Volume 15
Issue 1 *Volume 15, Issue 1*

Article 5

6-2025

Building Open Finance

Douglas W. Arner
Faculty of Law, The University of Hong Kong

Ross P. Buckley
University of New South Wales

Christine M. Wang
Faculty of Law, University of Hong Kong

Dirk A. Zetzsche
Faculty of Law, University of Luxembourg

BUILDING OPEN FINANCE

Douglas W. Arner[*]
Ross P. Buckley[**]
Christine Menglu Wang[***]
Dirk A. Zetzsche[****]

[*] Kerry Holdings Professor in Law, RGC Senior Research Fellow in Digital Finance and Sustainable Development, Senior Fellow, Asia Global Institute, and Associate Director, HKU-Standard Chartered Foundation FinTech Academy, University of Hong Kong; Senior Fellow, Melbourne Law School, University of Melbourne; Visiting Professorial Fellow, Faculty of Law and Justice, UNSW Sydney.
[**] Australian Research Council Laureate Fellow, and Scientia Professor, School of Private and Commercial Law, UNSW Sydney.
[***] Post-doctoral Fellow, Faculty of Law, University of Hong Kong.
[****] Professor in Financial Law, ADA Chair in Financial Law (Inclusive Finance), Co-lead, National Centre of Excellence in Research in Financial Technology, and Coordinator, House of Sustainable Governance & Markets, Faculty of Law, Economics and Finance, University of Luxembourg.
The authors gratefully acknowledge the financial support of the Hong Kong Research Grants Council Senior Research Fellowship program, the Australian Research Council Laureate Fellowship (FL200100007), and the Luxembourg National Research Fund (FNR), grant reference NCER22/IS/16570468/NCER-FT. The views herein are solely the authors and not necessarily the views of these funding bodies.

ABSTRACT

As one of the most digitalized sectors of the economy, finance is increasingly dependent on data. Over the past decade, the implementation of Open Banking and Open Finance in an increasing number of major jurisdictions around the world, including the European Union (EU), the United Kingdom (UK), Australia, Brazil, and the United Arab Emirates (UAE), seeks to break down data silos, empower consumers, and increase competition among financial service providers, aiming to maximize the value of financial data for innovation, growth, and competitiveness. In addition to mandatory requirements, other governance approaches to Open Finance, including collaborative arrangements and voluntary initiatives, are emerging. For example, Singapore and Hong Kong are actively supporting the development of Open Finance through collaboration between regulators and industry, while both China and India are seeking to develop new approaches to making data available to support development, innovation, and competitiveness. In the United States (US), industry associations have promoted Open Finance practices, and a new mandatory rule from the Consumer Financial Protection Bureau (CFPB) on personal financial data rights is currently pending.

There are complex problems in the interaction between financial regulation and data governance in Open Finance. Customer data shared through an Open Finance system is both subject to financial regulatory requirements, such as rules governing the collection, processing, and use of financial data, and to the general governance framework for data protection. Furthermore, Open Finance initiatives adopted by different jurisdictions affect information sharing in domestic financial markets and in the cross-border transfer of financial data. The trend towards data localization and the asymmetry of data sharing leads to an unlevel playing field between market players, thereby exacerbating the problem of regulatory fragmentation in Open Finance regimes. Given the evolving nature of digital finance and the complexity of integrating data into its process, the main challenge is to develop appropriate governance approaches that can maximize the benefits of data sharing while mitigating new cross-cutting challenges in finance and data regulation.

Based on an analysis of experiences to date in leading

jurisdictions, we synthesize a range of policy strategies to address the complex interplay of financial regulation and data governance inherent in building Open Finance. These hold important lessons also for the US as it moves forward. The multi-disciplinary nature of Open Finance requires coordination between regulators and industry to ensure policy coherence and technical interoperability. Where financial and data regulatory regimes intersect, it is important to establish a collaborative forum and/or provide general guidance to facilitate a better understanding of Open Finance governance and improve consistency in regulatory action across sectors. In response to the increasing digitalization of the economy, there is also the need to expand the scope of data sharing from the financial sector to other industries, and thus move towards a broader Open Data framework.

Keywords: Open Banking, Open Finance, Open Data, Innovation, Competition, Financial Regulation, Competitiveness, Data Governance

I. INTRODUCTION

As societies, economies, and finance become increasingly dependent on data, countries around the world are exploring ways to maximize the value of data for innovation, competition, and competitiveness, particularly in finance.[1] Over the past decade, the implementation of Open Banking or Open Finance in a number of major jurisdictions, including the European Union (EU), the United Kingdom (UK), Australia, Brazil, and the United Arab Emirates (UAE), is emerging as one of the leading strategies, impacting both financial regulation and data governance. This approach aims to transform finance by breaking down data silos, empowering consumers through control of their data, and involving a wider range of market players.[2] It is hoped that a growing number of new entrants to the financial markets, including FinTechs, TechFins, and BigTechs, will support efficiency, consumer benefits, innovation, competitiveness, growth, and development through better use of

[1] Douglas W. Arner et al., *Financial Data Governance*, 74(2) HASTINGS L. J. 235, 238 (2023).

[2] Ariadne Plaitakis & Stefan Staschen, *Open Banking: How to Design for Financial Inclusion*, THE CONSULTATIVE GROUP TO ASSIST THE POOR 2-3 (Oct. 2020), https://www.cgap.org/sites/default/files/publications/2020_10_Working_Paper_Open_Banking.pdf.

data.

The primary objective of establishing a system of Open Finance is to enable individuals to provide access to their data held by traditional financial institutions to other financial industry incumbents, new entrants, and others. This is seen first as a direct and valuable benefit in providing customer control of their data, rather than leaving control (or even ownership) of data with traditional financial institutions, such as banks. Second, Open Finance is based on the premise that portability of data will not only empower consumers but also encourage competition, particularly as new entrants are able to access and maximize the benefits from customer data, in a process of "datafication," thus promoting competition and diversity of business models as well as new technologies in financial services and products. Third, Open Finance is designed to improve competition between incumbents and new players in the financial markets. Access to massive customer data is a substantial advantage to incumbent financial institutions in assessing risk and providing services, but also an obstacle for other competitors to expand their business.[3]

Sharing customer data through a system of Open Finance arguably could facilitate the entry of third-party service providers into the financial sector and reduce associated switching costs to mitigate the data lock-in problem. Open Finance thus seeks to empower data portability and use in an increasingly digitalized financial sector, as a key step in addressing natural economies of scope and scale in finance combined with the network effects of data, reducing anti-competitive practices, and supporting innovation in finance.

In terms of governance frameworks for Open Finance, a number of strategies are emerging, with mandatory requirements, collaborative arrangements, or voluntary initiatives so far, as the main implementation approaches.[4] For example, the EU has taken the leading role in adopting mandatory Open Banking, with the implementation of the Second Payment Services Directive (PSD2) in 2015, which mandates customer control of banking data, requires data sharing between banks and third-party service providers,[5] and

[3] SCOTT FARRELL, BANKING ON DATA: EVALUATING OPEN BANKING AND DATA RIGHTS IN BANKING LAW 3-4 (2023).
[4] Douglas W. Arner et al., *Open Banking, Open Data and Open Finance: Lessons from European Union*, in OPEN BANKING (Linda Jeng eds., 2022).
[5] 'Directive (EU) 2015/2366 of the European Parliament and of the Council of 25

intends to move to Open Finance (thus extending beyond banks with the Third Payment Services Directive (PSD3) as proposed in 2023.[6] The UK implemented this PSD2 framework up to the point of exiting the EU and has continued to follow a mandatory approach thereafter.[7] Australia, Brazil, and the United Arab Emirates (UAE) have also established mandatory Open Finance regimes through a series of rules and regulations. By comparison, Singapore and Hong Kong have not mandated Open Finance, but have provided guidance on how to make financial data available through application programming interfaces (APIs). More recently, financial regulatory requirements and data governance rules in China have had significant implications for the overseas listing of companies that possess large amounts of personal information and face potential risks in relation to national security.[8] Similarly, India is implementing a framework focused on aggregation of data while preventing centralization.

In the US, the access and exchange of customer data are contractual matters and thus industry associations are taking initiatives to unify the financial sector around common standards for data sharing.[9] Furthermore, a mandatory rule from the Consumer Financial Protection Bureau (CFPB) is currently pending.[10]

In the context of Open Finance, there are complex problems in relation to the interaction between financial regulation and data governance. At its core, data shared through a system of Open Finance is subject to financial regulatory requirements that are applicable to financial data, such as rules governing the collection, processing, and use of credit information, and is also subject to the

---

November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC' (2015) *Official Journal L* 337 35 [hereinafter The Second Payment Services Directive].

[6] *Modernizing Payment Services and Opening Financial Services Data: New Opportunities for Consumers and Businesses*, EUR. COMM'N (Jun. 28, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543.

[7] The Retail Banking Market Investigation Order 2017 (Competition & Mkts. Authority) (U.K.), https://assets.publishing.service.gov.uk/media/5a759cc7ed915d506ee80283/retail-banking-market-investigation-order-2017.pdf.

[8] Wangluo Anquan Shencha Banfa (网络安全审查办法) [Measures for Cybersecurity Review] (promulgated by the Cyberspace Admin. of China and 12 other Dep'ts. and Comm'ns. on Dec. 28, 2021, effective Feb. 15, 2022), art. 7.

[9] Arner et al., *supra* note 1, at 261-62.

[10] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796 (Oct. 31, 2023) (to be codified at 12 C.F.R. pts. 1001 and 1033).

general regulatory regime for data security and information protection. [11] Thus, particular concerns can arise from the simultaneous but uncoordinated implementation of these regulatory regimes leading to regulatory conflicts. For example, full access to and sharing of personal financial information can be limited by the principles of data minimization and necessity under privacy regulation, thereby potentially undermining the effectiveness of an Open Finance regime. Furthermore, as one of the most globalized and digitalized industries, finance depends heavily upon data, especially cross-border data transfers. Open Finance regimes adopted by different jurisdictions will not only affect information sharing in their domestic financial markets but may well also impact cross-border data flows. Given the evolving nature of digital finance and the complexity of integrating data into its processes, it is essential to develop appropriate governance frameworks that can maximize the benefits of data sharing while addressing new challenges in both financial and data regulation.

The remainder of the paper proceeds as follows. Part II discusses the digitalization of financial services and its implications for the development of Open Finance. Part III presents a comparative analysis of governance frameworks for Open Finance, including mandatory, collaborative, and market-led approaches. Part IV examines the challenges of Open Finance governance in relation to regulatory fragmentation, data localization rules, and asymmetric data sharing. Part V considers how to build Open Finance, focusing on governance and the shift to Open Data. The final Part concludes.

II. THE DEVELOPMENT OF OPEN FINANCE

Finance has evolved over the past five decades into one of the most digitalized and globalized industries, as well as one of the most regulated. In the modern period of FinTech, since 2008, digital innovations, such as artificial intelligence, big data, cloud computing, and distributed ledger technology, are transforming the way traditional financial businesses operate and thus present great opportunities for new entrants to the market.[12] These developments have increased access to large amounts of customer data that can be used to improve risk management, service efficiency, product

[11] Arner et al., *supra* note 1, at 240-41.
[12] Erik Feyen et al., *Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy*, BANK FOR INT'L. SETTLEMENTS (Jul. 13, 2021), https://www.bis.org/publ/bppdf/bispap117.pdf.

diversification, and other related areas of finance. In this way, financial activities involving a wide range of incumbent and new market players are inextricably intertwined with the collection, processing, and analytics of massive data.

A. THE DIGITALIZATION AND DATAFICATION OF FINANCE

Financial market interactions between different service providers and customers are characterized by risk, with information asymmetries a significant source.[13] For example, a lack of information on creditworthiness will increase risk in lending, and investors in capital markets may suffer huge losses without access to and analysis of relevant trading information. Data in all its forms, including traditional financial information about customers and alternative data sourced from diverse online activities, is therefore at the core of evolving digital finance. The increasing integration of data with finance has significantly changed existing market practices and facilitated the development of new business models, ranging from mobile payments, crypto assets, and platform-based ecosystems of financial services to bespoke products tailored to different customer needs. Thus, data is not just information about market participants and transactions, but also an important driving force behind the digital transformation of finance. This digitalization and datafication process is extending the frontiers of financial services while posing some legal and regulatory challenges. The growing amount of data from traditional financial institutions and third-party service providers, coupled with the use of new technologies, makes it imperative to regulate the integration of data and finance.

The main objectives of financial regulation are to maintain financial stability, both through the safety of individual financial institutions as well as the stability of the entire system, support a stable monetary and payment system as a public good, enhance efficiency, protect customers, depositors and investors (including against fraud and misconduct), address issues of market integrity (particularly monetary laundering and terrorist financing), as well as a range of developmental objectives including growth, innovation, competitiveness, competition, and sustainable development.[14] In the

---

[13] *Id.* at 2.

