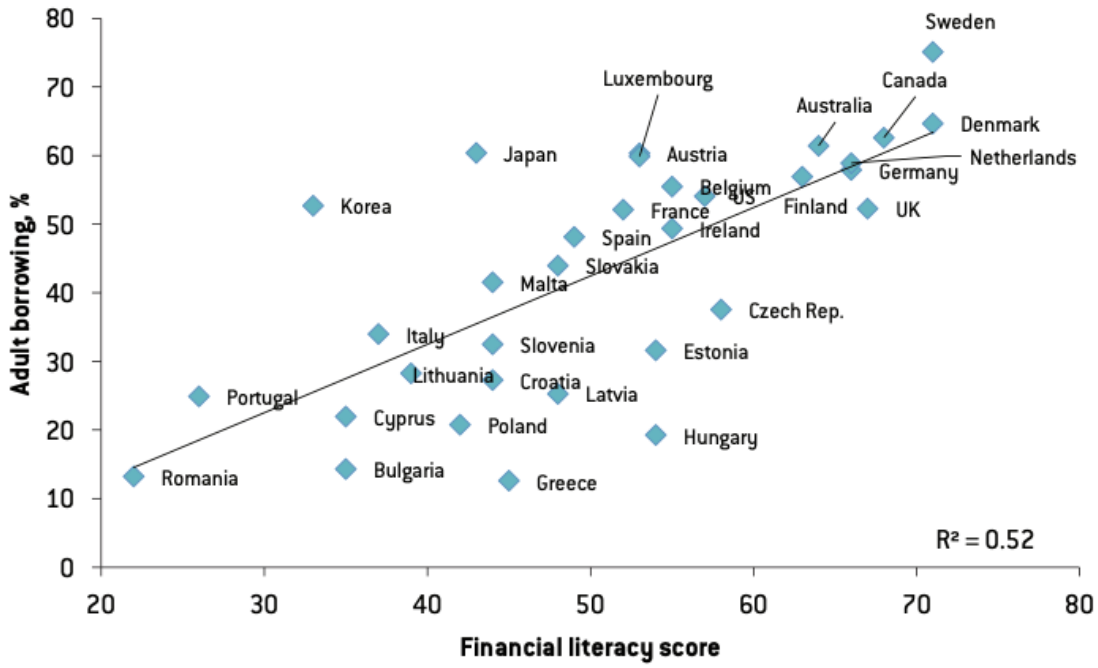
A further constraint results from persistent gaps in financial literacy in many countries in the EU. There is a clear correlation between financial literacy scores and the share of the adult population actively engaging in saving and borrowing, with the latter showing a particularly strong relationship (see Figure 4). In countries with poor financial literacy, only a small part of the population will engage in active comparisons of alternative financial products or share their data to facilitate such alternative offers. Those who do may well require additional disclosure to make informed choices. The new tools

[16] The EU Commission illustrates the potential of its open finance proposal to consumers with a number of 'use cases' relevant in consumer finance (on investment advice and insurance), and the EU financial data Expert Group also studied the case of the mortgage finance market (EU Commission, 2022b).

[17] Figures from the EU Commission impact assessment for the revised payment services directive: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52023SC0231.

designed to help consumers keep track of their data choices and access rights, importantly the permission dashboards (Recital 21 and Art. 8 FIDA), may be similarly ineffective in such countries.

Figure 4: Share of adults borrowing at a financial institution and the financial literacy score in EU countries



Source: Batasaikhan and Demertzis (2018), based on World Bank Global Financial Development Database and Standard and Poor's.

A concern for prudential supervisors will be that the expansion of non-bank lending in the Open Finance context may largely attract riskier borrowers. Evidence from the US indeed suggests that fintech lenders apply laxer screening methods and thereby attract borrowers who are more likely to default (Di Maggio and Yao, 2020). By contrast, customers who make their data available having consented to data access under the EU's FIDA will on average be more financially literate and of a higher credit quality. The consent-based data disclosure should allow non-bank lenders to focus on such customers, leaving established banks with a pool of clients of a lower credit quality.

The Commission also points to a possible risk of (discriminatory) exclusion of some categories of consumers and precludes certain data categories from data sharing for this reason (Recital 18). This risk seems overstated. In an environment of limited data availability, additional data provided by some consumers is likely to open up additional credit supply, without necessarily foreclosing access for others. Only when data access is widespread will the consumer's decision not to disclose his or her data be interpreted as an adverse signal of inferior credit quality.

Recommendation 7. *In countries with poor financial literacy, Open Finance needs to be introduced with additional safeguards for consumers against mis-selling and poor disclosure by data users.*

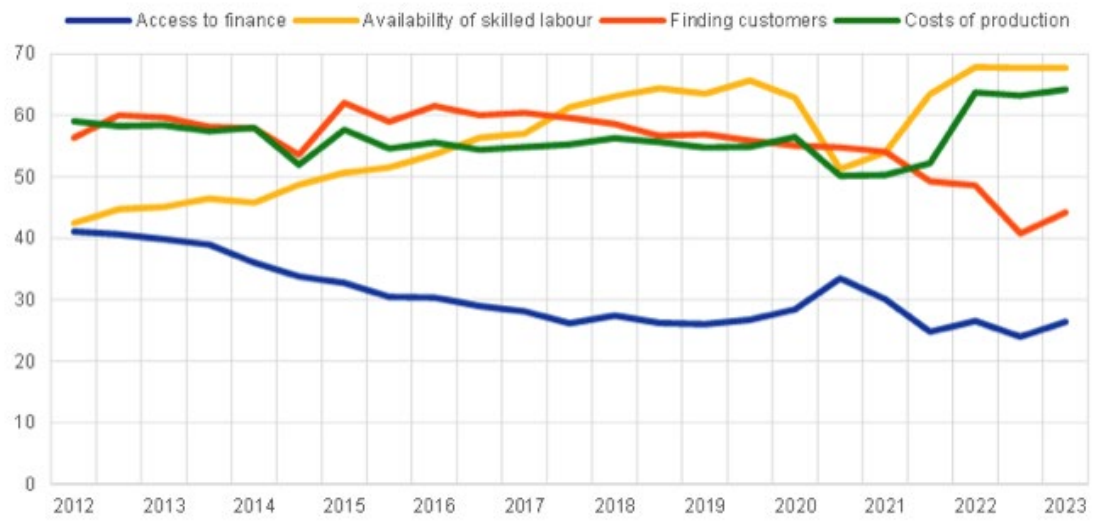
Recommendation 8. *The expansion of non-bank or fintech-based lending on the back of an Open Finance regime may lead to customers of high credit quality migrating to the non-bank sector. Banks' retail credit business may therefore ultimately need closer scrutiny by supervisors. The non-bank sector should also be part of a holistic macroprudential regime.*

4.2. Benefits for micro, small and medium-sized enterprises (MSMEs)

The market for SME credit suffers from two simultaneous types of information problems: the inability of the borrower to communicate his or her true creditworthiness, and the advantage of the incumbent lender over alternative providers of financial products and potential data users (see also section 3.2). SME lending is considered a risky business and lenders typically demand a premium, constraining supply. In addition, due to the hassle of securing an offer from an alternative provider borrowers restrain their demand for credit. Overall, the market clears at a much lower level of credit access and supply than would be efficient.[18]

The latest ECB survey on access to finance suggests a further decline in the availability of credit for SMEs up to the first quarter of 2023, though the financing gap reported by SMEs is not at the level seen during the financial crisis.[19] Respondents flagged access to finance as only a minor concern overall (Figure 5), and only 9 per cent reported a rejection of a credit application. Both these observations may be due to borrowers' restraint in credit applications as firms with lower turnover and employment still report credit constraints. In addition, the EU market for equity-type finance for SMEs, such as hybrid debt, and financing for young companies in their growth phase is underdeveloped.

Figure 5: Major problems faced by euro area enterprises



Source: SAFE data on access to finance.

Enterprises, and in particular smaller enterprises with only intermittent credit relationships, will benefit from Open Finance in similar ways as consumers. A combination of better access, lower search costs and a greater variety of products will lead to greater availability of credit. Micro-enterprises and single entrepreneurs typically intermingle personal finances and business finances so that these entities in any case also benefit through the wider availability of consumer financial products. Financial products from fintech firms and providers may also be more suitable and may address specific financing needs, for instance longer maturities or greater risk sharing.

Analysis done by the EU financial data Expert Group (EU Commission, 2022b) and the Commission's subsequent survey of professional stakeholders suggests that lenders indeed often lack sufficient information to adequately assess SME creditworthiness, to price credit risk, or to offer suitable products.

[18] See also Bank of England (2020).

[19] See ECB: Survey on the access to finance of enterprises: https://www.ecb.europa.eu/stats/ecb_surveys/safe/html/index.en.html.

The Commission's own impact assessment on the proposed regulation argues that SMEs would benefit if creditworthiness data that originated in loan transactions or credit rating assessments were made available in data sharing arrangements. Creditworthiness indicators are the only non-personal data category included in the proposed FIDA Regulation. This would give SMEs the option to make their data available to alternative providers of financial products in a more accessible way.[20]

Credit and other types of SME finance provided by fintechs and online platforms has been growing steadily across the advanced countries, in particular in countries with highly restrictive measures on business activities during the COVID pandemic (OECD, 2022). The EU Expert Group underlined that for SME finance to be broadened on the back of an open data regime, a variety of data holders and non-financial data would need to be covered, including for instance online commercial activity, supply chain activity or energy consumption. Intangible assets, such as patents, also make up an increasingly large proportion of corporate value, though can rarely be used in secured lending transactions. In this light, the scope of SME data that is to be shared under the proposed regulation is quite limited.

SMEs stand to gain from the introduction of the European Single Access Point (ESAP) for which a legislative process is ongoing. This will further expand the availability of corporate information. Large or listed EU firms will ultimately deposit all financial and non-financial disclosure information in this data platform, importantly on sustainability risks, and this will be widely accessible to investment firms and investors. This appears to be a direct and effective way for SMEs to disclose at least some financial data and also sustainability indicators.

Recommendation 9. *Data sharing arrangements for MSMEs should cover a wider scope of data, reflecting in particular the importance of intangible assets for small and young enterprises, such as start-ups.*

Recommendation 10. *The European Single Access Point (ESAP) could be utilised to access data also of smaller and non-listed SMEs, complementing data sharing arrangements under FIDA.*

4.3. Implications for financial services providers and the broader sector

Open Finance will enable and accelerate the broader spread of technology, innovation and digital business models in finance. Its effects on individual sectors, such as banks, insurance, and brokerage, can therefore not be identified in isolation, and indeed these effects are already unfolding. An assessment of the competition and financial stability effect therefore must draw on the by-now abundant literature on digital finance and the associated growth of non-bank financial services (e.g., in ESRB, 2022 or CEPR and IESE, 2021).

At the most basic level, Open Finance will facilitate the ongoing market entry of new third party providers (of both the fintech type and of larger technology firms) as data users and financial services providers. This will erode the market share of established incumbents, in particular in the banking system.

Downward pressure on margins and fee income within the banking sector may further depress the structurally weak profitability picture in the sector. This trend has already been evident in the retail investment space where brokerage fees have been declining for some time, as smaller fintech based brokerage services have steadily gained market share. At the same time, banks may find greater efficiency from more streamlined processing and access to data. Industry reports point to improved operational efficiency and workforce allocation, and also reduced costs in data acquisition in the decision making leading up to a credit decision (McKinsey, 2021).

[20] These are standardised balance sheet ratios or profit and loss indicators that are the key input in credit risk assessments.

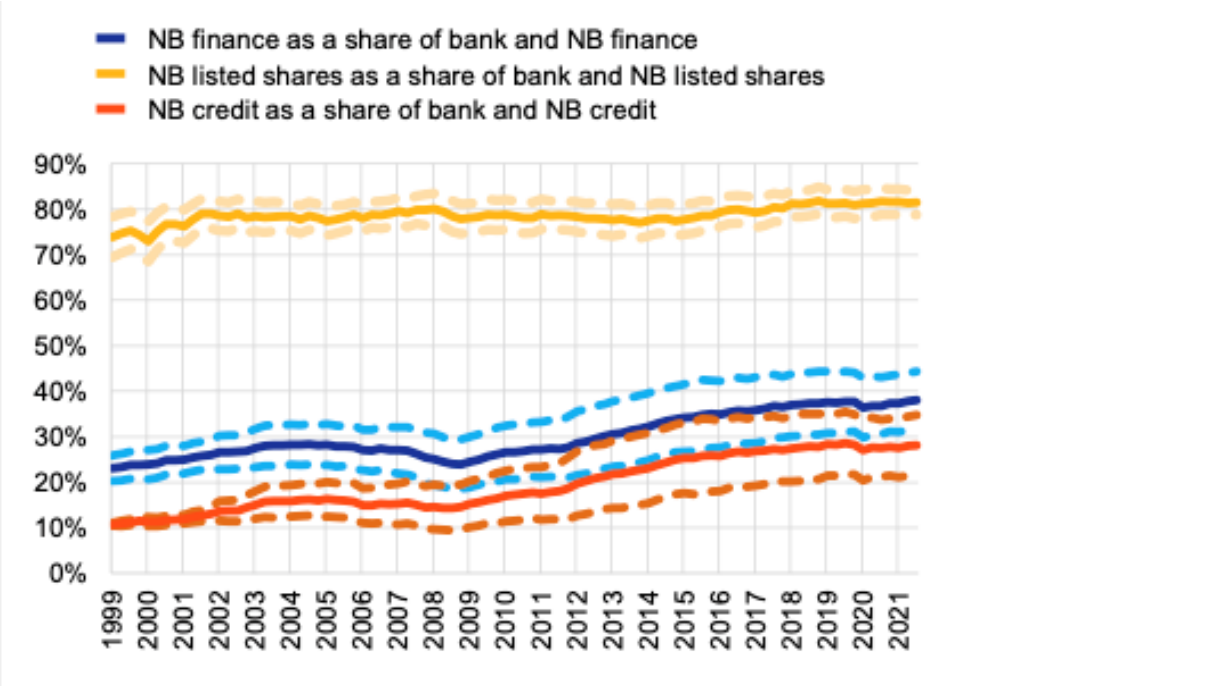
Banks' profitability will be further eroded by capital spending on IT infrastructure and on qualified staff. This may in part be required by FIDA and the need to make data suitable for data sharing arrangements, though there is any case a backlog of IT spending in the sector (ESRB, 2022). Costs for API development will be shared between data users and data holders within the data sharing schemes but will add to banks' IT expenses.

As prices of financial services fall and the ease of accessing them increases, use of financial services will likely rise. Financial services are also likely to be more directly tailored to individual customer needs, and less often bundled within a single product.

On the surface, this then suggests a realignment of the competitive landscape, distributing revenues and profits away from incumbent banks and towards new entrants in the fintech sector and also to large technology firms. The rise of fintech and other non-bank lenders in credit provision is a global trend that has been going on within the EU for some time, with non-bank credit accounting for roughly 26 per cent of total credit to enterprises in the euro area (Figure 6). Further disintermediation would lead to a loss of economies of scale and scope of banks, undermining in particular smaller and mid-sized banks. This seems to underpin the ongoing EU financial services agenda of making the financial system less bank-centric and fostering a consolidation of the excessively fragmented EU banking market.

But this view may well be too simplistic. The experience with PSD2 implementation has demonstrated that established banks can capitalise on having originated customer data and can foster associated digital services. Other jurisdictions with more established open banking frameworks, such as Singapore (reviewed in Section 7), demonstrate that banks can be innovators in API development and can capitalise on the associated digital services by non-bank providers and other fintech firms.

Figure 6: Non-bank finance as a share of total bank and non-bank finance provided to enterprises in the euro area



Source: ECB. Dotted lines represent upper and lower bounds after inclusion of other financial institutions.

4.4. Implications for EU capital markets

Capital markets in essence do not depend on financial intermediaries as they rely on open and non-discriminatory access to data shared between issuers and investors. For instance, an issuer's prospectus, its ongoing financial accounts and other disclosures should be freely and widely available.

In EU capital markets, numerous data sharing arrangement have emerged for specific data, including to satisfy regulatory, compliance or commercial obligations (AFME, 2022). This is often done through industry platforms with more restricted access or bilateral data sharing arrangements, for instance in central security depositories or other data pools.

The further expansion of data sharing has been a long-running theme in the agenda for the capital markets union (CMU) project, and seems particularly relevant for retail investment, which has not risen markedly in recent years (Figure 7).

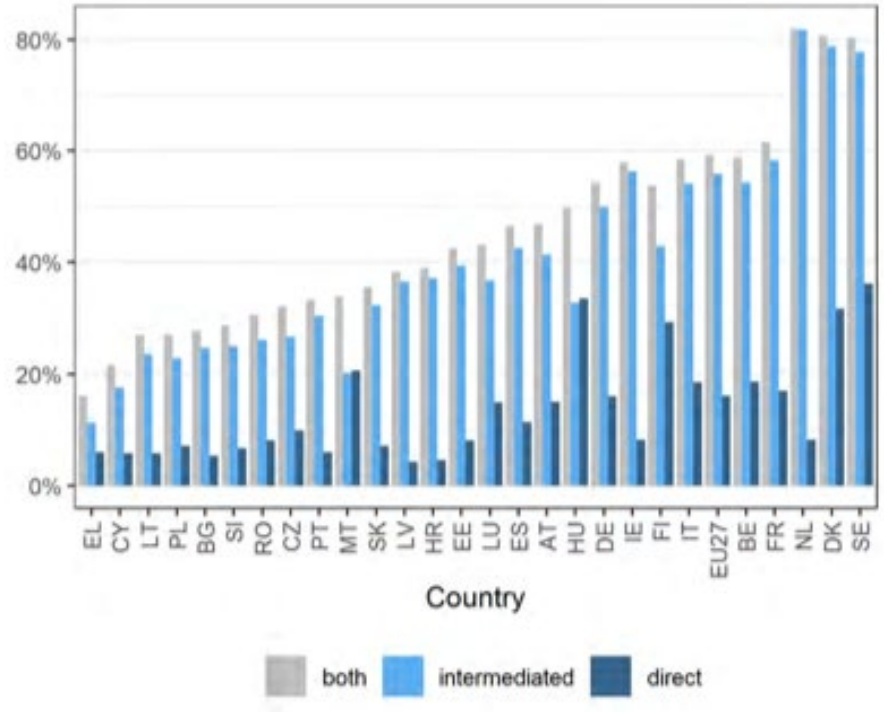
The High-level Forum on the Capital Markets Union (EU Commission, 2020) advocated open finance on the grounds that it would give consumers a better overview of their financial situation, and also easier access to tools that compare costs of alternative and innovative financial products and thus facilitate the switch of providers, such as brokers. The group called for provisions on access to financial data (covering in particular mortgages, pensions and insurance products). It also advocated a somewhat more selective approach to non-financial data, covering in particular sustainability disclosures and the related investor preferences. In the group's view, data sharing would underpin capital market development inasmuch as consumers who are better informed about their financial situation and alternative products are likely to become more active investors in the market for retail investment products. Open Finance and the sharing of data from investors and their preferences could help in the design of investment funds and of suitable portfolios for investors.

These recommendations and the rationale for open finance were subsequently echoed in the Commission's own work plan (EU Commission, 2021) and in industry position papers (e.g., AFME, 2022). Respondents in the Commission's retail investor survey also expect that the sharing of data on current investment holdings could encourage competition and the provision of other investment services (EU Commission, 2023a).

In essence, therefore, the expansion of retail investment should be viewed as an indirect benefit of Open Finance; however, it does not depend on the kind of data sharing envisioned by FIDA. As the Commission's own retail investment strategy makes clear (EU Commission, 2023), constraints to retail investment lie primarily in the way in which information is provided *to* investors, which is often overly complex, but not in any lack of data. Overall, data sharing is already working well in capital markets, and the future FIDA should not be seen as a major catalyst of the CMU project.

That said, survey evidence suggests that sustainability is now a key determinant of retail investor activity. Better and more transparent data on investor sustainability preferences could allow a better matching of investment products (Box 2).

Figure 7: Direct retail investment by households, 2020



Source: EU Commission CMU indicators, 2022.

Box 2: Open finance and the sustainability preferences of retail investors

Since 2022, MiFID rules require brokers and advisers to assess the sustainability preferences of clients before recommending individual investment products. This indeed meets the interest of a large share of retail investors with some surveys suggesting that up to two thirds of investors want to invest sustainably.