[14] *Big Tech in Finance: Opportunities and Risks*, BANK FOR INT'L. SETTLEMENTS 68 (2019), https://www.bis.org/publ/arpdf/ar2019e3.pdf.

context of digital finance, the entry of data-intensive companies, including FinTechs, TechFins, and BigTechs, into financial services, as well as the synergies of data analytics and emerging technologies, require the coordination of multiple regulatory and policy objectives that extend beyond traditional financial regulation, such as market competition, data security, and privacy protection.[15] There is a need to improve access to customer data for financial service providers to promote market competition and financial integrity and inclusion, while protecting data from unauthorized use and cyberattacks. The complex intersection of these regulations and policies is exemplified by Open Finance initiatives adopted in many jurisdictions.

B. OPEN BANKING AND OPEN FINANCE: EVOLUTION

Open Finance is an evolving trend around the world, and a commonly accepted definition of the practice is yet to evolve. In practice, the term mainly refers to a series of customer-permissioned data-sharing arrangements between financial institutions and third-party service providers. Open Finance can include management tools that consolidate all of an individual's financial information into one dashboard, seamless payment transfers between different bank accounts, and the provision of innovative financial services by third parties.[16] Basically, the implementation of Open Finance initiatives both requires the consent of customers as well as empowers consumers to share their financial data with a range of third-party service providers, such as other financial institutions, FinTechs, and BigTechs. As the technical foundation of Open Finance, the widespread use of APIs enables customer data to be securely transferred between financial service providers.[17] In this way, authorized third parties can aggregate customer data from a number of bank accounts to develop innovative financial services and products that meet different market needs.

Open Banking and Open Finance initiatives have been implemented in a number of jurisdictions, starting with the EU (including at the time, the UK), followed by Australia, Brazil, and others. Open Banking is a data sharing scheme between banks and

---

[15] *Id.* at 69.
[16] *Report on Open Banking and Application Programming Interfaces*, BANK FOR INT'L. SETTLEMENTS 8 (Nov. 19, 2019), https://www.bis.org/bcbs/publ/d486.pdf.
[17] Oscar Borgogno & Giuseppe Colangelo, *Data Sharing and Interoperability: Fostering Innovation and Competition through APIs*, 35(5) COMPUT. L. & SEC. REV. 105314, 20 (2019).

third-party service providers, intended to significantly change traditional business models in the financial sector and present the potential to usher in an ecosystem covering a wider range of market players. Thus, Open Banking seeks to create an environment conducive to service innovation and market competition, while improving financial inclusion and customer experience.[18] Open Finance extends beyond just banks to other financial services providers, whereas Open Data extends beyond the financial sector, with the objective of data portability across an economy, to maximize the benefits of data both to individuals as well as to the economy and society.

From the perspective of competition, banks have traditionally controlled vast amounts of customer data, which gives them an important advantage in developing financial products and services and constitutes a barrier to new market players. Open Banking can provide authorized third parties with secure and seamless access to customer data and enable them to deliver competing financial services, thus addressing the data lock-in problem and reducing the associated switching costs.[19] Open Finance extends this across the financial sector. In this way, there will be growing competition in the financial sector, especially as data and data-driven technologies become ever more integral to digital finance. Furthermore, Open Finance brings great opportunities for innovation for incumbents and new entrants alike. The use of cutting-edge technologies allows traditional financial institutions to reinforce the economies of scale and scope of their existing businesses.[20] Coupled with increasing access to customer data, the broad participation of FinTechs, TechFins, and BigTechs in financial markets has facilitated the development of new business models and inclusive services. These digital innovations enabled through the Open Finance ecosystem are transforming the way customers interact with different service

---

[18] Fredesvinda Montes Herraiz & Luis Maldonaldo, *Technical Note on Open Banking: Comparative Study on Regulatory Approaches*, THE WORLD BANK 6-7 (May 25, 2022), https://documents1.worldbank.org/curated/en/099345005252239519/pdf/P164770008e2c670fe0835a0e8692b499c2a.pdf.

[19] Oscar Borgogno & Giuseppe Colangelo, *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, 31(4) EUR. BUS. L. REV. 573, 597 (2020).

[20] Mark Carney, the former Governor of the Bank of England, delivered a speech on 'Building the Infrastructure to Realize FinTech's Promise' at the International FinTech Conference 2017 (Apr. 12, 2017), https://www.bankofengland.co.uk/-/media/boe/files/speech/2017/building-the-infrastructure-to-realise-fintechs-promise.pdf.

providers and unlocking the potential of data in the financial sector.

Open Finance, premised on access to massive customer data, empowers an increasing number of new players to enter the financial sector and supports innovation in services and products tailored for the needs of unbanked and underserved segments. These competitive and innovative activities can promote financial inclusion and strengthen system resilience with greater diversity.[21] The exchange and analysis of customer data sourced from many different participants in the Open Finance ecosystem improves the performance of existing financial businesses and also expands the range of innovative services offered by third parties. Therefore, customers, especially those marginalized by the traditional financial sector, will be among the main beneficiaries of Open Finance services. In addition, customers' greater control over the type and scope of data shared can enhance their bargaining power with large and established financial service providers, thus better protecting their rights and interests.

Furthermore, the use of standardized APIs in Open Finance is designed to mitigate the cybersecurity and customer protection risks arising from traditional data aggregation techniques employed by third-party service providers, such as screen scraping and reverse engineering.[22] These traditional techniques require customers to provide their authentication credentials, including usernames and passwords, to access their accounts and execute financial transactions.[23] In this case, customer data can be easily stolen or misused. The growing adoption of APIs facilitates real-time communication between banks and third-party service providers without human intervention, allowing them to share data in a more secure and stable manner.

Different jurisdictions are pursuing varied governance approaches to Open Finance, ranging from mandatory requirements, collaborative arrangements to voluntary initiatives.[24] Under the mandatory framework adopted by the EU, the UK, Australia, and Brazil, a series of regulatory rules have been introduced, requiring financial institutions to share customer data with authorized third parties through APIs and setting relevant standards for user digital identity. More recently, the UAE has established a regulatory

---

[21] Plaitakis & Staschen, *supra* note 2, at 6-7.
[22] BANK FOR INT'L. SETTLEMENTS, *supra* note 16, at 9.
[23] *Id.*
[24] Arner et al., *supra* note 4.

framework for the licensing, operating, and supervising of Open Finance, aiming to facilitate cross-sectoral sharing of customer data and financial transaction initiation.[25]

By comparison, Singapore and Hong Kong are characterized by active regulatory guidance and engagement in Open Finance initiatives, but without legislative mandates. In China, data is treated as an important factor of production,[26] and there is no specific legislation requiring financial institutions to share customer data with third-party service providers. The Chinese government issued recommended industry standards for security management of commercial bank APIs[27] and an implementation plan to encourage the establishment of information sharing platforms.[28] These guidelines contribute to the development of a basic governance framework for Open Finance. Likewise, India has developed Account Aggregators to manage the collection of and access to customer data with express consent, which creates a level playing field for new entrants to financial services.[29]

In the US, Open Finance is an industry-led voluntary strategy and the CFPB is proposing to implement rules that require covered entities (such as banks) to make transaction and account data available to consumers and authorized third parties and provide

---

[25] *CBUAE Issues the Open Finance Regulation to Ensure the Soundness and Efficiency of Services and Promote Innovation and Competitiveness,* CENT. BANK OF THE UNITED ARAB EMIRATES (Jun. 27, 2024), https://www.centralbank.ae/media/rxfeelkt/cbuaei-2.pdf.

[26] Guanyu Goujian Shuju Jichu Zhidu Genghao Fahui Shuju Yaosu Zuoyong de Yijian (关于构建数据基础制度更好发挥数据要素作用的意见) [Opinions on Building Basic Systems for Data and Putting Data to Better Use], CENT. COMM. OF THE CHINESE COMMUNIST PARTY AND THE STATE COUNCIL (Dec. 19, 2022), https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm (China).

[27] Shangye Yinhang Yingyong Chengxu Jiekou Anquan Guanli Guifan (商业银行应用程序接口安全管理规范) [Commercial Bank Application Programming Interface Security Management Specifications], THE PEOPLE'S BANK OF CHINA (Feb. 13, 2020), https://aibank.com/upload/attachs/2022/12/14-商业银行应用程序接口安全管理规范.pdf. (China).

[28] Jiaqiang Xinyong Xinxi Gongxiang Yingyong Cujin Zhongxiaowei Qiye Rongzi Shishi Fangan (加强信用信息共享应用促进中小微企业融资实施方案) [Implementation Plan for Promoting the Sharing and Use of Credit Information and Improving Financing of Micro, Small and Medium Enterprises], GENERAL OFFICE OF THE STATE COUNCIL (Dec. 22, 2021), https://www.gov.cn/zhengce/content/2021-12/29/content_5665109.htm. (China).

[29] Rajeshwar Rao, Deputy Governor of the Reserve Bank of India, made remarks titled 'Regulatory framework for account aggregators' during a virtual event organized by Indian Software Products Industry Round Table (Sep. 2, 2021), https://www.bis.org/review/r210916e.htm.

basic standards for data access.[30]

Thus, Open Finance initiatives take different forms in a number of jurisdictions, each designed to maximize the benefits of financial data sharing while mitigating risks associated with security and compliance.

III. OPEN FINANCE GOVERNANCE FRAMEWORKS

The implementation of Open Finance involves the full range of market participants, including financial institutions, third-party service providers, and customers. Furthermore, it requires a range of data-driven technologies, and more importantly, regulatory engagement by setting relevant standards and rules to bring significant benefits for its development. It also requires increased interaction between financial regulation and data governance. Based on the scale of participation, the scope of data sharing, and the degree of technical standardization, this Part considers the main designs for Open Finance governance which are evolving.

A. MANDATORY APPROACH

Data sharing between incumbent financial institutions and new third-party service providers is one of the key aspects of Open Finance, and thus adequate protection of such data and the underlying technology applications is important. In this context, a range of jurisdictions, including the EU, the UK, Australia, Brazil, and the UAE, have established a governance framework for Open Finance by introducing a series of mandatory rules. The regulation of Open Finance activities varies between these jurisdictions, but generally covers the requirements for data access by different parties, customer consent, and privacy, and data security. The development of APIs and their technical standards is also a matter of concern for regulators.

Generally speaking, after a decade of experience, it appears that jurisdictions mandating Open Banking or Open Finance are seeing the greatest impact in the context of empowering consumers, data, new entrants, and business models.

1. EUROPEAN UNION

With the implementation of the PSD2 in 2015, the EU adopted

[30] Required Rulemaking on Personal Financial Data Rights, *supra* note 10.

mandatory Open Banking rules, requiring banks to share their customer data with third-party service providers. Specifically, the PSD2 applies to payment institutions that have been granted authorization to provide and execute payment services, as well as providers of payment initiation services and account information services that do not hold user funds.[31] To facilitate the provision of payment services across the EU states, there are rules governing the access to payment accounts and the use of account information.[32] The PSD2 provides a stable regulatory framework for Open Banking and imposes an obligation on banks to share data with providers of payment initiation services and account information services through a secure interface. This obligation creates a level playing field between incumbents and new payment service providers and helps financial innovation to reach a wider market. In terms of the scale of participation, the EU's existing regulatory framework for Open Banking primarily focuses on data access by service providers at different stages of the payment chain. More recently, the European Commission has proposed amendments to the PDS2, aiming to improve the functioning of Open Banking and facilitate the entry of new innovative services in the market.[33] This proposal (the PSD3) will bring the financial sector into the wider Open Finance framework.

A. SCOPE OF DATA SHARING

The scope of customer data that can be shared is the foundation of the governance framework for Open Banking. Generally, data sharing between financial institutions and authorized third parties contains customer information on different bank accounts. Specifically, in the EU, the PSD2 applies to payment accounts that are held in the name of one or more consumers and used for the execution of payment transactions.[34] The European Commission has recently put forward a legislative proposal for a broader Open Finance framework to improve access to customer data beyond the scope of the PSD2, which covers data on loans, savings, investments, occupational and personal pension schemes, and non-life insurance

[31] The Second Payment Services Directive, *supra* note 5, arts. 4(4), (18)-(19).
[32] *Id*. arts. 66-67.
[33] EUR. COMM'N, *supra* note 6.
[34] The Second Payment Services Directive, *supra* note 5, arts. 4(12).

products.[35]

B. DEGREE OF TECHNICAL STANDARDIZATION

In the EU, the banking supervisor is responsible for the implementation and governance of Open Finance. The PSD2 provides a stable regulatory framework for access to payment accounts, requiring banks to share their customer data with authorized third parties through a secure interface. While it does not specify technical standards for the use of APIs, a series of industry-led specifications have emerged, such as the Berlin Group, [36] STET, [37] and PolishAPI. [38] These specifications provide the European payment industry with a range of technical solutions to ensure better compliance with the PSD2 regulatory requirements. Since there is no unified technical standard, the adoption of different API specifications is determined by individual banks and third-party service providers.

Supplementing the PSD2, the EU has mandated specific requirements for payment service providers to apply the procedure of strong customer authentication, protect the confidentiality and integrity of the user's personalized security credentials, and establish common and secure open standards for communication.[39] Under this regulation, account servicing payment service providers

---

[35] 'Proposal for a Regulation of the European Parliament and of the Council on a Framework for Financial Data Access and Amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) No 2022/2554' COM (2023) 360 final, art. 2.

[36] The 'Berlin Group' is a pan-European payments interoperability standards and harmonization initiative with the primary objective of defining open and common scheme. *See openFinance API framework*, THE BERLIN GROUP, https://www.berlin-group.org/open-finance (last visited Jul. 23, 2024).

[37] STET is formed by a group of major French banks to provide the European payment industry with harmonized solutions. STET released an open API to specify different interactions between third-party providers and account servicing payment service providers for carrying out the use cases of PSD2. *See PSD2 API V1.6*, STET, https://www.stet.eu/en/psd2/ (last visited Jul. 23, 2024).

[38] The PolishAPI standard is an essential part of Open Banking in the Polish financial market. It defines the interface that enables third parties to access payment accounts. *Specification of an Interface for the Needs of Services Provided by Third Parties on the Basis of Access to Payment Accounts*, THE POLISHAPI PROJECT GROUP (Dec. 12, 2019), https://polishapi.org/wp-content/uploads/2019/12/PolishAPI-specification-v3.0.pdf.

[39] 'Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication' (2018) *Official Journal L* 69 23.

shall establish dedicated interfaces used for authentication and communication, and ensure the same level of availability and performance of these interfaces.[40] There are also contingency measures if the dedicated API is unavailable or does not perform properly.[41] In addition, the proposed PSD3 will impose substantial requirements on dedicated data access and sharing APIs, aiming to standardize customer data and ensure high quality interfaces.[42] Therefore, banks and other payment account providers will be required to create a dashboard that allows consumers to see what data access they have granted in Open Banking and to whom.[43]

Looking forward, the EU is focusing on expanding from Open Banking to Open Finance and, eventually, to Open Data.

1. UNITED KINGDOM

The UK's Open Banking, initiated by the Competition and Markets Authority (CMA) in 2017, is an important step towards promoting competition in retail banking services. The CMA ordered the nine largest current account providers (the CMA9) to set up the Open Banking Implementation Entity (OBIE) responsible for developing and implementing relevant standards.[44] Under this regulatory regime, authorized third parties are allowed to access personal and business current account information or to initiate a payment on behalf of customers.[45] The OBIE supports account providers, FinTechs, and technical service providers seeking to join the UK's Open Banking system and maintains a directory of participants to facilitate sharing of customer-permissioned data in a secure manner. In the UK, account servicing payment service providers (ASPSPs), including banks, building societies and payments companies, are fundamental to the implementation of Open Banking. According to relevant regulations, ASPSPs are entities authorized to provide and maintain payment accounts for

---

[40] *Id*. arts 31-32.
[41] *Id.* art 33.
[42] *Payment Services: Revised Rules to Improve Consumer Protection and Competition in Electronic Payments*, EUR. COMM'N (Jun. 28, 2023), https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3544.
[43] *Id.*
[44] The Retail Banking Market Investigation Order 2017, *supra* note 7, art. 10.
[45] *Id.*

their customers.[46] The UK's Open Banking ecosystem currently extends beyond the CMA9 and comprises hundreds of regulated third-party providers, which mainly deliver financial decision-making, payment and borrowing services to a broad range of digitally enabled consumers and small businesses.[47]

A. SCOPE OF DATA SHARING

Under the UK's existing regulatory framework, there are similar requirements to the EU for the types of customer accounts that can share data. The CMA mandates access to relevant information on personal current accounts, business current accounts, and small and medium-sized enterprises (SMEs) lending products.[48] For example, personal current accounts are marketed to individuals to place funds, withdraw cash, hold deposits and execute payment transactions, and business current accounts are offered to business customers to make and receive payments and to manage cash flows.[49] The *Payment Services Regulations 2017* expand the scope of Open Banking by providing access to payment accounts.

B. DEGREE OF TECHNICAL STANDARDIZATION

In line with the UK regulations, the OBIE has established API standards for the CMA9 and other participants in Open Banking to facilitate customer-permissioned data sharing.[50] Specifically, these technical standards consist of different types of specifications, covering read/write API, open data API, directory, dynamic client registration, and management information reporting. The read/write APIs enable third-party providers to access information and initiate payments in a secure and efficient manner, and the open data APIs allow the development of endpoints, mobile and web applications for banking customers.[51] The Open Banking directory contains

---

[46] The Payment Services Regulations 2017 (U.K. Statutory Instruments 2017 No. 752), art. 2, https://www.legislation.gov.uk/uksi/2017/752/contents.
[47] *The Open Banking Impact Report*, OPEN BANKING LTD. (Oct. 19, 2023), https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-october-2023/.
[48] The Retail Banking Market Investigation Order 2017, *supra* note 7, art. 12.
[49] *Id.* art. 9.1.
[50] *Id*. art. 10.2.
[51] *See API Specifications Version 4.0*, OPEN BANKING LTD., https://standards.openbanking.org.uk/api-specifications/latest/ (last visited Jul. 23, 2024).

technical information about the roles and functions of each participant and supports interactions between banks and authorized third parties via APIs.[52] Moreover, the OBIE has issued guidelines on the roles and responsibilities of participants in Open Banking.[53] For example, there are security standards for the use of APIs, data access and handling, credentials management, and fraud controls, as well as procedures for payment service providers to enroll and operate with the Open Banking ecosystem.

Following Brexit, the UK replaced EU regulations with new technical standards on strong customer authentication and common and secure methods of communication,[54] which outline general obligations for access interfaces used by payment service providers. Further, the OBIE has developed operational guidelines to help payment service providers design effective and high-performing APIs while ensuring their compliance with regulatory requirements.[55] It defines key indicators for availability and performance of dedicated interfaces, provides guidance on how to design, test, and change APIs in accordance with regulations, and outlines policies, processes, and systems for problem resolution.

2. AUSTRALIA

In May 2018, the Australian government introduced the Consumer Data Right (CDR), designed as an economy-wide data-sharing regime, which enables the safe and secure transfer of consumer data through an automated system.[56] The CDR's roll-out commenced in the banking sector (where the CDR is referred to as 'Open Banking') and customers can choose to share their banking data with third parties that have been accredited by the Australian

---

[52] *Id.*

[53] *Open Banking Guidelines for Read/Write Participants*, OPEN BANKING LTD. (May 2018), https://www.openbanking.org.uk/wp-content/uploads/Guidelines-for-Read-Write-Participants.pdf.

[54] *Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication Instrument 2020*, FIN. CONDUCT AUTHORITY (Nov. 26, 2020), https://www.handbook.fca.org.uk/instrument/2020/FCA_2020_70.pdf.

[55] *See Operational Guidelines*, OPEN BANKING LTD., https://standards.openbanking.org.uk/operational-guidelines/latest/ (last visited Jul. 23, 2024).

[56] *See The Consumer Data Right*, AUSTL. COMPETITION & CONSUMER COMM'N., https://www.accc.gov.au/by-industry/banking-and-finance/the-consumer-data-right (last visited Jul. 23, 2024).

Competition and Consumer Commission (ACCC).[57] Under the CDR framework, consumers have greater control over their data and increased access to financial services and products that better match their needs.[58] As designated data holders, all Australian banks are required to participate in the CDR and share their data with accredited data recipients if requested by consumers.[59] The CDR's framework legislation, Part IVD of the *Competition and Consumer Act*, states that a person who holds one or more classes of information specified in the designation instrument is a CDR data holder and subject to sharing obligations.[60] At the time of writing, the regime has designated data holders in the banking, energy, telecommunication, and nonbank lending sectors.[61] Third parties seeking to access and use consumer banking data must, as a rule, apply for (at least restricted) accreditation and demonstrate compliance with relevant CDR requirements.[62] The ACCC is responsible for assessing the application process and maintaining an accreditation register.[63]

A. SCOPE OF DATA-SHARING

The Australian regulatory regime covers customer accounts

---

[57] Note, however, that as the regime progressed, data-sharing also became possible with third parties that do not require accreditation, *see* ANTON DIDENKO, NATALIA JEVGLEVSKAJA AND ROSS BUCKLEY, CUSTOMER DATA SHARING FRAMEWORKS: TWELVE LESSONS FOR THE WORLD, 17 (2024).

[58] Competition and Consumer Act 2010 Austl. Compilation No. 140/2010, s. 56AA https://www.legislation.gov.au/C2004A00109/2022-07-01/text.

[59] Competition and Consumer (Consumer Data Right) Rules 2020 Austl. Compilation No. 8/2020, sched. 3, https://www.legislation.gov.au/F2020L00094/latest/text.

[60] Competition and Consumer Act 2010, *supra* note 58, s. 56AJ.

[61] ANTON DIDENKO, JEVGLEVSKAJA & ROSS BUCKLEY, CUSTOMER DATA SHARING FRAMEWORKS: TWELVE LESSONS FOR THE WORLD, *supra* note 57, at 9. *Consumer Data Right: Non-bank Lending Sectoral Assessment*, U.S. DEP'T OF THE TREASURY (Aug. 2022), https://treasury.gov.au/sites/default/files/2022-08/p2022-300402-finalreport.pdf.

[62] Competition and Consumer Act 2010, *supra* note 58, s. 56AK. Note that third parties can obtain two levels of accreditation under the CDR regime: the highest level, known as unrestricted, and the sponsored level, which imposes certain limitations on the third party's involvement in the CDR system. Besides, under circumstances, certain non-accredited entities, such as 'trusted advisers', 'the CDR representatives' and such persons as may be specified by 'business consumers', can also get access to the CDR regime, see Competition and Consumer (Consumer Data Right) Rules 2020 (Austl. Compilation No. 8), rr 1.10AA, 1.10A(9), 1.10A(11) and 1.10C, https://www.legislation.gov.au/F2020L00094/latest/text.

[63] *Id.* s. 56CE.

within the banking sector and beyond, and thus can be characterized as Open Finance, extending into Open Data with its application to energy. The CDR rules apply to different types of bank products, such as savings accounts, current accounts, debit card accounts, credit or charge card accounts, home loans, mortgage accounts, personal loans, business finance, overdrafts, and asset finance.[64] The regulation also clarifies the meaning of customer data, account data, transaction data, and product specific data that is subject to the Open Finance framework.[65] Furthermore, as indicated above, the regime has been extended beyond Open Finance to other areas, including the energy, telecommunication, and nonbank lending sectors (although the roll-out in telecommunications was paused in mid-2023, to allow the CDR to mature in finance and energy first).[66] As a result, customers can also request data on their electricity accounts to facilitate credit assessments. This broader sharing of accounts and data is designed to improve the effectiveness of Open Finance in Australia.

B. DEGREE OF TECHNICAL STANDARDIZATION

Under the Australian regulatory framework, a Data Standards Chair and a Data Standards Advisory Committee have been established to review, develop, and amend relevant data standards.[67] The Chair is required to make one or more binding data standards that cover the processes for requesting data and obtaining authorizations, the collection, use, disclosure, security, types, and formats of CDR data, the requirements in relation to performance and availability of systems and public reporting of compliance information, and the provision of ancillary services for communications between CDR participants.[68] After consultation with the ACCC and the Office of the Australian Information Commissioner (OAIC) who enforces the Privacy Safeguards and the privacy related CDR rules (see section IV.A below), a set of technical standards such as APIs, data schemes, and security

[64] Competition and Consumer (Consumer Data Right) Rules 2020, *supra* note 59, sched. 3 cl. 1.4.
[65] *Id.* sched. 3 cl. 1.3.
[66] Australian Government, Federal Budget (26 May 2023) Consumer Data Right Newsletter, https://mailchi.mp/f43e9452f613/consumer-data-right-newsletter-26-may-2023.
[67] *Supra* note 59, at pt. 8 cl. 8.1.
[68] *Supra* note 59, at pt. 8 cl. 8.11.

measures have been published to support the implementation of Open Finance. For example, there are foundational and generally applicable technical principles for API definitions and development, as well as detailed specifications for APIs that expose different endpoints to obtain the CDR data.[69] These standards improve the consistency and compatibility of APIs, facilitating secure and efficient data-sharing between participants in the Australian Open Finance ecosystem. Importantly, using unified data standards can address interoperability problems caused by banks and authorized third parties choosing different technical standards. As part of the governance framework, nonbinding standards have also been developed to facilitate voluntary extensions for CDR implementation.