The Commission's FIDA impact assessment argues that the personalisation of investment advice based on shared customer data could help to meet these requirements and match investments to the sustainability preferences of investors. Sustainability-related customer information is included in the scope of data covered by the Regulation, and this is expected to enable customers to more easily access financial services that are aligned with their sustainability preference and needs. These data could be contained in regular mortgage, credit, loan and savings accounts and data held by investment firms (see also Recital 13 FIDA).

ESMA guidelines require that firms explain the concept of sustainability to clients based on a questionnaire, and in the process also assess preferences regarding minimum portions of sustainable investment, adverse impacts, and that they also obtain other suitability indicators. Apart from a common suitability assessment, this will require a more detailed conversation in which clients are introduced to a number of key concepts.

Initial sustainability assessments will therefore involve a somewhat more bespoke approach that will likely be different for each broker and investment adviser. Questionnaire responses may nevertheless become usable and transferrable through data sharing schemes.

5. PRIVACY AND DATA GOVERNANCE

KEY FINDINGS

- The proposed Regulation on a framework for Financial Data Access (COM(2023) 360 final) (FIDA) does not replace the GDPR (Regulation (EU) 2016/679), but rather serves as a complement to it.
- This means that access to personal financial data must be based on the grounds recognised by the GDPR. Most access to personal financial data that has been granted to date under PSD2 has been based on the necessity to fulfil a contract (Art. 6(1)(b) GDPR), rather than on informed consent (Art. 6(1)(a) GDPR).
- GDPR provides in principle the right of the user to port data, but this has been difficult to rely on in practice, in part because there are many exclusions from the right, and in part because of a lack of common agreed-on standards. FIDA tries to address this problem by creating explicit obligations for data holders to port certain kinds of financial data to the user or to designated data users when requested by the user, and by creating financial data sharing schemes that would establish standards and would also set maximum fees for the porting of financial data.
- FIDA aligns the use of personal financial data with the GDPR in other ways as well.
- FIDA provides mechanisms for data users located in non-EU/EEA third countries to receive the financial data of EU/EEA consumers if they fulfil suitable conditions. In principle, this should enable suitable US-based and UK-based data users to access the data of EU/EEA consumers, because both countries enjoy adequacy decisions under the GDPR. There are many other countries that do not enjoy an adequacy decision, and there is also a risk of legal challenges to the adequacy decisions of the US and the EU, so this area is likely to be a risk area for FIDA for quite some time.
- Overall, the approach taken to the privacy of personal financial data in the proposed new FIDA and PSR legislation appears to be appropriate.

The FIDA Impact Assessment (EU Commission, 2023b) demonstrates that many stakeholders are concerned about privacy for online financial transactions, as well they ought to be; however, FIDA's solution has been to address this by improving alignment between the GDPR and the successors to PSD2.

The proposed Regulation on a framework for Financial Data Access (COM(2023) 360 final) (FIDA) does not replace the GDPR (Regulation (EU) 2016/679), but rather serves as a complement to it. Recital 48 of the FIDA makes this clear: "Regulation (EU) 2016/679 applies when personal data are processed. It provides for the rights of a data subject, including the right of access and right to port personal data. This Regulation is without prejudice to the rights of a data subject provided under Regulation (EU) 2016/679, including the right of access and right to data portability."

We consider this approach to be in order.

Recommendation 11. *Stakeholders are very concerned about the privacy of their financial data; however, the GDPR, in conjunction with clarifications provided in the FIDA, appears to address these concerns adequately. No further action appears to be required.*

In the sub-sections that follow, we seek to clarify how the FIDA interacts with GDPR. How the various pieces of new Open Finance legislation seek to address security, a closely related aspect, is addressed in Section 6.4.

5.1. The right to access personal data

Processing of personal data is permissible under Article 6(1) GDPR "… only if and to the extent that at least one of the following applies: (a) the data subject *has given consent* to the processing of his or her personal data for one or more specific purposes; (b) processing is *necessary for the performance of a contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; …[21]" [emphasis added]

Operationally, the chief means by which FIDA implements this is by requiring the data holder to "request data users to demonstrate that they have obtained the permission of the customer to access the customer data held by the data holder". (Art. 5(3)(c) FIDA) Ensuring purpose limitation in the use of the data is then the function of Art. 6 FIDA, which is imposed on the data user.

As already noted, this provision is fully applicable to data provided under the FIDA. Recital 10 of the FIDA further clarifies that the customer's data "can be processed for the agreed purposes in the context of the service provided. The processing of personal data must respect the principles of personal data protection, including lawfulness, fairness and transparency, purpose limitation and data minimisation." Article 80 of the PSR likewise requires GDPR compliance.

Our interviews with stakeholders suggest that most of the access to personal financial data that has been granted to date under PSD2 has been based on its necessity to fulfil a contract (Art. 6(1)(b)), rather than on informed consent (Art. 6(1)(a)). There appear to be two main reasons for this.

First, it is not difficult for financial data users to demonstrate that the data is needed to fulfil a contract. Most online financial services are provided for remuneration under contract in any case, so this does not impose a significant additional burden on the consumer or the data user. By contrast, obtaining informed consent in the absence of a contract tends to be burdensome both for the data subject (i.e. the consumer) and for the data user.

Second, and relatedly, the European Data Protection Board (EDPB) has sometimes been sceptical of the use of informed consent. The agency is concerned that large online platforms and large search engines provide a service that users are not willing to do without, implying that the user is more or less compelled to consent to the provision of personal data, like it or not. If the data is clearly related to the performance of a contract, and if the user has explicitly acknowledged as much in the contract, the online financial service provider / data user mitigates this risk.

5.2. The right to port personal data

In theory, the GDPR already provides consumers with all of the rights that they would need to port their personal data from one financial services provider to another; however, these rights have been difficult to apply in practice for reasons that are similar to those that apply in many other domains, including e-health (Marcus et al. (2022)). Recital 5 of the FIDA provides a succinct summary of a well-known problem: "Under the current Union framework, the data portability right of a data subject [under the GDPR (Regulation (EU) 2016/679)] is limited to personal data and can be relied upon only where it is technically feasible to port the data. Customer data and technical interfaces in the financial sector

[21] The text goes on to provide four possible additional justifications that will only rarely apply.

beyond payment accounts are not standardised, rendering data sharing more costly. Further, the financial institutions are only legally obliged to make the payment data of their customers available."

FIDA seeks to mitigate these limitations, first, by placing an explicit and sufficiently detailed obligation on data holders to provide their data to share customer personal and non-personal data upon the customer's request; and second, by driving the creation of standards and modalities of use through *financial data sharing schemes* (see Section 6.1) so as to ensure technical feasibility (Recital 48 FIDA).

5.3. Redress for consumers in case problems arise

FIDA leaves it to the financial data sharing schemes to determine "the contractual liability for data breaches as well as how to resolve potential disputes between data holders and data users regarding liability" (Recital 25 FIDA). These arrangements are to be based on the GDPR, including the right to compensation and liability under Art. 82 GDPR.

5.4. Supervision and enforcement

Responsible use of customer data and respect for privacy rights rests with the data user organisations, which are to be authorised in individual member states as financial information service providers (Recital 33). A central register is to be compiled at the European Banking Authority (EBA), which will also keep track of the financial data sharing schemes (Recital 43).

Overall, this represents a potentially significant expansion of the role of national competent authorities, which are primarily tasked with conduct in financial markets and the authorisation of financial products. Under FIDA, national competent authorities are set to become guardians of data rights, and are expected to cooperate with their counterparts under the GDPR in enforcing FIDA (Recital 36). This coordination may not be sufficiently established or resourced, and there is little in the FIDA Regulation which would suggest support from EU-level supervisors, such as the EBA or ESMA.

5.5. International data transfers

FIDA contemplates international interoperability with third countries (see especially Art. 14(2) FIDA), but data users in third countries are subject to a few additional controls beyond those that apply to EU/EEA-based data users. Beyond that, there are many practical impediments that would need to be overcome for data holders based in countries to which the EU has not granted an adequacy decision under the GDPR.

Data users in third countries must not only comply with relevant FIDA provisions but must designate a legally liable representative in one of the Member States in which they intend to access financial data. The competent Member State authority is expected to attempt to put in place information sharing arrangements with its counterparts in the third country where the data user firm is located. Unsurprisingly, authorisation to use information cannot be granted to firms in jurisdictions that are judged to be non-cooperative for tax purposes, or to be high-risk. (Art. 14(2) FIDA)

Transfer of personal data outside of the EU/EEA is at significant risk in our view. Transfers of personal data from the EU to the United States were substantially disrupted in the recent past as a result of two CJEU rulings that are widely referred to informally as *Schrems I* and *Schrems II* (Marcus, 2020). Transfer of personal data between EU/EEA countries is generally permissible as long as the GDPR is fully complied with but transfer to third countries flows through a different and more demanding part of the GDPR (Arts. 44-50 GDPR).

Transfers of personal data to compliant firms in the US and the UK are currently allowed under *adequacy decisions*, and adequacy decisions are also in place for a handful of other countries including Japan; however, there is still a substantial risk to international cooperation with third countries under FIDA. First, there are a great many countries that are not subject to adequacy decisions; and second, there is substantial risk that the adequacy decisions for the US and/or the UK might be struck down by future court decisions.

Even though Art. 49 GDPR provides a list of potential means that seek in theory to enable firms to deal with transfers of personal data to third countries in the absence of an adequacy decision, this is for the most part not a problem that the financial firms can solve. The fundamental issue in both Schrems I and Schrems II had nothing to do with commercial privacy; rather, the cases hinged on allegations that surveillance of the personal data of Europeans by US intelligence services was excessive (Marcus, 2020). Contracts between financial firms cannot bind the conduct of the US government.

If striking agreements to limit government surveillance with like-minded friendly governments is exceedingly difficult, it goes without saying that agreements with secretive or authoritarian governments whose values and interests are not aligned with those of the EU can be expected to be totally impractical.