3. BRAZIL

The Banco Central do Brasil (BCB) carried out public consultation on regulatory proposals for the implementation of Open Banking in August 2019, and several months later issued a resolution setting out the scope of participation and services, as well as requirements for data sharing and responsibilities.[70] Under this governance structure, financial institutions, payment institutions and other entities licensed by the BCB can participate in the Open Banking ecosystem and share data with customer consent. [71] Depending on the data and services shared, there is mandatory and voluntary participation for different types of institutions. Specifically, customer data sharing is mandatory for universal banks, commercial banks, investment banks, foreign exchange banks, and federal saving banks of a certain size; in terms of services shared, participation in Open Banking is also mandatory for account service providers, payment initiation service providers, and institutions that have domestic correspondent agreements to receive and forward

[69] Consumer Data Standards have been developed as part of the introduction of the CDR legislation and act as a specific baseline for the implementation of Open Banking in Australia. *See* CONSUMER DATA STANDARDS, https://consumerdatastandardsaustralia.github.io/standards/#introduction (last visited Jul. 23, 2024).

[70] Joint Resolution No. 1, dated May 4th, 2020, provides for the implementation of Open Banking (Braz.), https://www.bcb.gov.br/content/config/Documents/Open_Banking_Regulation_Joint%20Resolution_No_1_Updated.pdf.

[71] *Id.* art. 1.

loan proposals by electronic means.[72] The sharing of data and services is voluntary for other financial and payment institutions, subject to the provision of dedicated APIs and the registration of their participation in Open Banking. In addition, Brazil allows the partnership between institutions authorized to operate by the BCB and non-regulated entities to share data and services covered by Open Banking.[73] The implementation of Open Banking in Brazil is gradual, taking place in four phases based on the specific type of data and services shared.

A. SCOPE OF DATA SHARING

In Brazil, the Open Banking regulatory regime comprises the sharing of data on products, services and customer transactions related to deposits accounts, savings accounts, payment accounts, credit operations, foreign exchange operations, investment, insurance and open pension funds, and also the sharing of services for initiating payment transactions and forwarding loan proposals.[74] The BCB does not restrict the scope of data sharing to banking and/or payments, but covers many types of financial services. While some of these services are not under the BCB's jurisdiction, Brazil's regulations provide an inclusive and competitive environment for different financial institutions to share customer data.

B. DEGREE OF TECHNICAL STANDARDIZATION

The BCB requires institutions participating in Open Banking to make dedicated interfaces available for data and services sharing.[75] Participating institutions are required to draft and commit themselves to a convention that contains technical standards, operational procedures, security standards and certificates,

---

[72] *Id.* art. 6; Resolution No. 4,553, dated January 30th, 2017, establishes the segmentation of financial institutions and other institutions licensed by the Central Bank of Brazil for the purpose of proportional implementation of prudential regulation (Braz.), art. 2, https://www.bcb.gov.br/content/financialstability/Brazilian_Prudential_Financial_Regulation_Docs/ResolutionCMN4553.pdf; Resolution No. 3,954, dated February 24th, 2011, amends and consolidates rules on hiring domestic correspondents (Braz.), art. 8, https://www.bcb.gov.br/nor/denor/resolution_cmn_3954_english.pdf.

[73] Joint Resolution No. 1, *supra* note 70, art. 36.

[74] *Id.* art. 5.

[75] *Id.* art. 23.

implementation of dedicated APIs, data and services layout, and other related provisions.[76] While the BCB does not directly formulate this convention, it coordinates the initial self-regulatory efforts of participating institutions to ensure their compliance with Open Banking regulations. The industry-led convention and its revisions are also subject to the BCB's approval.[77] In addition, the BCB has issued specific normative instructions covering the scope of data and services, APIs, services provided by the Open Banking governance structure, security, and client experience.[78] The API-related instruction provides additional functionality to facilitate access to different types of customer-permissioned data and services, such as registration data, credit card, accounts, and credit operations.[79] Brazil has also created a testing environment for Open Banking APIs under a sandbox regime to verify their security and functional compliance.

4. UNITED ARAB EMIRATES

In 2023, the Central Bank of the UAE (CBUAE) launched a Financial Infrastructure Transformation Program aimed at promoting digitalization and innovation in the financial services sector.[80] The CBUAE has recently issued Open Finance Regulation to develop a comprehensive framework for the licensing, supervision, and operation of relevant services and to improve cross-sectoral data sharing in the financial system.[81] Participation in the UAE's Open Finance framework is mandatory for a number of licensees, including banks, finance companies, payment service and systems providers, exchange houses, loan-based crowdfunding companies, insurance brokers and companies, and other financial

---

[76] *Id.* art. 44.
[77] *Id.* arts. 46-47.
[78] Demarest, *Central Bank Issues New Versions of Manuals Related to the Functioning of Open Banking in Brazil*, DEMAREST (Apr. 22, 2021), https://www.demarest.com.br/central-bank-issues-new-version-of-manuals-related-to-the-functioning-of-open-banking-in-brazil/.
[79] *Id.*
[80] *CBUAE Launches A Financial Infrastructure Transformation Programme to Accelerate the Digital Transformation of the Financial Services Sector*, CENT. BANK OF THE UNITED ARAB EMIRATES (Feb. 12, 2023), https://www.centralbank.ae/media/5jnfyjcn/cbuae-launches-a-financial-infrastructure-transformation-programme-to-accelerate-the-digital-transformation-of-the-financial-services-sector-en.pdf.
[81] Open Finance Regulation (Central Bank Circular No. 7/2023, effective Apr. 15, 2024) (United Arab Emirates), https://rulebook.centralbank.ae/en/rulebook/open-finance-regulation.

institutions.[82] Licensed institutions are required to grant access to customer data and the ability to initiate transactions on related accounts and products. Importantly, the CBUAE introduces a new category of regulatory license and a compliance regime for Open Finance providers, enabling them to undertake data sharing and service initiation.[83] The UAE adopts a phased approach to implementing the Open Finance framework, starting with banks and insurance companies.

A. SCOPE OF DATA SHARING

Under the UAE's Open Finance framework, licensees must share customer data on a range of accounts and products, including deposits, payment, savings, credit and debit cards, loans, standing orders, stored value facilities, foreign exchange, mortgages, and insurance.[84] The Open Finance Regulation applies primarily to the UAE's banking and insurance sectors and does not cover securities accounts or products. Open Finance providers are prohibited from processing sensitive data, such as personal data related to the physical, psychological, mental, genetic or sexual condition of a person, even with the explicit consent of users.[85] Screen scraping or any other similar data extraction activities for the provision of Open Finance services are expressly prohibited.[86] Therefore, licensees cannot collect customer information from other systems through automated processes.

B. DEGREE OF TECHNICAL STANDARDIZATION

In terms of implementation details, the UAE's Open Finance consists of the trust framework, the API hub, and the common infrastructure services to facilitate data sharing and transaction initiation. The trust framework includes the participant directory and digital certificates to provide identity validation and access management services for participants in the Open Finance framework, as well as an API portal to hold documentation on

[82] *Id.*
[83] *Id.*
[84] *Id*. art. 5.
[85] *Id*. arts. 1(49), 4(1), 4(5).
[86] *Id*. art. 15(2).

technical standards and business rules.[87] The API hub centralizes access to Open Finance services by aggregating APIs of different participants into a single point of implementation, thus harmonizing technical standards.[88] The CBUAE, in collaboration with other regulators, is responsible for developing technical requirements to provide guidance on Open Finance services, such as digital access specification, cybersecurity, and management of centralized consent.[89] It is worth noting that the UAE is the first country to implement a consolidated trust framework and centralized API hub, which ensures secure connectivity to the banking and insurance markets and is accessible only to authorized third-party service providers.[90]

Furthermore, the common infrastructure services include a consent and authorization manager, service assurance, reporting and analytics, administration tools, and other value-added enablers to support the management of privacy directives and enquiries, operational data and participant performance analysis, and dispute resolution in the Open Finance framework.[91] Coupled with appropriate authentication processes and secure communications, customers can have control over their personal data and access to a diverse range of financial services. In addition to the CBUAE's regulations, Open Finance providers shall adopt and implement industry standards and best practices in relation to technology risk and information security.[92] The CBUAE and other regulators have also issued the guidelines for financial institutions to mitigate risks arising from the use of enabling technologies, including APIs, artificial intelligence, biometrics, big data analytics, cloud computing, and distributed ledger technology.[93] Specifically, there are a set of key principles related to governance, design,

---

[87] *Id*. sched. 1.
[88] *Id.*
[89] *Id.* art. 26.
[90] *AI Etihad Payments launches Open Finance to strengthen the financial services sector in the UAE,* CENT. BANK OF THE UNITED ARAB EMIRATES & AI ETIHAD PAYMENTS (Apr. 23, 2024), https://www.centralbank.ae/media/4kfjymcz/al-etihad-payments-launches-open-finance-to-strengthen-the-financial-services-sector-in-the-uae-en.pdf.
[91] Open Finance Regulation, *supra* note 81, sched. 1.
[92] *Id.* art. 24(4).
[93] *Guidelines for Financial Institutions Adopting Enabling Technologies*, CENT. BANK OF THE UNITED ARAB EMIRATES ET AL. (Nov. 15, 2021), https://www.sca.gov.ae/assets/747a7cdf/guidelines-for-financial-institutions-adopting-enabling-technologies-2021.aspx.

management and monitoring, outsourcing, and business continuity of APIs.[94] Incumbents and new entrants to financial services are encouraged to adopt standardized APIs published by relevant regulators or the industry to ensure technical security and data interoperability. In this way, the implementation of Open Finance in the UAE will be subject to a high degree of technical standardization.

B. COLLABORATIVE APPROACH

Instead of introducing mandatory rules, some jurisdictions such as Singapore and Hong Kong have adopted a collaborative approach to Open Finance. Through collaboration with industry, regulators in these jurisdictions are actively encouraging the development of Open Finance and seeking to provide policy support for market participants to establish scalable data practices. Furthermore, given the importance of APIs, government agencies and participating industries are coordinating their efforts to set technical standards for secure data sharing in Open Finance.

Compared to jurisdictions adopting mandatory approaches, jurisdictions taking collaborative approaches are seeing much slower progress in empowering consumers and finance through data. In fact, these jurisdictions are increasingly adding mandatory elements in specific contexts, such as the expansion of credit data sharing requirements and systems.

1. SINGAPORE

The Monetary Authority of Singapore (MAS) has been collaborating with the industry to promote the development of Open Finance and has encouraged the adoption of standardized APIs by launching a number of initiatives, such as digital infrastructure for data aggregation and sharing. In November 2018, the API Exchange was established as a cross-border and open-architecture platform to facilitate collaboration between financial institutions and FinTechs.[95] It has brought different FinTech innovations into the marketplace and accelerated digital transformation of financial

---

[94] *Id.* paras. 2.6-2.10.

[95] ASEAN Bankers Association et al., *World's First Cross-Border, Open-Architecture Platform to Improve Financial Inclusion,* MONEY AUTH. OF SING. (Sept. 18, 2018), https://www.mas.gov.sg/news/media-releases/2018/worlds-first-cross-border-open-architecture-platform-to-improve-financial-inclusion.

institutions, expanding their reach and impact.[96]

Two years later, the MAS and the Smart Nation and Digital Government Group jointly initiated the Singapore Financial Data Exchange (SGFinDex), which enables individuals to consolidate their financial information from different government agencies and financial institutions, such as banks, insurers, and the Central Depository Limited.[97] By using a national digital identity and centrally managed online consent system, the SGFinDex helps individuals understand better their financial health and facilitates data sharing between participating institutions based on common API standards. Specifically, data sets shared through the SGFinDex include savings accounts, credit cards, loans, unit trusts, investment schemes, equities, bonds, structured products, and insurance policy and coverage details from financial institutions, as well as related accounts, housing loans, and tax information from government agencies.[98] Whereas there is no mandatory requirement for financial institutions in Singapore to open up their data, more than sixty percent of professionals consider the adoption of Open Finance a "must-have" and agree that this strategy has a positive impact on the financial sector, such as providing consumers with a wider range of fair financial services.[99] Further, the Singapore Trade Data Exchange was launched to promote the trusted and secure sharing of international trade data in the supply chain ecosystem.[100] This infrastructure extends the scope of data sharing to supply chains and allows financial institutions to verify the authenticity of trade transactions, thus laying the foundation for Open Data.

In terms of technical standardization, the Association of Banks in Singapore, in collaboration with the MAS and the industry, has released an API playbook setting out a comprehensive governance

---

[96] *See* APIX, https://apixplatform.com (last visited Jul. 23, 2024).

[97] *See Singapore Financial Data Exchange (SGFinDex)*, MONEY AUTH. OF SING., https://www.mas.gov.sg/development/fintech/sgfindex (last visited July 23, 2024). The Central Depository Limited is a wholly owned subsidiary of the Singapore Exchange and provides integrated clearing, settlement, and depository services for a wide range of products in the securities market.

[98] *Id.*

[99] *Finastra Global Survey Shows Appetite for Open Finance in Singapore Against Backdrop of Constrained Investment,* FINASTRA (Dec. 7, 2022), https://www.finastra.com/sites/default/files/file/2022-12/Press%20release_State-of-the-Nation-Research_Sing_final.pdf.

[100] *See* SING. TRADE DATA EXCHANGE, https://sgtradex.com (last visited July 23, 2024).

framework for the design and use of APIs.[101] This document provides implementation guidelines, data standards, information security standards, and governance mechanisms for key stakeholders developing and using APIs in the financial services industry. There are several principles for the design of APIs, such as openness, extensibility, interoperability, independence, transparency, stability, and loose coupling.[102] Based on the type of data and APIs, the playbook also identifies and develops a list of applicable data and security standards. Importantly, more than 400 APIs with detailed descriptions and functionalities are recommended, which cover different business processes in the financial services industry. The MAS launched the Financial Industry API Register for financial institutions to submit and update information on their available APIs.[103] These open APIs are divided into four main functional categories: product, sales and marketing, servicing, and transaction. Each functional category is classified as transactional or informational based on data sensitivity and authentication requirements.[104] Accordingly, the register can track information on financial products, services, and transactions, allowing for better customer experiences and a higher degree of standardization.

2. HONG KONG

In July 2018, the Hong Kong Monetary Authority (HKMA) published an open API framework for the banking sector, which adopts a risk-based principle and a four-phase approach to implement various API functions.[105] Under this framework, the HKMA allows banks flexibility for implementing open APIs and recommends existing international standards and practices to the industry. Based on data sensitivity and risks involved, open API functions are divided into four categories: product and service information, subscription and new applications for products and

---

[101] *Finance-as-a-Service: API Playbook*, ASS'N OF BANKS IN SING. & MONETARY AUTH. OF SING. (Nov. 2016), https://abs.org.sg/docs/library/abs-api-playbook.pdf.
[102] *Id.* at 16.
[103] *See Financial Industry API Register*, MONETARY AUTH. OF SING., https://www.mas.gov.sg/development/fintech/financial-industry-api-register (last visited July 23, 2024).
[104] *Id.*
[105] *Open API Framework for the Hong Kong Banking Sector*, H. K. MONETARY AUTH. (July 18, 2018), https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf.

services, account information, and transactions.[106] These APIs facilitate access to product, service, and account information that covers deposits, loans, investments, and insurance, support the customer acquisition process, and enable payments and transfers with customer authorization. There is a list of recommended architecture, operation, and technical standards in the framework. On this basis, banks should refer to regulatory requirements and relevant industry practices and maintain holistic controls on data and cybersecurity.[107]

Moreover, the HKMA encourages banks to collaborate with third-party service providers through bilateral arrangements with a common baseline. The third-party governance for different categories of open APIs requires appropriate and clear commercial contracts to define roles, responsibilities, security, and customer protection, ranging from the simple registration process to onboarding checks and monitoring, infrastructure resilience, and incident handling.[108] According to the HKMA's report, more than twenty retail banks have launched open API functions to make their product and service data available, while the active participation of third-party service providers from various industries such as FinTech and telecommunications has driven the high adoption rate of Phases I and II API use cases.[109] To promote the secure and efficient implementation of Phases III and IV APIs, the Hong Kong Association of Banks has developed an industry-level common baseline governing the banks' partnership with third parties,[110] and a set of technical standards covering user experience, customer authentication, data, information security, and operation.[111] These practices, with the support of API technology, enable service providers in the banking sector to aggregate and access customer data in a standardized manner.

The Commercial Data Interchange (CDI), launched in October

---

[106] *Id.* para. 11.
[107] *Id.* paras. 26–28.
[108] *Id.* paras. 29–31.
[109] *The Next Phase of the Banking Open API Journey*, H. K. MONETARY AUTH. at. 13–16 (May 2021), https://www.hkma.gov.hk/media/eng/doc/key-functions/ifc/fintech/The_Next_Phase_of_the_Banking_Open_API_Journey.pdf.
[110] *Open API Framework for the Hong Kong Banking Sector Common Baseline,* H. K. ASS'N OF BANKS (Dec. 14, 2021), https://www.hkab.org.hk/files/record/fintech/1/HKAB_-_Common_Baseline-1675853755.pdf.
[111] *Phase III Banking Open API Standards*, H. K. ASS'N OF BANKS (Dec. 14, 2021), https://www.hkab.org.hk/files/record/fintech/2/Phase%20III%20Banking%20Open%20API%20Standards%20(1)-1665466382.pdf.

2022, serves as a financial infrastructure to facilitate the secure sharing of commercial data and streamline banking processes, such as credit assessment and Know Your Customer (KYC) processes.[112] The CDI is essential to Hong Kong's Open Banking strategy by connecting data providers, data consumers, and other participating entities from various industries, including finance, payment and e-commerce, trade and sales, and supply chain. The HKMA has issued a set of governance documents, standardized agreements, and templates for CDI participants to delineate their responsibilities and provide technical guidance, as well as maintain a centralized list of available commercial data.[113] This framework enables each participant to develop its own application for data exchange, while allowing flexibility in interoperating with different systems to promote a wider adoption of the CDI. More recently, the HKMA launched the Interbank Account Data Sharing (IADS) pilot program, with the participation of twenty-eight banks to share deposit account information of retail, corporate, and SME customers.[114] The CDI and IADS initiatives mark an important step in Hong Kong's implementation of Open Banking, helping the financial sector unlock the potential of data and technology.

C. OTHER APPROACHES: BUILDING DATA ECOSYSTEMS

In addition to mandatory and collaborative approaches, a number of jurisdictions are now seeking to develop and implement broader data strategies, often in the context of seeking to build wider data ecosystems. These strategies often include elements of Open Finance. China and India are the leading examples. These usually focus less on consumer empowerment and data control (which is central to the mandatory approaches) and more on mechanisms to mandate the aggregation of data to maximize potential benefits to the wider ecosystem (which is also an element of the mandatory steps being taken in the collaborative strategies considered in the previous section).

---

[112] *See About CDI*, COM. DATA INTERCHANGE, https://cdi.hkma.gov.hk/about-cdi/ (last visited July 23, 2024).
[113] *Commercial Data Interchange Framework*, H. K. MONETARY AUTH. (Mar. 2024), https://cdi.hkma.gov.hk/wp-content/uploads/CDI-Framework-2024-Mar.pdf.
[114] Press Release, H. K. Monetary Auth., Interbank Account Data Sharing Pilot Programme (Dec. 21, 2023), https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/12/20231221-3/.

1. CHINA

China has not yet established a governance framework for Open Finance. Rather, in the context of digital transformation, China is attaching greater importance to data as a factor of production. The government provides guidance on how to unlock the value of data while mitigating the associated economic and societal risks.[115] It contains several principles aimed at lowering the threshold for market players to obtain data, and promotes the secure sharing and use of data.[116] With policy support for building data exchanges, this guidance helps break the data monopoly of FinTech giants and facilitates data-driven innovation in the financial sector. Coupled with introducing data security and personal information protection laws, China has made a continuous effort to open up data that is gathered in various service scenarios and to improve governance of data infrastructure through close collaboration between the government, industry associations, and private businesses.

Additionally, China actively encourages the development of its credit data system, with the emergence of nontraditional financial service providers such as FinTechs and BigTechs.[117] These companies have leveraged innovative technologies to collect, use, and disseminate massive amounts of customer information, thus improving the coverage of credit services. At the end of 2021, the Chinese government released a notice to promote effective sharing of credit information and increase SMEs' access to financing.[118] By establishing information-sharing platforms at the local level, this initiative can integrate a wider range of enterprise information into the credit reporting system through collaboration among different government departments. In the credit market, China has gradually developed a comprehensive framework to facilitate data access and sharing between the public and private sectors, laying the foundation for the development of Open Finance. In addition, the People's Bank of China (PBOC) issued the *Measures for the Administration of*

---

[115] Opinions on Building Basic Systems for Data and Putting Data to Better Use, *supra* note 26.
[116] *Id.* art. 2.
[117] See Menglu Wang et al., *From Credit Information to Credit Data Regulation: Building an Inclusive Sustainable Financial System in China*, 33 (2) WASH. INT'L L.J. 270 (2024), for a more detailed discussion of China's credit reporting system.
[118] Implementation Plan for Promoting the Sharing and Use of Credit Information and Improving Financing of Micro, Small and Medium Enterprises, *supra* note 28.

Credit Reporting Services in September 2021.[119] This regulation focuses on the collection, processing and use of credit information to identify and determine the credit status of individuals and enterprises.[120] Commercial banks and other licensed financial institutions specializing in credit business are required to submit their customers' credit information to the centralized credit reporting system managed by the PBOC.[121]

In addition to regulatory rules and policy guidelines, there are industry standards for the development and use of APIs. Although not legally binding, these standards are used by regulators and companies to determine compliance with technical requirements for APIs. For example, the PBOC released the API security specification for commercial banks.[122] This standard specifies the types and security levels of interfaces, security design and integration, operation and maintenance monitoring, service termination, and other security requirements that apply to APIs for external interconnection of commercial banks and provide reference for security assessment institutions.[123] More importantly, the specification clarifies the roles, responsibilities, and functions of participants in API services, including users who initiate application requests, third-party application agencies, and commercial banks.[124] The API has a uniform identifier consisting of commercial bank code, the types of interfaces and services, and other codes.[125] These API security standards for commercial banks provide technical support for the implementation of Open Finance. On this basis, some large banks in China have partnered with third-party service

---

[119] Zhengxin Yewu Guanli Banfa (征信业务管理办法) [Measures for the Administration of Credit Reporting Services] (promulgated by the People's Bank of China, Sept. 17, 2021, effective Jan. 1, 2022), (China). *English translation available at.* http://www.pbc.gov.cn/en/3688241/3688687/3688693/4393542/2021111916465019962.pdf.

[120] *Id.* art. 3.

[121] Geren Xinyong Xinxi Jichu Shujuku Guanli Zanxing Banfa (个人信用信息基础数据库管理暂行办法) [Interim Measures for the Administration of the Consumer Credit Information Basic Database] (promulgated by the People's Bank of China, Aug. 18, 2005, effective Oct. 1, 2005), art. 6, (China). *English translation available at.* http://www.asianlii.org/cn/legis/cen/laws/imftaotbdoici782/.

[122] Commercial Bank Application Programming Interface Security Management Specification, *supra* note 27.

[123] *Id.* art. 1.

[124] *Id.* arts. 7–12.

[125] *Id.* Annex B.

providers to adopt open banking APIs and develop best practice models for different financial businesses.[126]

2. INDIA

Over the past decade years, India has pursued on an ambitious plan to overhaul its digital infrastructure by developing the so-called "India Stack".[127] As one aspect, with increasing access to data, this initiative helps extend the reach of payment services and boost competition in the financial sector. The implementation of India Stack relies on significant synergies of a digital identity system, an interoperable payments network, and regulatory mechanisms for data sharing, and thus involves different regulators and market participants.[128] The Reserve Bank of India (RBI) has been actively encouraging the adoption of Open Finance by establishing a regulatory framework for the registration and operation of Account Aggregator, a nonbanking financial company that manages the consent and transfer of data.[129] According to the RBI's directions, financial information providers such as banks, banking companies, nonbanking financial companies, asset management companies, depository participants, insurance companies, and insurance repositories shall share customer information with an Account Aggregator for transferring to the intended recipients.[130]

In addition, the National Payments Corporation of India (NPCI) has launched the Unified Payments Interface (UPI) to incorporate digital payment service providers into the banking system, thus promoting financial inclusion. The UPI enables access to multiple bank accounts through a single mobile application and instant

---

[126] *2022 Kaifang Yinhang Shengtai Jinrong Baipishu (2022 开放银行生态金融白皮书) [2022 Open Banking Ecological Finance White Paper],* CHINA FIN. CERTIFICATION AUTH. ET AL. (Dec. 7, 2022), https://www.cebnet.com.cn/upload/resources/file/2022/12/07/199023.pdf.

[127] Yan Carriere-Swallow et al., *India's Approach to Open Banking: Some Implications for Financial Inclusion* 4 (Int'l Monetary Fund, Working Paper WP/21/52, 2021), https://www.imf.org/en/Publications/WP/Issues/2021/02/26/Indias-Approach-to-Open-Banking-Some-Implications-for-Financial-Inclusion-50049.

[128] See INDIA STACK, https://indiastack.org/index.html (last visited July 23, 2024), For more detailed information. India Stack contains a set of open APIs and digital public goods to unlock the economic potential of identity, data, and payments.

[129] Master Direction – Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, RBI/DNBR/2016-17/46 (dated Sept. 2, 2016, updated as on Feb. 22, 2024) (India), https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.