Recommendation 12. *There is a substantial risk of disruption to data sharing arrangements for financial personal data with data users in third countries, especially in the case of the US and the UK. The concerns over government surveillance raised in CJEU cases such as Schrems I and Schrems II are legitimate, but pragmatic solutions will be needed. This is fundamentally a GDPR issue – it cannot be solved in PSR or FIDA.*

6. DATA INFRASTRUCTURE AND IT RESOURCES

KEY FINDINGS

- The lack of consistent standards and application programming interfaces (APIs) has been a major impediment to the effectiveness of PSD2 to date.
- In the proposed Regulation on a Framework for Financial Data Access (FIDA), the Commission seeks to solve the lack of standards by obligating each data holder and data user to adhere to at least one financial data sharing scheme. Each financial data sharing scheme would be associated with a set of rules and modalities with which its members would be obliged to comply when exchanging data bilaterally with one another.
- FIDA includes a provision to empower the Commission to provide standards if the sector is unable or unwilling to produce them. This will hopefully not be necessary, but it constitutes an appropriate and vitally important safeguard provision.
- Even so, the risk of barricades and "slow rolling" on the part of incumbent data holders is substantial. There is a significant risk that suitable standards either will not appear at all, or else will be slow to appear. This is a high risk area that will warrant attentive monitoring as FIDA goes into implementation.
- The Commission has been promoting effective cross-border use of identity and authentication services via the eIDAS since 2014, and signalled its hope of using an enhanced version of eIDAS as part of Strong Customer Authorization (SCA). Given that financial service providers continue to make substantial investments in non-eIDAS-based SCA, it is unlikely that eIDAS-based SCA to have a major impact on Open Banking at this time.
- The concentrated market for cloud services, with most EU firms using services from just three service providers all of which are based in the United States, has raised numerous concerns. The concerns over limited interoperability among them, and high switching costs, are potentially mitigated by the proposed (and politically agreed) Data Act. Whether the lack of a first-tier EU-based cloud service provider poses a problem for online financial services in the long term remains to be seen.
- SCA has been seen as a major success for PSD2, and has reduced fraud by as much as an estimated 80%; however, there are known gaps. The proposed Payment Services Regulation (PSR, sometimes referred to as PSR3) as proposed in COM(2023) 367 final) would oblige a broader range of financial services providers to implement SCA, and to strive by various means to reduce the risk of fraud by means of "social engineering".
- Infrastructure security is dealt with by a mix of DORA, PSR, and FIDA.
- Lack of skilled experts in financial services ICT is likely to pose challenges for the sector.

Implementation of the Open Finance regime will drastically expand the types of data designated for sharing between data holders and data users, and the types of actors involved in such data sharing. This will accentuate demands on the industry to define suitable data formats (APIs), to invest in infrastructure such as cloud services, and to put in place sufficient and skilled IT staff. The experience with digital identities, or efforts to put in place a new framework, and legislation to strengthen cybersecurity will be instructive for FIDA.

As we have emphasised throughout, while the proposed Financial Data Access Regulation (FIDA) is key, FIDA must be understood as part of the overall EU legal *acquis*. For the cybersecurity and resilience of EU financial infrastructure, and also for digital identities, other EU laws are relevant, including eIDAS, DORA, and the proposed new Payment Services Regulation (PSR) and PSD3 which are to replace and augment PSD2.

6.1. Standardisation of data formats and application programming interfaces

The Commission's 2020 Retail Payments Strategy (EU Commission (2020b)) already identified the lack of consistent standards and application programming interfaces (APIs) as a major impediment to the effectiveness of PSD2 up to that point in time. "The existence of many different application programming interfaces (API) standards, which are key for efficient and secure access to payment accounts data, as well as different API functionality levels, have presented challenges for third party providers, in particular those that were already in business before PSD2." Multiple assessments have reached similar conclusions.

These concerns notwithstanding, the Commission's ex post evaluation of PSD2[22] argued that requiring a shift to a single standard would be too disruptive and costly for stakeholders, many of whom have already made substantial investments in existing data exchange tools and APIs. This same reasoning is evident in the Commission's Impact Assessment (EU Commission, 2023b).

The Commission's proposed FIDA Regulation nonetheless has the effect of obligating data holders and data users to adhere to at least one *financial data sharing scheme* (see also Section3.5). Each financial data sharing scheme would be associated with a set of rules and modalities with which its members would be obliged to comply when exchanging data bilaterally with one another.

On its face, the proposed approach seems promising, but how it might play out in practice remains to be seen. Data holders such as banks will not necessarily be incentivised to share their data. Consequently, it is possible that they will seek to delay agreement on standards or try to make the financial data sharing schemes less than optimally effective.

Indeed, the classic literature on standards compliance in the presence of positive network effects (Katz & Shapiro, 1985; Farrell & Saloner, 1985) finds that in certain markets, standards compliance will be widespread because all market players perceive net benefits – standards compliance can be win-win for all. In markets however where one or more incumbents perceive that the interoperability resulting from standards compliance would limit their ability to exploit their market power, and that this loss would exceed any likely gains from positive network effects, they may resist complying with voluntary standards. Key questions here are, first, whether we are in the second case for some of the markets of interest, and second, in what ways might incumbents attempt to circumvent or subvert the call for adherence to standards in Art. 5 FIDA?

It would be possible in principle for the European institutions to establish a single standard themselves, or to task some third party to do so, and FIDA provides for this option (Art. 11 FIDA); however, this approach has only rarely been taken in other thematic areas, and for good reason. First, the specialist knowledge required to design good standards is likely to exist in the firms in the sector, not in the EU institutions. Second, the EU institutions might well be motivated by political concerns – they are not necessarily free from conflict of interest.

[22] COM(2023) 365 final.

The Commission's proposed text envisions the Commission providing standards if it is impossible for the sector to produce them (Art. 11 FIDA). This will hopefully not be necessary, but it constitutes an appropriate and vitally important safeguard provision. Even so, one has to wonder whether the Commission can ensure the timely emergence of effective standards if some stakeholders (for instance, data holders who wish to maintain their incumbency advantage) actively oppose or "slow roll" the process.

Once standards are in place, the obligation of the data holder to conform to recognised standards in making data available to the data user is explicit in FIDA: "When making data available …, the data holder shall: (a) make customer data available to the data user in a format based on generally recognised standards and at least in the same quality available to the data holder …" (Art 5(3) FIDA).

***Recommendation 13**. There is a significant risk that suitable standards either will not appear at all, or else will be slow to appear. The empowerment of the Commission to implement standards (Art. 11 FIDA) mitigates this problem but may not fully solve it. This is a high risk area that will warrant attentive monitoring as FIDA goes into implementation.*

6.2. Digital identity and eIDAS

Starting in 2014, the Commission sought to promote effective cross-border use of identity and authentication services with a Regulation on electronic identification and trust services for electronic transactions (eIDAS) (Regulation (EU) No 910/2014). It was recognised that some Member States, notably Estonia, had achieved good success with e-government solutions that built on electronic identity technology.

eIDAS was based on the principle of mutual recognition of Member State digital identity technologies. This approach was doomed to failure – it did not generate enough cross-border commonality and failed to achieve a critical mass of usage. eIDAS suffers to some extent from a traditional chicken-and-egg problem. Users have not adopted it because there are not enough interesting applications that make use of it, and application developers have not made use of eIDAS because not enough consumers have taken it up.

In the Retail Payments Strategy (COM(2020) 592 final), the Commission signalled its intent to use an enhanced version of eIDAS "to support the fulfilment of *Strong Customer Authentication [SCA]* requirements under PSD2 for account login and initiation of payment transactions".

The Commission put forward proposed amendments to eIDAS to try to improve its effectiveness (informally referred to as *eIDAS 2*) (COM(2021) 281 final). The debate over the proposal has been contentious, and in any case, there is reason to doubt that it would have much of an impact on SCA for retail payment services if it were enacted. That ship has sailed. The financial services community has already made substantial investments in SCA that does not rely on eIDAS, and continues to do so.

Widespread adoption of some eIDAS solution might conceivably help to build critical mass for the use of eIDAS in other applications, so there continues to be reason to hope for ultimate success; however, one should not be over-optimistic. As regards retail payment services, a successor to eIDAS is not likely to be a game-changer.

***Recommendation 14.** Efforts to enact an enhanced eIDAS identification and trust framework continue, and are in order, but it seems unlikely that an enhanced eIDAS could have a major impact on how SCA is implemented. One should not expect too much of eIDAS.*

6.3. Cloud data services

The cloud data services market in the EU is highly concentrated. It is estimated that the three largest providers hold about 72% of all EU contracts for cloud service, and none of these three (Amazon Web Services (AWS), Microsoft (Azure), and Google) are based in the EU. This potentially poses challenges for competition, and for open digital strategic autonomy (Netherlands ACM, 2022).

The Netherlands ACM identified competition problems to the extent that switching among cloud providers is difficult and is further complicated by egress fees that cloud service providers charge for taking data out of their services. Many firms use more than one cloud service provider, but typically for unrelated applications, because interoperability among the cloud services is poor in practice.

The approach to mitigation of these concerns that has already been taken in the proposed (politically agreed) Data Act (COM(2022) 68 final) has been to promote the establishment of data interchange standards, and to facilitate the ability of users to switch among cloud service providers.

It is conceivable that the ownership of the main cloud service providers by US-based firms might at some point be viewed as problematic, but this might not be a serious concern. First, any transfer of personal financial data from the EU to the US is currently permissible because the United States has been granted an adequacy decision, thus solving (for the moment, at least, see Section 5.5) the limitations on transatlantic data transfers that were imposed by the CJEU's Schrems II decision. Second, the cloud service providers are presumably well able to localise the storage of personal financial data of EU consumers within the EU if they need to do so.

Various EU and Member State initiatives (notably Gaia-X) aim to strengthen the EU's role in the provision of cloud services. How effective these efforts will be in generating meaningful EU-based cloud capacity remains to be seen. To date, cloud capacity of EU-based cloud service providers has been growing, but not as quickly as that of the US-based cloud service providers. (Netherlands ACM, 2022))

Recommendation 15. *The concentrated market for cloud services, with most EU firms using services from just three service providers all of which are based in the United States, has raised numerous concerns. The concerns over limited interoperability among them, and high switching costs, are potentially mitigated by the proposed (politically agreed) Data Act. Whether the lack of a first-tier EU-based cloud service provider poses a problem for online financial services in the long term remains to be seen.*

6.4. Cybersecurity

As a general observation, the shift from today's Open Banking to tomorrow's Open Finance does not fundamentally change the security problems that need to be tackled; however, it greatly expands the exposure of sensitive financial data to potential malefactors. Data that once might have been under the exclusive control of a single large data holder such as a bank will now be scattered among multiple data user organisations. To become a data user, each organisation will need to be vetted by the national competent authority, but there is still an obvious risk when multiple not-yet-fully-proven firms gain access to highly sensitive data.

The PSD2 obligation to implement SCA is viewed as having been extremely positive, but many issues remain. Aside from that, implementation was substantially delayed in many Member States.

Under SCA, two-factor authentication is required. This means that authentication must depend on at least two distinct elements of what the consumer *knows* (e.g. a password), what the consumer *has* (e.g.

a particular smartphone), or what the consumer *is* (e.g. biometric identification). The likelihood that two of these are compromised at once is much lower than the likelihood that any one is compromised.

One of the major thrusts of the proposed *Payment Services Regulation* (*PSR)* is to attempt to oblige a broader range of financial services providers to implement SCA, and to strive by various means to reduce the risk of fraud by means of "social engineering".

6.4.1. Broader applicability of the obligation to employ SCA

The FIDA Impact Assessment and the supporting VVA/CEPS study (European Commission, 2023c) explain that PSD2 fails to clearly or explicitly impose SCA for (1) *Mail Orders or Telephone Orders (MOTOs)* or for (2) *Merchant Initiated Transactions (MITs)*. The exclusion of MOTOs was intentional since PSD2 Recital 95 states that "there does not seem to be a need to guarantee the same level of protection to payment transactions initiated and executed with modalities other than the use of electronic platforms or devices, such as paper-based payment transactions, mail orders or telephone orders".

MITs are excluded to the extent that Article 97(1) of PSD2 applies only to the payer, and thus presumably not to actions initiated by the merchant payee.

The PSR provides clarifications that attempt to deal with each of these omissions or ambiguities in the application of SCA. For MITs, the payer is required to use SCA when the payment mandate is created, but SCA is not required for each subsequent transaction thereafter. If a payment is initiated other than by online means, it qualifies as a MOTO, but online the non-online portions are exempted from the obligation to employ SCA. The PSR further cautions that it is not permissible to use an acquirer outside of the EU/EEA to circumvent the obligation to employ SCA. (Recitals 108 and 109, PSR)

6.4.2. Reducing the risk of fraud via "social engineering"

As the FIDA Impact Assessment explains (EU Commission (2023b), pp. 8-9), even though the SCA has been effective in shutting down many forms of technology-based fraud, other forms of fraud have grown. The Commission explains that "… "pre-payment fraud" can take the form of invoice fraud (where invoices are intercepted and the merchant account number is substituted [by] that of the fraudster), or more sophisticated *"Authorised Push Payment" (APP)* frauds involving social engineering of the payer through direct interaction (e.g. manipulation of the payer into believing s/he is dealing with a genuine payee or even with a bank representative). Cases of such APP fraud … cannot be tackled by SCA because, technically and legally, most of these fraudulent transactions have been authorised by the payer using SCA. The fraud is in fact taking place before SCA without the payer knowing that s/he is being defrauded. The consumer thinks in good faith that s/he is sending money to recipient X, whereas in reality s/he is sending money to a fraudster."

FIDA attempts to reduce this risk in several different ways. The most important of these is the proposed unique identifier verification service. "Payers intending to send a credit transfer to a given payee may, as a result of fraud or error, provide a unique identifier which does not correspond to an account held by that payee. To contribute to the reduction of fraud and errors, payment service users should benefit from a service which would verify whether there is any discrepancy between the unique identifier [e.g. the IBAN] of the payee and the name of the payee provided by the payer and, should any such discrepancies be detected, notify the payer …" (Recital 70, PSR) The PSR creates an obligation whereby the payer is notified within a few seconds of attempting a payment, and before completing the authorisation of the payment, if the name of the payee does not appear to match the name on the account (based on its unique identifier such as an IBAN) to which the money is being transferred. The proposed PSR would broaden an obligation that the Commission had already proposed in 2022 (in

COM(2022) 546 final) for SEPA instant payments such that the obligation to verify would now apply to payment services providers offering any credit transfer in any EU currency.

The legislative proposal is upbeat on this approach, and it indeed seems promising, even if it entails costs for the firms. It has the potential to reduce "social engineering" fraud where a consumer is induced to make a payment to a fraudster, thinking that the payment is going to a legitimate payee. "Such services, in the countries where they exist, have had a substantial positive impact on the level of fraud and errors." (Recital 70, PSR)

The Payment Information Service Provider (PISP) would bear the liability to the payer if it improperly applies the unique identification verification, or if the verification malfunctions, and this results in an improper transfer.

Recommendation 16. *The* unique identifier verification scheme *that has been put forward in the PSR seems to be a promising approach to deal with certain kinds of Authorised Push Payment (APP) fraud. Something along these lines appears to be needed.*

Many other forms of "social engineering" fraud have emerged or have grown in recent years. An egregious example occurs when a fraudster successfully impersonates a bank employee. PSR seeks to address this to some extent by clarifying who is liable for which forms of fraud (Arts. 59 and 60 PSR); by promoting information sharing among PSPs, and also with providers of electronic communications; and by requiring PSPs to educate consumers as to the risks.

Recommendation 17. *The measures to combat fraud that are put forward in the PSR proposal are in principle appropriate, but the threat landscape is sure to require continued attention from policymakers.*

6.4.3. Operational cybersecurity

Operational and infrastructure security for financial transactions is already addressed in numerous existing or proposed laws, notably including the Regulation on digital operational resilience for the financial sector (DORA) (Regulation (EU) 2022/2554), the PSR, and to a lesser degree in FIDA.

With DORA, the EU is attempting to integrate and harmonise cybersecurity obligations that had previously been scattered across multiple legislative instruments. It was a response to the recognition that in a highly interconnected financial sector, it was risky and potentially destructive to have fragmentation at Member State level as regards such basic things as ICT-related incident reporting and digital operational resilience testing. There was also a clear need for information and intelligence sharing in relation to cyber threats and vulnerabilities. DORA seeks to address these for all network and information systems supporting the business processes of financial entities in a harmonised manner across the EU.

Infrastructure security appears at many points in the PSR, including Articles 2 and 80. For SCA as introduced in PSD2, PSR seeks to clarify a key aspect of the two factor authentication.

EU laws including DORA already entail extensive requirements for the security of financial data. FIDA effectively ensures that the security requirements of DORA (and of the PSR to the extent relevant) are also applicable to the financial data sharing process. "When making data available …, the data holder shall … communicate securely with the data user by ensuring an appropriate level of security for the processing and transmission of customer data…" (Art. 5(3) FIDA).

The European Union Agency on Cybersecurity (ENISA) has some significant and appropriate tasks in DORA. Their expertise might be of considerable value for Open Finance. They are mentioned only in passing in the PSR (in Art. 81(2)), and not at all in FIDA.

Recommendation 18. *The security-related provisions in DORA, PSR and FIDA seem to be generally appropriate; however, it is not obvious that the expanded threat landscape implicit in having so many organisations, including some rather young organisations, holding sensitive data has been fully reflected in the planning of the PSR.*

Recommendation 19. *The threat landscape can be expected to continue to evolve rapidly. With this in mind, the review periods envisioned may be too long (5 years in Art. 108 PSR, 4 years in Art. 31 FIDA).*

Recommendation 20. *PSR and FIDA should provide a clear and explicit advisory role for the European Union Agency for Network and Information Security (ENISA).*

6.5. Skills

Implementation of the various provisions of FIDA can be expected to entail non-trivial investments of time and energy on the part of both data holders and actual and prospective data users (EU Commission, 2023b), but the skills needed to implement data sharing are in short supply in the EU at present and for the foreseeable future (Batura et al. (2023, forthcoming); IDC & Lisbon Council (2023)). Banks in particular have been complaining about skill shortages for many years. The shortage of cybersecurity skills is particularly worrisome in this context.

Many initiatives have been launched to strengthen EU digital skills training, but this can be expected to be a persistent problem for multiple reasons. First, EU competence for education and training is limited, so the responsibility falls largely to the Member States. Second, it is not sufficient merely to train workers – it is equally important to retain them. The brain drain to the USA and to other parts of the world has posed a challenge. And third, even in the best of circumstances, it will take time to train enough workers sufficiently.

At EU level, the lack of digital skills can be expected to be addressed to some extent within the framework of the Digital Education Action Plan 2021-2027 as a part of the European Skills Agenda; however, large gaps will presumably remain. [23]

Recommendation 21. *Shortfalls in the number of skilled ICT professionals available is a general problem for the EU in the near and medium term, and some programmes are in place to try to mitigate the problem. Lack of ICT skills in the financial sector, including cybersecurity skills, is likely to become an acute problem, and there is a risk that PSR and FIDA exacerbate this problem. Possible mitigation measures might include education, training and re-training, and facilitating entry from skilled and carefully vetted professionals from third countries.*

[23] Communication from the Commission. European Skills Agenda for sustainable competitiveness, social fairness and resilience, COM(2020) 274, 01.07.2020 and Communication from the Commission. Digital Education Action Plan 2021-2027 Resetting education and training for the digital age, COM(2020) 624, 30.09.2020.

7. INTERNATIONAL EXPERIENCE

KEY FINDINGS

- Most OECD countries promote the expansion of data sharing provisions in payments and banking. Only a few countries cover non-financial data, such as utilities.
- The UK stands out for having a dedicated supervisory structure, and for seeking to promote SME credit through data sharing.
- Australia has consistently promoted the benefits of consumer data sharing and has made consumer data rights more transparent. Dedicated programmes and fiscal spending underpin the digital agenda, with a government website setting out benefits to consumers.
- Singapore underlines the benefits of an organic, market-driven approach to open banking, and also wide-ranging inclusion of consumers' financial and government data in consolidated accounts. There is also experience with the cross-border exchanges of API standards.
- API development is generally market-led, not defined in regulation. Industry-run collective arrangements mandated by regulation, as proposed in FIDA, appear unique.
- The UK has reflected open finance in two bilateral trade agreements under which data do not need to be localised.
- In general, given diverging privacy and data rights standards, inter-operability with non-EU/EEA jurisdictions will be challenging.

7.1. Experience in non-EU jurisdictions

EU rulemaking needs to be understood in the context of changes in financial services technology and services business models which impact all markets. Regulation in jurisdictions outside the EU should also inform the EU's own efforts with a view to keeping the EU financial market open to cross-border services provision and innovation.