[130] *Id.* arts. 3(1) xi, 7.1, 7.6.

money transfers between different participating institutions.[131] The NPCI is responsible for approving the participation of issuer banks, payments banks, third-party application providers, and prepaid payment instrument issuers in the UPI system. A payments bank is a new type of banking license introduced in India, with lower regulatory requirements but restrictions on the scope of financial activities.[132] Third-party service providers seeking to participate in the UPI system are required to obtain a payments bank license or operate through an institution with a banking license.[133] Although there is no formal regulatory framework for Open Finance in India, the launch of the Account Aggregator and the UPI system facilitates secure sharing of financial information and efficient interbank transactions. Currently, the number of banks participating in the UPI has exceeded 500,[134] and more than 300 institutions have been certified and provide services in the Account Aggregator ecosystem.[135] These statistics show broad market support for India's existing approach to data.

A. SCOPE OF DATA SHARING

As a key component of India Stack, the Aadhaar system, launched in 2010, provides a secure, recognized digital identity that can authenticate individuals for a range of government and business services. It collects demographic and biometric data on Indian residents, verifies their identity through the electronic Know Your Customer (e-KYC) process, and generates a digital signature for sharing with different service providers.[136] Building on this system, India links the users' Aadhaar identity, bank accounts, and mobile

---

[131] *Unified Payments Interface*, NAT'L PAYMENTS CORP. OF INDIA, https://www.npci.org.in/what-we-do/upi/product-overview (last visited July 23, 2024).

[132] Banking Regulation Act, 1949 (India), s. 22, https://www.indiacode.nic.in/bitstream/123456789/1885/1/A194910.pdf; *Guidelines for Licensing of Payments Banks*, RSRV. BANK OF INDIA (Nov. 27, 2014), https://rbidocs.rbi.org.in/rdocs/Content/PDFs/PAYMENT271114.pdf.

[133] *See UPI Roles & Responsibilities*, NAT'L PAYMENTS CORP. OF INDIA, https://www.npci.org.in/what-we-do/upi/roles-responsibilities (last visited July 23, 2024).

[134] *See UPI Live Members*, NAT'L PAYMENTS CORP. OF INDIA, https://www.npci.org.in/what-we-do/upi/live-members (last visited July 23, 2024).

[135] *See Certified Entities in the Account Aggregator Ecosystem*, SAHAMATI, https://sahamati.org.in/certified-entities/# (last visited July 23, 2024).

[136] *See Identity*, INDIA STACK, https://indiastack.org/identity.html (last visited July 23, 2024).

phones to improve access to finance. In respect of data, the Account Aggregator system has also been established to facilitate the sharing of customer-permissioned financial information. The RBI specifies the types of financial information that can be shared, including deposits, deposit receipts, investment products, insurance policies, pension schemes, and goods and services tax returns.[137] Although initially implemented in the financial sector, the data-sharing system is expanding into other important sectors in India, such as healthcare and e-commerce.

B. DEGREE OF TECHNICAL STANDARDIZATION

The Unique Identification Authority of India is a public agency tasked with providing Aadhaar identity authentication services through the e-KYC process. It has established technical specifications for e-KYC and authentication APIs, covering data flow and formats, communication protocols, and security requirements.[138] These standards provide guidance on how to improve KYC experiences and authenticate individuals using specified APIs. In terms of mobile payments, the UPI defines a markup language that standardizes fund transfer instructions to enable interoperability between fund custodians and front-end payment applications.[139] Although participation in the UPI system is not mandatory, this shared interface facilitates seamless connectivity between banks, third-party payment service providers, merchants, and customers, without the need to develop individual APIs.

In addition, there are a set of API specifications designed to facilitate the secure sharing of financial information through the Account Aggregator.[140] The Account Aggregator system contains

---

[137] Master Direction – Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, *supra* note 129, art. 3(1) ix.

[138] *Aadhaar E-KYC API Specification – Version 2.1,* UNIQUE IDENTIFICATION AUTH. OF INDIA (May 2017), https://uidai.gov.in/images/resource/aadhaar_ekyc_api_2_1.pdf; *Aadhaar Authentication API Specification – Version 2.5*, UNIQUE IDENTIFICATION AUTH. OF INDIA (Jan. 2022), https://uidai.gov.in/images/resource/Aadhaar_Authentication_API-2.5_Revision-1_of_January_2022.pdf.

[139] *India's Unified Payment Gateway for Real-time Payment Transactions: Unified Payment Interface*, NAT'L PAYMENTS CORP. OF INDIA (July 13, 2022), https://www.npci.org.in/PDF/npci/upi/Product-Booklet.pdf.

[140] *NBFC - Account Aggregator (AA) - API Specification Version 2.0.0*, RSRV.

various interfaces to support interactions between customers, financial information providers, and users. The technical specifications provide a detailed description of APIs with different functions, including account discovery and linking, consent management, data flow, notification, and monitoring to ensure the interoperability of participating institutions.[141] Account Aggregators, as well as financial information providers and users, are required to conduct an impact assessment on their technology systems and make necessary changes to align with the API specifications.[142]

D. MARKET-LED APPROACH

Other jurisdictions, in particular the US, have taken a hands-off approach to Open Finance, allowing maximum flexibility for the market to establish a framework for data access and sharing. In this context, Open Finance is evolving as an industry-driven initiative rather than a regulatory mandate, and thus government involvement in the process is limited, mainly by issuing nonbinding guidelines. Without mandatory rules, the industry has taken the lead in developing technical standards for the implementation of Open Finance. Although appealing, industry segmentation and competition have meant that this approach has been relatively cumbersome, leading a number of jurisdictions that initially focused on market-led development to move towards mandatory, collaborative, or ecosystem approaches.

Over the past few years, the market-led approach has promoted Open Finance practices in the US, while section 1033 of the *Dodd-Frank Wall Street Reform and Consumer Protection Act* (Dodd-Frank Act) provides a legal basis for access to consumer information.[143] Under this section, a covered entity (such as a bank) shall make available to a consumer, upon request, information about

---

BANK INFO. TECH. PVT. LTD. (Aug. 9, 2023), https://specifications.rebit.org.in/artefacts/NBFC-AA_API_Specification_v2.0.0.pdf.

[141] *See Account Aggregator Ecosystem API Specifications*, RSRV. BANK INFO. TECH. PVT. LTD., https://api.rebit.org.in (last visited July 23, 2024).

[142] *NBFC - Account Aggregator (AA) - API Specification Adoption Strategy Version 1.0.0*, RSRV. BANK INFO. TECH. PVT. LTD. (Aug. 9, 2023), https://specifications.rebit.org.in/artefacts/NBFC-AA_API_Specification_Adoption_Strategy.pdf.

[143] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111–203, § 1033, 124 Stat. 1376, 2008 (2010) (codified at 12 U.S.C. § 5533).

financial products or services, including information relating to transactions and accounts.[144] In accordance with the Dodd-Frank Act, the CFPB issued nonbinding consumer protection principles for financial data sharing and aggregation in October 2017.[145] These principles cover data access, scope and usability, informed consent, payment authorization, security, transparency, accuracy, dispute resolution, and accountability mechanisms, which help safeguard consumer interests in financial services.[146] Later in July 2018, the US Department of the Treasury (Treasury) released a report containing a range of issues and recommendations for nonbank financial institutions and FinTech firms in the digital era.[147] In the US, many financial services companies, data aggregators, and FinTech application providers have collaborated to collect and disseminate customer financial data using different technical methods. As the practice of obtaining data through screen scraping poses significant risks, the Treasury calls for more secure and efficient data-sharing protocols, such as bilateral or open APIs.[148] The report also recommends that the Treasury work with financial regulators to strengthen public-private partnerships to facilitate the adoption of trustworthy digital legal identity products and services in the financial sector. [149] These joint efforts may help the US market establish an effective governance framework for financial data access and sharing, further promoting the development of Open Finance.

In addition to nonbinding guidelines, several industry associations in the US have developed a set of technical standards for data sharing through APIs. For example, the National Automated Clearing House Association established a working group to focus on API standardization in the payments industry.[150] It aims to address

---

[144] *Id.*

[145] *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, CONSUMER FIN. PROT. BUREAU (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[146] *Id.*

[147] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, U.S. DEP'T OF THE TREASURY (July 2018), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf.

[148] *Id.* at 34–35.

[149] *Id.* at 41–44.

[150] The National Automated Clearing House Association (NACHA) is responsible

technical problems arising from the use of unique, incompatible, and customized APIs by different financial services providers. The adoption of category-based standardized APIs has promoted secure data exchanges across interoperable systems and powered more than four million payment transactions.[151] Moreover, the Financial Data Exchange (FDX), launched in 2018, creates a common and interoperable technical standard (known as FDX API) for customer financial data sharing.[152] This platform increases data standardization and interoperability in the financial sector by connecting a wide range of financial institutions, data aggregators, FinTech firms, payment service providers, public utilities, and consumer groups. In October 2021, the FDX updated the API standard to include design guidelines for consumer dashboards and mechanisms for standardizing user consent, and to introduce reciprocal data sharing between data providers and third-party FinTechs.[153] These US industry standards have been the driving force for the implementation of Open Finance.

As a result of relatively slow progress, both in building Open Finance through a market-led approach as well as in developing a comprehensive approach to data regulation more generally, the CFPB has been considering a change in direction. Recently, the CFPB proposed a rule to implement personal financial data rights that would accelerate the shift towards mandatory adoption of Open Finance.[154] Under this proposed rule, card issuers, financial institutions, and other payment facilitation providers are required to make data available through dedicated APIs.[155] Authorized third

---

for governing the automated clearing house network that drives direct deposits and payments with the capability to reach all US banks and credit union accounts. *See AFINIS Interoperability Standards*, NACHA, https://www.nacha.org/afinis-interoperability-standards (last visited July 23, 2024).

[151] *Phixius by NACHA: Trusted Payment-Related Information at the Speed of Business*, NACHA, https://www.nacha.org/content/phixius (last visited Oct. 31, 2024).

[152] The Financial Data Exchange is an industry standards body operating in the US and Canada that facilitates secure sharing of permissioned consumer and business financial data using a common and interoperable technical standard. *See About FDX*, FIN. DATA EXCH., https://financialdataexchange.org/FDX/FDX/About/About-FDX.aspx?hkey=dffb9a93-fc7d-4f65-840c-f2cfbe7fe8a6 (last visited July 23, 2024).

[153] Fin. Data Exch., *Financial Data Exchange (FDX) Releases FDX API 5.0,* FIN. DATA EXCH. (Oct. 21, 2021), https://financialdataexchange.org/FDX/News/Press-Releases/Financial_Data_Exchange_Releases_FDX_API_5.0.aspx.

[154] Required Rulemaking on Personal Financial Data Rights, *supra* note 10.

[155] *Id.* pt. IV.A.2.

parties are allowed access to several types of covered data, including transaction information, account balance, information to initiate payments, contractual terms and conditions, upcoming bill information, and basic account verification information.[156] The CFPB also requires industry standards to be developed by a fair, open, and inclusive standard-setting body.[157] There are basic operational, performance, and security requirements for the establishment and maintenance of APIs to ensure that consumers and third parties can make requests and have timely access to covered data in a usable electronic form.[158] However, the US regulatory framework for Open Finance is still a work in progress, and its impact on market participants such as banks, FinTech firms, and consumers remains to be seen. If the regulation takes effect as proposed, the US will move toward to a mandatory approach to Open Finance, allowing consumers greater control over their financial data and standardizing data-sharing between financial services companies and third parties.

IV. CHALLENGES OF OPEN FINANCE GOVERNANCE

Open Finance seeks to create an ecosystem of financial institutions, FinTech firms, other third-party service providers, consumers, and regulators to facilitate effective use of customer data and promote innovation in the financial sector. There is no single approach to implementing Open Finance across jurisdictions, with approaches ranging from mandatory rules to public-private collaboration and industry-led initiatives, although mandatory approaches are increasingly being seen as more successful. As discussed earlier, governance frameworks for Open Finance involve a complex interplay between financial regulations, data protection laws, and technical standards. Access to and sharing of financial data is often subject to separate but related regulatory rules. However, the intersection of these laws and regulations aimed at achieving different policy objectives such as financial innovation, data security, and customer protection is not always harmonious, and thus brings new challenges when seeking to build Open Finance governance. In addition to data governance, financial regulation, and mandatory rules for Open Finance, technical infrastructure plays a very

[156] *Id.* pt. IV.B.3.
[157] *Id.* pt. V.A.6.
[158] *Id.* pt. IV.C.2.

important role in successfully building Open Finance.