Naturally, most countries define open finance in the context of their existing open banking frameworks. An OECD survey of 31 countries found an explicit definition of open banking rights and data sharing rights only in the UK, Australia and five other countries, in addition to the EU's PSD2 framework (OECD, 2023). Only three jurisdictions also already envisage the regime of 'open finance', among them Australia, though the expansion of data rights is incremental.

7.1.1. The UK

The implications of the data economy for the UK's financial sector were assessed in the 'Future of Finance' report published in 2019, which formed the basis of a strategy document shortly thereafter (Bank of England, 2019a and 2019b). One of the five new priority areas defined in that strategy envisages the creation of an open platform to boost access to finance by small businesses and households. This would help small businesses harness their data through a portable credit file, allowing greater access to more diverse and competitive financing options. The central bank's plan was to draw

on a government review of data resources, standards and technology, with a view to expanding choice for of end-users of financial services.[24]

The Financial Conduct Authority (FCA), as the supervisor responsible for consumer financial services, consulted on its future approach to open banking and open finance in 2021 and is currently in the process of drafting a new guidance. A new oversight committee was established in early 2022, and the FCA and the Payments System Regulator tabled recommendations on the next stage of open banking in April 2023.[25] These recommendations flagged three objectives: (1) unlocking the potential of open banking payments to support competition and innovation by creating greater choice between payments methods and enabling opportunities to build the next generation of payments, including more efficient and tailored services; (2) adopting an open banking model that is scalable for future expanded data sharing; and (3) establishing a sustainable footing for the ongoing development of the open banking ecosystem (relating in particular to safeguards against financial crime and cybersecurity issues).

In essence, the UK sees open banking as a key part of its financial market development. The sharing of a wider set of data beyond the payments system is envisaged, though as yet not legislated, even though a dedicated regulatory structure is in place that will seek to coordinate data sharing between the payments system and other parts of the financial system.

7.1.2. Australia

Australia already defined a comprehensive *Consumer Data Right (CDR)* under its competition act of 2010. Under the Consumer Data Right rules, data holders are required to participate in data sharing and to make certain data available. In the past three years, there has been a rapid expansion of the open banking regime.

Since 2021, customers of the four major banks, which account for the bulk of the system, can share their data with other providers. Datasets from non-bank lenders can in principle be designated for data sharing in a similar way to those of banks. Since 2021, the rollout of the CDR has been funded with considerable outlays in the federal budget as part of Australia's digital economy strategy. The government is in principle committed to most of the 100 recommendations of a wide-ranging enquiry into the future expansion of the Consumer Data Right act. [26]

To be eligible to receive consumer data under the CDR framework, data recipients must be accredited by the Competition Commission. Accredited data recipients initiate the data access request on behalf of a consumer if the consumer provided their express consent for the data recipient to collect such data. In addition, a number of commercial intermediaries also collate financial data from banks and other parties, provide additional services, and make this data available via APIs. These intermediaries are also able to operate under the Consumer Data Right act, once they too have become accredited data recipients and have met regulatory requirements (specifically, the general privacy laws to the extent that they handle personal information). In a 2022 survey of 31 OECD countries, Australia was one of only five countries to have established APIs as a mandatory obligation for banks and other financial institutions under data sharing framework (OECD, 2023).

---

[24] See an update on the SME platform here: https://www.bankofengland.co.uk/research/future-finance/champion-a-platform.

[25] Joint Regulatory Committee (2023): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1150988/JROC_report_recommendations_and_actions_paper_April_2023.pdf

[26] Report available at: https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report, statement by the Australian Treasury available here: https://openfuture.world/open-finance-global-progress-ebook-australia/

Australia's open banking regime was extended in late 2022 to a number of energy providers, and a law is currently under consideration that would give consumers greater leeway in instructing data users to also perform certain tasks, such as payment initiation. In 2023, the government committed to a considerable further extension of the Consumer Data Right, covering among others telecommunications providers. Open finance is already defined in law as non-bank lending, general insurance, and superannuation (pensions), though not yet implemented.

7.1.3. Singapore

Singapore has adopted an industry-led approach to open banking and finance. Data sharing is not mandatory, though widely practiced, and subject to the Personal Data Protection Act.

APIs are not standardised but can be exchanged on APIX, a central platform that also serves as a 'sandbox' in which data protocols can be tested.[27] APIX has been used by providers across the Asia region, and in 2022 about 50 financial institutions and 140 fintech companies participated. The largest banks also host their own API platforms. DBS, the country's largest bank, runs the largest API developer platform based on which numerous merchants participate in the bank's payments programmes.

Singapore established one of the first public digital platforms to pool personal financial data from both financial institutions and government sources, SGFinDex. The platform draws on the country's digital identity system whereby consumers provide consent through a centrally managed system. 15 financial institutions and the central securities depository participate and can be individually authorised for data sharing on the platform by the consumer, and data from government sources (e.g. retirement accounts, medical bills and mortgage payments) are also accessed. This is designed to help individuals retrieve and manage their personal financial information.

Recommendation 22. *Open Finance should be part of the closer coordination with UK financial regulators, including within the EU-UK TCA.*

Recommendation 23. *Data holders and fintechs should be encouraged to exchange and test APIs on a central platform that is open to non-EU parties, emulating the success of Singapore with such a model.*

Recommendation 24. *As demonstrated by other countries, promoting use cases and consumer benefits on a government-run website can build trust and interest in data sharing.*

7.2. What need for 'interoperability'?

Scale economies and network effects of data use can arise both within the EU single market, and in the form of financial services provision from third countries. The fintech industry is evolving, and global players, notably large technology firms, can be expected to vie for entry to the European market. Openness to fintech firms and data intermediaries from other jurisdictions could significantly expand the number and quality of third-party providers.

Interoperability is the concept that describes the compatibility of data standards and formats that allows different data holders to communicate with each other, subject to the consumer's informed consent. Standards for APIs are a necessary but not sufficient condition for such data exchanges. Interoperability is relevant for the communication between data holders and users in different sectors of the economy. In the UK, for instance, a 'smart data' working group seeks to bridge such divisions and includes utilities regulators, and some key government agencies, such as the Department for Work and

[27] See APIX: Collaborate to innovate: https://apixplatform.com/about-us.

Pensions. Within the EU/EEA, interoperability is a key ambition of FIDA and its industry-run data sharing schemes.

Interoperability also describes the compatibility of standards of *different* jurisdictions.

The OECD survey does not suggest that this has been an objective in rulemaking in other jurisdictions. A notable exception are the two free trade agreements which the UK recently concluded with Australia and New Zealand. Under these agreements, financial services market access cannot be conditioned on local data storage within the partner's territory. This is subject to each party's privacy and data protection provisions, though was seen as a boost to the scope for digital financial services as part of bilateral trade relations (Beck and Petit, 2023).

As noted in Section 5.5, the EU's ability to profit from international cross-border open finance is likely to be severely constrained with any countries that do not hold an adequacy decision under the GDPR.

8. THE WAY FORWARD

KEY FINDINGS

- A key goal of the EU is to move from Open Banking to Open Finance, as embodied in the proposed FIDA regulation.
- FIDA must be understood as part of the overall EU legal acquis. FIDA was intended to work in concert with a broad range of existing law and regulation, as well as with a new regulation that replaces and supplements PSD2.
- The overarching objectives of FIDA are (1) to increase competition in the offering of a wide range of financial services; (2) to provide greater consumer choice; and (3) to facilitate market entry of new and innovative financial service providers.
- Key areas that warrant further elaboration over the course of the FIDA trilogue are (1) the expansion of the regulatory perimeter; (2) bridging divisions within the single market; and (3) making industry-led initiatives work.
- The legislative proposal is short on detail on how the resources, let alone the competences, of EU-level supervisors (EBA, EIOPA and ESMA) need to be beefed up to reflect the expansion of the regulatory perimeter with the shift towards Open Finance.
- A number of known deficiencies in GDPR can be expected to adversely impact the effectiveness of FIDA in practice.
- In order to create economies of scope and scale that reflect the EU as a whole, it is necessary to have consistent rules that enable cross-border financial transactions across the EU/EEA.
- A robust Open Finance system for the EU must provide for (1) obligations on a wide range of incumbent data holder financial institutions to provide data and in some cases interoperability with an even wider range of incumbent and new third party financial data user service providers; (2) standards that make interoperability and portability efficient, secure, respectful of consumer privacy, and cost-effective, including for cross-border operation; and (3) a compensation model that provides the right incentives to all parties.
- We see important strengths in the proposed financial data sharing schemes; however, a major concern reflects lack of clarity when data holder and data user do not agree on which standards and which maximum compensation should govern.
- We also see a significant risk as regards data transfers to non-EU/EEA countries, for instance if an adverse court ruling were to strike down a GDPR adequacy decision to a major trading partner such as the UK or the USA.

This section and the next provide our overall findings and recommendations to policymakers. In Section 8.1, we summarise the gaps and limitations that we have identified in the Open Finance framework as proposed. In Section 8.2, we sketch an ideal long-term framework, and summarise the key themes in recommendations that could help deliver it. Chapter 9 recapitulates each of our recommendations and notes the page on which they first appeared.

8.1. Gaps in the existing framework

In line with the Commission strategies on digital finance and on payment services and drawing on extensive input from stakeholders, the EU's goal today is to build on existing law and policy in order to implement *Open Finance*. The Commission's initiative comes at an opportune moment, as most of the broader framework for digital and data governance has already been put in place, and as technology is about to fundamentally reshape business models in finance.

The overarching objectives of FIDA are (1) to increase competition in the offering of a wide range of financial services; (2) to provide greater consumer choice; and (3) to facilitate market entry of new and innovative financial service providers.

Open Finance, as articulated in the FIDA, promises to expand access to finance for consumers and smaller enterprises and to expand the variety of financial products, which are likely to be more suitable to individual credit needs or investment preferences. Banks will remain the mainstay of the EU financial market, though their innovation and IT investment will be held back by various cyclical and long-term structural problems (ESRB, 2022). In this context, digital finance facilitated by greater data sharing under FIDA could be a much-needed boost to credit access and financial sector resilience. These potential gains need to be weighed against important risks, importantly stemming from poor financial literacy and as yet patchy prudential supervision of the non-bank financial sector.