A. FRAGMENTATION OF OPEN FINANCE REGULATION

Regulators involved in Open Finance governance may include the banking supervisor, other financial regulators, the central bank, the competition authority, the consumer protection bureau, and the data protection authority, depending on the focus of different policy objectives. For example, the central bank or banking supervisor (which are frequently but not always the same institution) in some jurisdictions, such as the EU, Brazil, Singapore, and Hong Kong, is primarily in charge of overseeing the implementation of Open Banking-Finance (usually as limited by the scope of authority of the particular central bank or the banking-financial regulator). In other cases, such as the UK and Australia, Open Finance has been initiated by the competition authority to create a level playing field in financial services. The US has aspects of both: the CPFB (a division of the central bank) is responsible for rulemaking on financial data rights.[159] Given that rules governing data sharing between financial institutions and third parties are implemented by multiple authorities, there is an issue of regulatory fragmentation both within and across jurisdictions. As a result, in India and China, central strategies have been developed, crossing over the entire economy, albeit in both with the central bank (RBI and PBOC) taking a key role in the context of financial data sharing, aggregation, and access.

In the context of financial data access, control of data, and data sharing, regulatory conflicts may arise at different levels. First, in many jurisdictions, data protection is an important part of the broad governance framework for Open Finance, and thus the complexity of the tradeoffs between financial and data regulatory objectives is emerging.[160] Open Finance interacts with general data regulation but is evolving separately, with the EU being a pioneer in adopting mandatory rules for financial data sharing. In the EU, the implementation of *General Data Protection Regulation*[161] (GDPR) in 2018, together with the PSD2, provides a comprehensive framework for Open Banking. The GDPR applies to the processing

---

[159] *See supra* Part III.

[160] Arner et al., *supra* note 1, at 275.

[161] 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)' 2016 O.J. (L 119) 1.

of personal data, including data processed in the context of payment services as defined by the PSD2.[162] Whereas the PSD2 sets out rules related to data protection and account security, its interaction with the GDPR, which imposes higher protection requirements for the processing of personal data, creates complexity and uncertainty.[163] For example, sensitive payment data [164] under PSD2 differs considerably from the definition of sensitive personal data in the GDPR. Under Article 9 of the GDPR, the processing of personal data which is particularly sensitive in relation to fundamental rights and freedoms is prohibited unless the conditions of a specific derogation are met.[165] Payment service providers may obtain access to sensitive information about an individual, such as personal health data revealed by electronic payments of medical bills from the individual's bank account. [166] In this case, the GDPR requires technical measures to prevent the processing of payment account information containing special categories of personal data, potentially limiting access to and use of customer data that is essential to the provision of payment services under the PSD2.

Along with the EU, the UK and Australia have also adopted a mandatory approach to Open Finance. In the UK, the CMA mandated nine of the largest banks to implement common standards for Open Finance and facilitate secure data-sharing with third parties.[167] The provision of additional customer attribute data to third parties could prevent fraud beyond payments, such as identity theft in credit applications and the use of fraudulent account details, thus improving risk management. However, the blurring lines of responsibility between banks and third parties for fraud prevention present several challenges, one of which is that sharing customer attribute data may conflict with data minimization requirements.[168] This challenge exemplifies the coordination failure between

---

[162] *Id.* Recital 6.
[163] *Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR*, EUR. DATA PROTECTION BD. paras. 1–3 (Dec. 15, 2020), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf.
[164] The Second Payment Services Directive, *supra* note 5, art. 4(32). Sensitive payment data means data, including personalized security credentials which can be used to carry out fraud.
[165] General Data Protection Regulation, *supra* note 161, art. 9.
[166] EUR. DATA PROT. BD., *supra* note 160, paras. 51–58.
[167] *See supra* Section III.A.2.
[168] *The Future Development of Open Banking in the UK,* THE OPEN BANKING STRATEGIC WORKING GRP. 143–144 (Feb. 2023), https://www.jbs.cam.ac.uk/wp-content/uploads/2023/02/2023-ccaf-future-development-of-open-banking.pdf.

financial regulation and data governance in Open Finance, as prioritizing the objective of managing fraud risks potentially leads to the subordination of privacy protection.

Similarly, the Australian government has introduced the CDR rules to grant the banking sector rights to access and transfer consumer data.[169] The CDR primarily constructs data portability as a competition law mechanism, which reveals the uncertain role of information privacy law as part of the Open Finance initiative.[170] Under this regulatory regime, data portability is a multifaceted concept that creates complex interactions between competition and information privacy requirements. Specifically, the definition of CDR data relating to a CDR consumer[171] is incompatible with personal information about an identifiable individual under privacy law.[172] In this case, two regulatory frameworks, the Privacy Safeguards for CDR data and the Australian Privacy Principles for personal information, may impose duplicated privacy obligations on accredited data recipients in Open Finance.[173] The potential overlap is likely to increase the complexity and cost of regulatory compliance, and thus undermine the efficiency of Open Finance governance.

In Brazil, the implementation of Open Finance must comply with data protection regulation, Lei Geral de Proteção de Dados Pessoais (LGPD), that establishes a new legal framework for the processing of personal data.[174] The legal basis of this newly enacted legislation is not significantly different from that of the EU's GDPR, with one important exception being that the LGPD allows data

---

[169] *See supra* Section III.A.3.

[170] Mark Burdon & Tom Mackie, *Australia's Consumer Data Right and the Uncertain Role of Information Privacy Law,* 10(3) INT'L DATA PRIV. L. 222, 228 (2020).

[171] Competition and Consumer Act 2010, *supra* note 58, s. 56AI.

[172] CDR data relates to a CDR consumer and personal information is about an identifiable or reasonably identifiable individual. By comparison, the term 'relates' has a broader meaning than 'about'. *See* Privacy Act 1988 (Austl. Compilation No. 98), s. 6(1), https://www.legislation.gov.au/C2004A03712/latest/text.

[173] Burdon & Mackie, *supra* note 170, at 228–32. The Privacy Safeguards set out privacy rights and strict obligations on businesses collecting and handling CDR data. The Australian Privacy Principles are the cornerstone of the privacy protection framework and govern standards, rights, and obligations in relation to personal information.

[174] Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.08.2018 (Braz.), https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

processing for credit protection without consumer consent.[175] The interplay between the LGPD and Open Finance has implications for the sharing of data on products, services, and customer transactions related to credit operations. In this case, the specific legal basis may be frequently used by financial institutions and third parties involved in the Brazilian Open Finance system to process personal data required for credit.

Likewise, the strategy in India is accompanied by the development of a data protection regime. The RBI has set regulatory requirements for Account Aggregators to facilitate the consent-based collection and sharing of financial information.[176] Account Aggregators are licensed as nonbanking financial companies responsible for managing the consent and transfer of customer data. On this basis, India then promulgated the Digital Personal Data Protection Act in 2023, introducing the concept of a consent manager as a single point of contact to enable data principals to give, manage, review, and withdraw consent through an accessible, transparent, and interoperable platform.[177] From the perspective of data regulation, Account Aggregators function as a consent manager for financial data and provide related services to institutions participating in India. By separating consent management from data flows, Account Aggregators facilitate the efficient transfer of financial information while protecting customer privacy. However, this separation does not ensure that financial data is only used for the purpose for which the data was shared or is stored for the period initially agreed.[178] Although Brazil and India have created data governance frameworks, there are concerns about whether the initiatives can operate in a way that enhances public trust in data-sharing practices.

As an example of the market-led approach, the US has yet to establish a regulatory framework for Open Finance, and in this

---

[175] *The Role of Consumer Consent in Open Banking*, THE WORLD BANK 23–24 (Dec. 2021), https://documents1.worldbank.org/curated/en/099425002082230437/pdf/P17050 50aeb8e704f088260f228802b73b8.pdf.

[176] Master Direction – Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, *supra* note 129.

[177] Digital Personal Data Protection Act, 2023 (No. 22 of 2023, dated Aug. 11, 2023) (India), art. 2(g), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20P rotection%20Act%202023.pdf.

[178] Siddharth Tiwari et al., *The Design of A Data Governance System*, BANK FOR INT'L. SETTLEMENTS 17 (July 2022), https://www.bis.org/publ/bppdf/bispap124.pdf.

context, industry associations have taken the lead in developing technical standards for data access and sharing.[179] In terms of financial data governance, the Gramm-Leach-Bliley Act (GLBA) addresses concerns about customer financial privacy, requiring financial institutions to protect the security and confidentiality of customers' personal information and prevent unauthorized access to or use of such information.[180] More specifically, the Fair Credit Reporting Act (FCRA) regulates the collection, dissemination, and use of personal information contained in consumer reports.[181] The CFPB has drafted rules on personal financial data rights that would allow authorized third parties to access data about consumers' transactions and accounts.[182] This proposed regulation raises a number of issues for data providers, third parties, data aggregators, and other stakeholders in the financial sector. For instance, a new data protection and privacy framework would be established, in addition to the existing regulatory regimes (the GLBA and the FCRA) applicable to financial data providers and recipients, to further safeguard consumers against unauthorized data-sharing practices.[183] The CFPB's rules add a layer of complexity to the roles of financial institutions and third parties under different privacy regimes, creating regulatory compliance challenges as they implement the Open Finance framework.

Second, there are problems with the harmonization of API standards in Open Finance, thus issues around not only standards but also sharing infrastructure are taking an increasingly central role in building Open Finance. The lack of common technical standards and the economic cost for smaller financial institutions and third parties to develop APIs pose serious challenges to Open Finance governance in some jurisdictions.[184] The adoption of APIs is an essential part of Open Finance initiatives, facilitating the secure and efficient exchange of customer data between parties. This requires a high degree of technical standardization and a viable data-sharing

---

[179] *See supra* Section III.C.
[180] Gramm-Leach-Bliley Act, Pub. L. No. 106–102, § 501, 113 Stat. 1338, 1436–1437 (1999) (codified at 15 U.S.C. § 6801).
[181] Fair Credit Reporting Act, 15 U.S.C § 1681.
[182] Required Rulemaking on Personal Financial Data Rights, *supra* note 10.
[183] Alexandra Steinberg Barrage et al., *First Impressions on CFPB's Proposed Open Banking Rule: Considerations for Key Stakeholders*, DAVIS WRIGHT TREMAINE LLP INSIGHTS (Oct. 25, 2023), https://www.dwt.com/blogs/financial-services-law-advisor/2023/10/cfpb-consumer-data-access-third-parties-fintechs#page=1.
[184] BANK FOR INT'L. SETTLEMENTS, *supra* note 16, at 6.

architecture. In the EU, the PSD2 mandates banks to provide authorized third parties with access to customer data via a dedicated interface, but it does not specify API standards. Resultantly, a series of industry-led technical specifications have emerged.[185] However, the lack of standardization and interoperability among different APIs hinders their ability to cover a wider range of banks, as setting up and maintaining technical connections with each bank is a resource-intensive process, especially for small ASPSPs.[186] In practice, some third-party service providers have faced significant obstacles in accessing payment accounts data because of the poor quality of APIs used or the large differences in API implementation across the system.[187] Furthermore, there are new developments in the EU payments market, such as the emergence of premium APIs that allow access to functionalities beyond those mandated by the PSD2. Through premium APIs, some market players are able to offer the same or additional payment services without applying for a third-party provider license required by the PSD2, creating an uneven playing field.[188] In the absence of common technical standards, payment service providers using premium APIs are likely to gain a competitive advantage, whereas customers may not be adequately protected because they cannot distinguish between licensed and unlicensed third parties.[189]

The UAE's Open Finance framework contains a centralized API hub, with the aim of establishing a harmonization of technical specifications for data exchanges between different participants.[190] As this regulation has just come into effect, it remains to be seen what effect the API aggregator will have on the standardization of Open Finance.

Instead of mandatory requirements, regulators in Singapore and Hong Kong have collaborated with industry to promote the development of Open Finance by establishing data exchange platforms and issuing API implementation guidelines.[191] These initiatives enable customers to have greater access to and control

---

[185] *See supra* Section III.A.1.
[186] Ivan Bosch Chen et al., *A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*, Eur. Comm'n 59 (Feb. 2, 2023), https://www.ecri.eu/sites/default/files/a-study-on-the-application-and-impact-of-directive-ev0423061enn.pdf.
[187] *Id.* at 92.
[188] *Id.* at 62–63.
[189] *Id.*
[190] Open Finance Regulation, *supra* note 85, at sched. 1.
[191] *See* Open Finance Regulation, *supra* note 85, at Sections III.B.1, III.B.2.

over their financial data. Both jurisdictions have adopted an open API framework with a list of recommended technical and security standards.[192] Financial institutions and third-party service providers can refer to those API standards and industry practices for data access and sharing. In the US, the FDX has developed a common API standard and improved data portability by connecting a range of financial institutions, data aggregators, FinTechs, and other related service providers.[193] However, these API frameworks are not mandatory for Open Finance services, allowing the market flexibility to implement different technical standards for data sharing. As a result, there may be multiple networks of technical connections between financial institutions and third parties participating in Open Finance. Given the potential difficulties in ensuring interoperability between different networks, Open Finance systems that rely on this type of API implementation are likely to be fragmented.[194] The existence of multiple networks may increase the complexity of regulating market participants using different technical standards, as well as the cost of enabling API interconnection across the Open Finance system.[195]

Likewise, in Mainland China, the PBOC has issued the API security specification for commercial banks, which contains a set of recommended industry standards.[196] While these standards provide technical support for the implementation of Open Banking, they are not legally binding and mainly apply to APIs of commercial banks for external interconnection. Thus, it is practically difficult to ensure that the APIs used by third parties to access customer financial data also meet the same technical standards and security requirements.