Our overall assessment is that the FIDA and PSR Regulations and the new PSD3 Directive that were put forward in June 2023, together with the existing *acquis* including GDPR, DORA, and more, collectively define a coherent framework for Open Finance in the EU. The Commission has done a competent job of analysing both the strengths and the weaknesses of the existing Open Banking framework implemented by PSD2 and has crafted sensible measures.

Our analysis has identified three key challenges that warrant further elaboration over the course of the trilogue by the co-legislators:

- the expansion of the perimeter of financial regulation and related implications for the GDPR and cybersecurity;
- bridging divisions within the single market; and
- making industry-led initiatives work.

8.1.1. Managing the shift from *Open Banking* to *Open Finance*

The EU had already laid the basic foundations of *Open Banking* with the enactment of the Payment Services Directive (PSD), especially with the enactment of PSD2 in 2016. PSD2 enabled competitive entry of new forms of third-party providers and provided them with controlled access to personal financial information that previously had been in most cases available only to the traditional banks that held the consumers' accounts.[28]

FIDA imposes data sharing obligations on a much broader range of data holders, including not only banks but also insurance companies, pension funds and investment companies. This creates numerous new tasks in financial supervision, importantly the authorisation of data users and the assessment of

[28] Data portability rights also exist in other EU legislative acts, including GDPR, but these have been largely ineffective as regards financial data due to (1) lack of specificity in obligations, (2) lack of standards for data transfer and application programming interfaces (APIs), and (3) inadequate specification of payment arrangements for the data.

data sharing schemes. Deferring largely to national competent authorities does not do justice to the challenge of uniform treatment and market integration in a highly dynamic sector.

We find the Commission proposal silent on how the resources, let alone the competence and mandates, of EU-level supervisors (EBA, EIOPA and ESMA) need to be beefed up to reflect the shift towards Open Finance (see also Section 5.4). In preparing the implementation of FIDA, a sound supervisory structure should also be in put in place, and cybersecurity and data privacy risks need to be addressed as part of this preparation. This seems to call for more centralisation and coordination with EU-level supervisory bodies, including EBA, EIOPA and ESMA, and better resourcing of these agencies.

FIDA must be understood as part of the overall EU legal *acquis*. FIDA was intended to work in concert with a broad range of existing law and regulation, as well as with new legislation that replaces and supplements PSD2. A robust Open Finance framework would be unthinkable without effective controls over the data protection and security of personal financial data. But as we explained in Section 5.1, FIDA does not create a new framework for the protection of personal data; rather, it draws on the existing GDPR. In a few instances, FIDA seeks to explain how the new FIDA rules relate to the GDPR, but FIDA complements the GDPR – it neither replaces nor alters it.

Recommendation 25. *The resources of EU-level supervisors (EBA, EIOPA and ESMA) should be strengthened to reflect additional responsibilities and the expanded regulatory perimeter, and the needed support of counterpart agencies in the Member States.*

Recommendation 26. *Subsidiarity and the needed inclusiveness of new market structures also warrant expanding the competencies of EU-level supervisors. Specifically, financial data sharing schemes are to span different markets and types of financial actors and should evolve with the dynamic technology. Their authorisation and ongoing supervision should therefore be an EU-level matter.*

8.1.2. Privacy

That FIDA leaves consumer privacy to GDPR, rather than seeking to introduce new measures, is entirely appropriate; however, many characteristics of GDPR have proven to be problematic. These are GDPR deficiencies, not FIDA deficiencies as such, but they can be expected to impact the effectiveness of FIDA in practice.

First, while the rigidity of GDPR obligations may be positive in terms of its ability to protect consumers, that same rigidity is negative in terms of ease of use, and also in terms of its ability to enable innovation. Secondly, that same rigidity makes it difficult to find compliant solutions to the legitimate concerns that were raised by the Schrems I and Schrems II cases (see Section 5.5), thereby putting at risk international transfers of personal data to key EU trading partners. Finally, GDPR's one stop shop enforcement mechanism has proven to be deeply problematic. It leads to poor allocation of staff resources among the national Data Protection Authorities of the Member States, and also to probable incentive problems where responsibility for regulation falls to those Member States that have the least incentive to enforce aggressively (because the Member States compete with one another to gain the headquarters of digital online firms, in part by offering a regulatory climate that the firms perceive as favourable).

Recommendation 27. *A number of known deficiencies in GDPR can be expected to adversely impact the effectiveness of FIDA in practice. Its rigidity appears to impact ease of use as well as its ability to enable innovation. GDPR's one stop shop enforcement leads to poor allocation of staff resources among the Data Protection Authorities of the Member States, and also to probable incentive problems among the Data Protection Authorities. These are GDPR issues that cannot be fixed in FIDA.*

8.1.3. Cybersecurity aspects

FIDA has nothing to say about cybersecurity. It draws on the overall risk management framework established by DORA, which should be implemented swiftly ahead of the liberalisation of data transfers. As regards payment-related information, Open Finance benefits from the Strong Customer Authentication (SCA) that was initially put in place in PSD2, and which will be strengthened with the enhancements that appear in the new PSR that was proposed at the same time as FIDA.

8.1.4. Bridging barriers within the Single Market

The fundamental legal basis for FIDA, and indeed the rationale for implementing Open Finance at EU rather than Member State level, rests on the Single Market provisions of Art. 114 TFEU. These rest in turn on Art. 26 TFEU, whereby the EU is to establish and maintain the internal market as "an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured".

FIDA is proposed as a Regulation. This is appropriate in our view. In order to create economies of scope and scale that reflect the EU as a whole, it is necessary to have consistent rules that enable cross-border financial transactions within the EU/EEA. This is clearly not the case today – most financial institutions operate in a single Member State, and cross-border financial transactions between institutions in two different Member States are far from being frictionless.

The revisions of PSD2 already reflect concerns that were visible in the recent review of PSD2 over fragmentation in its implementation of PSD2. The revised payments system legislative proposal has been broken up into a Regulation (the PSR), which contains most of the operative aspects of PSD2, and a Directive that deals with Member-State-specific aspects.

8.1.5. Making private sector-led data sharing schemes work

A major concern relates to the *financial data sharing schemes* (Art. 11 FIDA) that are intended to "develop data and interface standards, joint standardised contractual frameworks governing access to specific datasets, and governance rules related to data sharing". They play a central role in FIDA. Rather than proposing a single standard for the interchange of financial data, the Commission puts the initiative in the hands of private sector led collective arrangements. We see many positive aspects to the proposal:

- It promotes a market-led approach to standards formulation.
- It permits the coexistence of multiple standards, which recognises the current reality that firms have already made significant investments in solutions that conform to existing standards.
- It avoids needlessly burdening the Commission or the Member States with the task of formulating standards in areas where they do not necessarily have sufficient subject matter expertise.

With that said, however, we have our doubts as to whether the approach is workable in exactly the form put forward in the current legislative proposal. The FIDA proposal seems to ignore the risks of market fragmentation and incompatible incentives, which could undermine the very objective of data sharing schemes.

While every data holder or data user is obliged to belong to at least one common financial data sharing scheme, sometimes a particular data holder and data user will not belong to *the same* financial data sharing scheme; in other cases, the data holder and data user have two or more financial data sharing schemes in common and could in principle choose the venue for a data transfer that corresponds to

either scheme, or for that matter to some other scheme. FIDA obliges the data holder to provide data "in a format based on generally recognised standards", but it does not provide a means for determining which of multiple standards (possibly including standards that have not been adopted by any financial data sharing scheme) should be used. Given that some incumbents would prefer not to share data at all, we see multiple risks on the standards deployment and adoption side: (1) the creation of standards might be subject to strategic blockades or "slow rolling"; (2) some parties may be motivated to promote relatively ineffective or inefficient standards; (3) data users might well feel compelled to accept data in any of a large number of standard formats, thus raising fixed costs in infrastructure development, and impeding the effectiveness of the scheme as a whole. This risk of incompatible incentives comes on top of the risk that the schemes do not keep pace with technological innovations.

FIDA seeks to guard against the first of these risks by empowering the Commission to create standards if there is no realistic prospect that they would otherwise emerge (Art. 11 FIDA). This is an important safeguard – Parliament should resist any natural temptation to water it down. But the other risks remain, largely due to a general lack of certainty as to which of multiple standards should be chosen. It is hard to judge in advance how serious a problem this is – for PSD2, about 80% of market players are said to have converged on a single API standard (the Berlin Group). But PSD2 does not have to deal with compensation issues for data, which are potentially far more divisive.

We do not see an easy fix, but we believe that the design of the financial data sharing schemes requires significant re-thinking at EU level, as well as ongoing attention by supervisory agencies.

Recommendation 28. *The inclusiveness and openness of data sharing schemes will be essential for the success of FIDA. The regulation needs to be clarified to explain which standards should be used for a transfer if the data holder and the data user do not belong to the same financial data sharing scheme. The clarification must carefully avoid a needless burden on either the data holder or the data user. Alternatively, a new approach to designing and implementing standards for data transfer may be needed.*

Recommendation 29*. FIDA urgently needs redesign as to how maximum charges are to be set in the case where the data holder and the data user do not belong to the same financial data sharing scheme.*

8.2. What should an ideal Open Finance framework look like?

Ultimately, the PSD2 benefits of an Open Finance framework in the EU stem from a combination of three key features in the regulation: (1) obligations on a wide range of incumbent data holder financial institutions to provide data and in some cases interoperability with an even wider range of incumbent and new third party financial data users; (2) standards that make interoperability and portability efficient, secure, respectful of consumer privacy, and cost-effective, including for cross-border operation; and (3) a compensation model that provides the right incentives to both data users and data holders across all key financial sectors.

In the implementation and in the further development of the EU Open Finance regime, three issues will therefore need to be kept in sight:

First, the time frame of the initial liberalisation. The digital economy thrives on scale of data use and multiple datasets being combined. This would suggest that data sharing arrangements should be introduced for all data categories at the same time, rather than phased in gradually. Cybersecurity is key and implementation of DORA is a precondition for wider data sharing.

Second, the further expansion of the scope of data covered. As a longer-term issue, we believe that greater integration between the payments framework established by PSR and PSD3 and the overall framework put in place by FIDA will ultimately be needed, but the Commission's approach of treating

this as a long term rather than an immediate goal is sensible. A more ambitious 'open data' architecture may also be desirable in the long term, in which case non-financial data can also be drawn on, for instance from utilities or telecoms providers. This calls for an architecture that is consistent with the other European data spaces, in particular that for industrial data.

Third, the openness to other jurisdictions. A significant risk relates to the use of financial data by institutions in countries that share values with the EU, such as the UK and the USA. As we explain in Section 5.5, transfers are currently permitted under GDPR adequacy decisions, but court challenges to these decisions should be expected. There are other countries whose values are largely in line with those of the EU; but for which no adequacy decision is in place. In the absence of an adequacy decision, it will be nearly impossible for an EU/EEA financial institution to share the personal data of an EU/EEA resident with a financial institution in a non-EU/EEA country. If there were to be an adverse court decision regarding a major trading partner, it might lead to a significant, abrupt disruption to trade.

Recommendation 30. *There is no sharp dividing line between payments-related data and other financial data. Ultimately, there should be a single legal framework for data sharing in banking and in other areas of finance.*

9. RECAPITULATION OF RECOMMENDATIONS

In this section, we re-state the recommendations that were developed in this report, along with the number of the page on which each recommendation first appeared.

REFERENCES

- Association for Financial Markets in Europe (2022), "Open Finance and Data Sharing", available at: https://www.afme.eu/key-issues/digital-finance.
- Croxson, K., J. Frost, L. Gambacorta and T. Valletti (2022), "Platform-based business models and financial inclusion", BIS Working Paper no. 986, available at: https://www.bis.org/publ/work986.pdf.
- McGuiness, M. (2023), "From open banking to open finance: what does the future hold?", speech at the European Parliament, available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_1819.
- OECD (2021): Enhancing access to and sharing of data, available at: https://www.oecd.org/sti/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm.
- Wandhöfer, R. and H. Nakib (2023), "Redecentralisation – building the digital financial ecosystem", Palgrave Macmillan.
- Association for Financial Markets in Europe (2022), "Guiding Principles for data sharing: a perspective for European Capital Markets", available at: https://www.afme.eu/key-issues/digital-finance.
- Bank of England (2019a), "The Future of Finance", available at: https://www.bankofengland.co.uk/report/2019/future-of-finance.
- Bank of England (2019b), "New economy, new finance, new Bank", available at: https://www.bankofengland.co.uk/-/media/boe/files/report/2019/response-to-the-future-of-finance-report.pdf.
- Bank of England (2020), "Open data for SME finance", available at: https://www.bankofengland.co.uk/paper/2020/open-data-for-sme-finance.
- Batasaikhan, U. and M. Demertzis (2018): "Financial literacy and inclusive growth in the European Union", Bruegel Policy Contribution, available at: https://www.bruegel.org/sites/default/files/wp_attachments/PC-08_2018.pdf.
- Batura, O.; Wion, A.; Marcus, J.S.; Godlovitch, I.; Wiewiorra, L. et al. (2023, forthcoming), "The emergence of non-personal data markets", study for the ITRE Committee of the European Parliament.
- Bazarbash, M. (2019), "Fintech in financial inclusion: machine learning applications in assessing credit risk", IMF Working Paper no. 19/109, available at: https://www.imf.org/en/Publications/WP/Issues/2019/05/17/FinTech-in-Financial-Inclusion-Machine-Learning-Applications-in-Assessing-Credit-Risk-46883.
- Beck, T. and A. Petit (2023), "Recent trends in UK financial sector regulation and possible implications for the EU, including its approach to equivalence", European Parliament Study, available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)740067.
- Borio, C., S. Claessens and N. Tarashev (2022), "Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big tech", Financial Stability Institute Occasional Paper no. 19, available at: https://www.bis.org/fsi/fsipapers19.htm#:~:text=The%20choice%20between%20EB%20and,entities%20causes%20that%20of%20activities.

- Carstens, A., S. Claessens, F. Restoy and H. Shin (2021), "Regulating big techs in finance", BIS Bulleting No. 45, available at: https://www.bis.org/publ/bisbull45.pdf.
- CEPR and IESE (2021), "The bank business model in the post-Covid-19 world", available at: https://media.iese.edu/research/pdfs/ST-0549-E.pdf.
- CEPR and IESE (2022), "Technology and finance", available at: https://media.iese.edu/research/pdfs/75956.pdf.
- Demertzis, M. and C. Martins (2023), "The value added of central bank digital currencies", Bruegel Policy Brief, available at: https://www.bruegel.org/policy-brief/value-added-central-bank-digital-currencies-view-euro-area.
- Di Maggio, M. and V. Yao (2020), "Fintech borrowers: lax screening or cream-skimming?", *The Review of Financial Studies,* v. 34, no. 10.
- EU Commission (2020a), "Final Report of the High-Level Forum on the Capital Markets Union", available at: https://finance.ec.europa.eu/publications/high-level-forum-capital-markets-union_en.
- EU Commission (2020b), Retail Payments Strategy, COM(2020) 592 final.
- EU Commission (2021), "Capital markets union: Commission adopts package to ensure better data access and revamped investment rules", available at: https://finance.ec.europa.eu/publications/capital-markets-union-commission-adopts-package-ensure-better-data-access-and-revamped-investment_en.
- EU Commission (2021), "Empowering EU capital markets for SMEs", Report of the Technical Expert Stakeholder Group on SMEs, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3858732.
- EU Commission (2022b), "Report on Open Finance", Expert Group on European Financial data space, available at: https://finance.ec.europa.eu/publications/report-open-finance_en#:~:text=The%20report%20on%20open%20finance,perspective%20of%20the%20Expert%20Group.
- EU Commission (2023), "Impact assessment report accompanying a proposal for a Directive of the European Parliament and of the Council", SWD (2023) 278 final, available at: https://finance.ec.europa.eu/publications/retail-investment-strategy_en.
- EU Commission (2023a), "Proposal for a regulation of the European Parliament and of the Council on a framework for financial data access", Com (2023) 360 final.
- EU Commission (2023ba), "Impact Assessment Report accompanying the proposal for a regulation of the European Parliament and Council on a framework for financial data access", SWD (2023) 224 final, Brussels, 28.6.2023.
- European Commission (2023c), "A study on the application and impact of directive 2015/2366 on Payment Services (PSD2), available at: https://www.ceps.eu/ceps-publications/a-study-on-the-application-and-impact-of-directive-eu-2015-2366-on-payment-services-psd2/
- European Financial Services Roundtable (2022): EFR Paper on PSD2 lessons and implications for open finance.

- European Systemic Risk Board (2022), "Will video kill the radio star – digitalisation and the future of banking", Report of the Advisory Scientific Committee, available at: https://www.esrb.europa.eu/pub/pdf/asc/esrb.ascreport202201_digitalisationandthefutureofbanking~83f079b5c7.en.pdf?87d77f9d8be17bcd1c5bacb79455b1f0.
- Farrell, J.; and Saloner, G. (1985), 'Standardization, compatibility and innovation', *RAND Journal of Economics* 16, 70-83.
- Goldfarb, A, and C. Tucker (2019), "Digital Economics", *Journal of Economic Literature,* vol. 57 (1), pp. 3-43.
- IDC & Lisbon Council (2023), "European Data Market Study, 2021-2023: D2.4 Second Report on Facts and Figures", available at: https://digital-strategy.ec.europa.eu/en/library/results-new-european-data-market-study-2021-2023.
- Katz, M.; and Shapiro, C. (1985), 'Network externalities, competition, and compatibility', *American Economic Review* 75, 424-440.
- Marcus, J.S. (2020), "New challenges to transfers of personal data from the EU to the United States", available at: https://www.bruegel.org/2020/07/new-challenges-to-transfers-of-personal-data-from-the-eu-to-the-united-states/.
- Marcus, J.S.; Martens, B.; Carugati, C.; Bucher, A.; and Godlovitch. I. (2022), "The European Health Data Space", study for the ITRE Committee of the European Parliament, available at: https://www.bruegel.org/report/european-health-data-space.
- McKinsey Global Institute (2021), "Financial data unbound: the value of open data for individuals and institutions", Discussion Paper, available at: https://www.mckinsey.com/industries/financial-services/our-insights/financial-data-unbound-the-value-of-open-data-for-individuals-and-institutions .
- Mills, S. (2019), "Open finance: an opportunity for financial services", speech delivered at the Investments and Savings Alliance, Financial Conduct Authority, available at: https://www.fca.org.uk/news/speeches/open-finance-opportunity-financial-services.
- Netherlands ACM (Authority for Consumers and Markets) (2022), "Market Study Cloud services"2, Document no. ACM/INT/440323, at: https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf.
- OECD (2022), "Financing SMEs and entrepreneurs 2022", available at: https://www.oecd.org/cfe/smes/financing-smes-and-entrepreneurs-23065265.htm.
- OECD (2023), "Shifting from Open Banking to Open Finance: Results from the 2022 OECD survey on data sharing frameworks", OECD Business and Finance Policy Papers, OECD Publishing, Paris, available at: https://doi.org/10.1787/9f881c0c-en.
- Polasik, M., A. Huterska, R. Iftikhar and S. Mikula (2020), "The impact of the payment services directive 2 on the PayTech sector development in Europe, *Journal of Economic Behavior and Organisation,* vol. 178, pp. 385-401.
- Stournaras, Y. (2019), "A new European landscape towards a unified credit market and the role of the credit bureau", speech at the ACCIS conference, available at: https://www.bis.org/review/r190816d.pdf.

- World Bank (2019), "Disruptive technologies in the credit information sharing industry: developments and implications", available at: https://documents1.worldbank.org/curated/en/587611557814694439/pdf/Disruptive-Technologies-in-the-Credit-Information-Sharing-Industry-Developments-and-Implications.pdf.

This study assesses the potential benefits, costs and risks of data sharing in the EU financial sector and implications for consumers, enterprises and the financial sector itself. We examine the coherence of a proposed regulation on financial data access with the broader EU data legislation and recommend a number of changes and modifications.

This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies at the request of the Committee on Economic and Monetary Affairs (ECON).

PE 754.188
IP/A/ECON/2023-05

Print ISBN 978-92-848-1202-8 | doi:10.2861/197064 | QA- 02-23-109-EN-C
PDF ISBN 978-92-848-1201-1 | doi:10.2861/479067 | QA- 02-23-109-EN-N