The establishment of Account Aggregators in India illustrates another model of data sharing through an intermediary technology platform.[197] An important feature of Account Aggregators is that they manage customer consent to the transfer of financial data, but are not allowed to store, process, and sell the data. The RBI has introduced a set of open API-based technical standards for

---

[192] ASS'N OF BANKS IN SING. & MONETARY AUTH. OF SING., *supra* note 101; H. K. MONETARY AUTH., *supra* note 118.
[193] FIN. DATA EXCH., *supra* note 152.
[194] *Enabling Open Finance through APIs*, BANK FOR INT'L. SETTLEMENTS 5 (Dec. 2020), https://www.bis.org/publ/othp36.pdf.
[195] *Id.*
[196] Commercial Bank Application Programming Interface Security Management Specification, *supra* note 27.
[197] *See supra* note 85, at Part III.A.5.

participants in the Account Aggregator ecosystem,[198] aiming to ensure interoperability and the integrity of data flows. However, this data sharing system functions well when a large number of customer accounts maintained by different financial institutions are connected to the Account Aggregator and information users can securely access the aggregated data.[199] In India, regulated entities in the financial sector are not mandated to participate in the Account Aggregator ecosystem despite having common technical standards. Thus, it remains a challenge to improve data consistency across different sources and formats in financial services.

Thus, both governance as well as standards and other infrastructure are central to building Open Finance.

B. DATA LOCALIZATION

Over the past decade, many jurisdictions have strengthened the implementation of data localization laws, posing a challenge to the free flow of personal financial information across borders. Data localization involves maintaining digital sovereignty through a set of rules governing data mobility, ownership, security, and other relevant factors, with the aim to protect and maximize the value of domestic data.[200] These regulatory requirements restrict the transfer of certain data that is deemed sensitive, important, or related to national security. However, as finance is one of the most digitalized industries and relies heavily on data analytics, the free flow and sharing of customer data is fundamental to the widespread adoption of Open Finance, especially in the context of increasing cross-border financial activities. Thus, the trend towards data localization presents a complex problem for Open Finance governance.

First, data localization is implemented through equivalent standard restrictions, that is, data may only be transferred to countries with an equivalent level of data protection.[201] For example, the EU's GDPR allows the transfer of personal data to a third country or an international organization if the European Commission has decided that the country or organization ensures an

---

[198] RSRV. BANK INFO. TECH. PVT. LTD., *supra* note 90.
[199] Rao, *supra* note 29.
[200] Douglas W. Arner et al., *The Transnational Data Governance Problem*, 37 BERKELEY TECH. L.J. 623, 660—62 (2022).
[201] *How the Trend towards Data Localization Is Impacting the Financial Services Sector*, INT'L. REG. STRATEGY GRP. 14 (Dec. 2020), https://www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf.

adequate level of protection and, in the absence of such a decision, a controller or processor may transfer personal data only if appropriate safeguards are in place and enforceable rights and effective legal remedies are available.[202] Following Brexit, the UK enacted the Data Protection Act 2018, which includes general principles for the transfer of personal data similar to the GDPR.[203] A controller may not transfer personal data to a third country or an international organization unless the transfer is based on adequacy regulations, appropriate safeguards, or special circumstances.[204] The newly enacted Data Governance Act adopts a GDPR-like approach to conditional cross-border data flows.[205] These regulatory requirements have certain data localization effects in practice. In Australia, an Australian Privacy Principles entity may disclose personal information to an overseas recipient that is subject to a substantially similar data protection law or binding scheme.[206] Likewise, Brazil only permits the transfer of personal data to countries or international organizations that provide an adequate level of protection, or where the controller guarantees that the data transfer complies with data subject rights and the data protection regime in the LGPD.[207] According to the UAE legislation, personal data may be transferred and shared across borders if there is a proper level of protection, which includes rules related to the protection of data privacy and the exercise of data subject rights, as well as the existence of a supervisory authority to impose appropriate measures against the data controller or processor.[208] Under these regulatory regimes, a major challenge for global financial services companies is how to comply with and harmonize multiple types of data transfer requirements to ensure adequate data protection.

Second, a growing number of jurisdictions designate certain types of data as sensitive or critical, thereby restricting the transfer

---

[202] General Data Protection Regulation, *supra* note 161, arts. 45—46.
[203] Data Protection Act 2018 (U.K. Pub. General Acts 2018 c. 12), https://www.legislation.gov.uk/ukpga/2018/12/contents.
[204] *Id.* ss. 72—77.
[205] 'Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act)' 2022 *Official Journal L* 152 1.
[206] Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Austl. Compilation No. 1), sched. 1 cl. 8.2(a), https://www.legislation.gov.au/C2012A00197/latest/text.
[207] Lei Geral de Protecao de Dados Pessoais, *supra* note 174, art. 33.
[208] Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data (United Arab Emirates), art. 22, https://www.uaelegislation.gov.ae/en/legislations/1972/download.

of such data.[209] Specifically, in India, the RBI mandates that all payment data shall be stored only in onshore systems, including end-to-end transaction details, and information relating to payments or settlements such as the customer's name, the Aadhaar number, account details, and payment credentials.[210] Payment systems encompass clearing, payment, or settlement services involving credit cards, debit cards, smart cards, money transfers, or similar operations.[211] While there are no restrictions on processing cross-border payment transactions, the relevant data should be deleted from offshore systems and transferred back to India within 24 hours.[212] In addition to payment data, records of insurance policies and claims are also required to be stored only in data centers in India.[213] The RBI previously banned American Express Company and Diners Club International from issuing new cards to domestic customers as they were non-compliant with local data storage rules.[214] As a result, these data localization requirements increase infrastructure costs for payment service providers operating across borders and impair their ability to detect financial fraud.

Likewise, Mainland China has a restrictive policy stance on cross-border data transfers, which is not limited to personal information. The Cybersecurity Law enacted in 2016 requires critical information infrastructure operators (CIIOs) to store personal information and important data within China; if necessary to transfer such data abroad, a security assessment should be conducted in accordance with relevant regulations.[215] Critical

---

[209] INT'L. REG. STRATEGY GRP., *supra* note 201, at 30.

[210] The Reserve Bank of India issued a directive requiring system providers to store all payment data in India. *Storage of Payment System Data*, RSRV. BANK OF INDIA (June 26, 2019), https://www.rbi.org.in/commonperson/English/Scripts/FAQs.aspx?Id=2995.

[211] Payment and Settlement Systems Act, 2007 (Act No. 51 of 2007, dated Dec. 20, 2007) (India), s. 2(1)(i), https://www.indiacode.nic.in/bitstream/123456789/2082/4/a2007-51.pdf.

[212] RSRV. BANK OF INDIA, *supra* note 210.

[213] Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulation, 2015 (F. No. IRDAI/Reg/10/100/2015, dated Aug. 12, 2015) (India), s. 3(9), https://irdai.gov.in/document-detail?documentId=604674.

[214] Nupur Anand, *RBI Bans AmEx, Diners Club from Issuing New Cards for Violating Data Rules*, REUTERS (Apr. 23, 2021), https://www.reuters.com/article/idUSKBN2CA26S/.

[215] Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. of the Nat'l People's Cong. on Nov. 7, 2016, effective June

information infrastructure refers to important network facilities and information systems in crucial industries such as public communications and information services, energy, transportation, water, finance, public services, e-government affairs, and national defense, which may seriously endanger national security and public interests in the event of damage, loss of function, or data leakage.[216] Further, where CIIOs purchase network products and services, and network platform operators carry out data processing activities that affect or may affect national security, they are subject to a cybersecurity review.[217] More recently, the Cybersecurity Administration of China (CAC) issued detailed measures for the security assessment of outbound data transfers.[218] Under this regulation, the cross-border transfer of personal information and important data is forbidden unless specific conditions are met. Specifically, CIIOs and data processors that transfer important data abroad or export personal information beyond a prescribed volume threshold should undergo a security assessment to evaluate the adequacy of their safeguard measures.[219] However, there has been growing concern over the vague definitions of CIIOs and important data, as well as "uneven local implementation" in different industries.[220] These legal uncertainties will lead to increased compliance costs, especially for data-driven companies with

1, 2017), art. 37, https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm (China).

[216] Guanjian Xinxi Jichu Sheshi Anquan Baohu Tiaoli (关键信息基础设施安全保护条例) [Regulations on the Security Protection of Critical Information Infrastructure] (promulgated by the State Council on Jul. 30, 2021, effective Sep. 1, 2021), art. 2, https://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm (China).

[217] Measures for Cybersecurity Review, *supra* note 8, at art. 2.

[218] Shuju Chujing Anquan Pinggu Banfa (数据出境安全评估办法) [Measures for the Security Assessment of Outbound Data Transfers] (promulgated by the Cybersecurity Admin. of China on Jul. 7, 2022, effective Sep. 1, 2022), https://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm (China).

[219] *Id.* arts. 2-4; Cujin he Guifan Shuju Kuajing Liudong Guiding (促进和规范数据跨境流动规定) [Provisions on Promoting and Regulating Cross-Border Data Flows] (promulgated by the Cybersecurity Admin. of China on Mar. 22, 2024), art. 7, https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm (China).

[220] In practice, there are great differences in data classification and grading standards in different regions and industries. Inst. for Stud. on A.I. & L. of Tsinghua U., *Woguo Shuju Anquan Fa Shengxiao Yilai Xingzheng Zhifa Qingkuang Baogao (我国《数据安全法》生效以来行政执法情况报告) [Report on Administrative Enforcement of China's Data Security Law Since Its Entry into Force]*, ANQUAN NEICAN (安全内参) [SECRSS.COM] (Jun. 17, 2023), https://www.secrss.com/articles/55729.

overseas operations.

By comparison, in the US, Hong Kong, and Singapore, there are fewer restrictions on the storage, processing, and transfer of data. For example, Hong Kong is seeking to become a gateway for international digital service providers to develop data centers in the Greater China region, largely due to its permissive cross-border data regulations (which–like a large number of other jurisdictions around the world–are based on the previous EU Data Protection Directive) and well-established network capacity.[221] While the Office of the Privacy Commissioner for Personal Data (PCPD) sets out mandatory conditions for data transfer in the privacy protection legislation, the relevant provision has yet to come into force.[222] Instead, the PCPD has issued guidelines containing model contractual clauses for the cross-border transfer of personal data for voluntary compliance by data processors and users.[223] Given the close integration of the Greater Bay Area, the CAC, the PCPD, and the Innovation, Technology and Industry Bureau have jointly formulated a standard contract for cross-boundary flows of personal information to facilitate the provision of relevant services.[224] On this basis, an "early and pilot implementation" arrangement for the standard contract has been implemented in the banking, credit referencing, and healthcare sectors.[225] Hong Kong's financial

---

[221] *Cross-border data regulations in the European Union and South Korea*, RSCH. OFFICE OF THE LEGIS. COUNCIL SECRETARIAT 7 (Jan. 26, 2024), https://app7.legco.gov.hk/rpdb/en/uploads/2024/IN/IN02_2024_20240126_en.pdf.

[222] Office of the Priv. Comm'r for Personal Data, *Response to the media enquiry on Section 33 of PDPO and cross-border data sharing*, OFFICE OF THE PRIV. COMM'R FOR PERSONAL DATA (Sep. 23, 2019), https://www.pcpd.org.hk/tc_chi/news_events/media_enquiry/enquiry_20190923.html.

[223] *Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data*, OFFICE OF THE PRIV. COMM'R FOR PERSONAL DATA (May 2022), https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_model_contractual_clauses.pdf.

[224] *Guidance on Cross-boundary Data Transfer: Standard Contract for Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)*, OFFICE OF THE PRIV. COMM'R FOR PERSONAL DATA (Dec. 2023), https://www.pcpd.org.hk/english/resources_centre/publications/files/standard_contract_gba.pdf.

[225] *See Facilitating Cross-boundary Data Flow within the Great Bay Area*, DIGIT. POL'Y OFF., https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/mainland/cross-boundary_data_flow/ (last visited July 23, 2024).

industry is thus seeking to benefit from less restrictive policies on cross-border data transfers, leveraging its position as an innovation hub to develop digitally enabled services.

The policy stance of the U.S. and Singapore is generally against data localization. Specifically, the U.S. has no national data privacy law. However, there are state-level regulations that restrict government agencies or contractors from outsourcing data processing offshore, such as the California Consumer Privacy Act.[226] Given the growing importance of free data flows and digital economic activities, the U.S. policy objective is to minimize data localization measures. At the same time, in recent years, there have been increasing restrictions on data transfers from a national security standpoint, highlighting that this is in fact a global trend, and arguably one that is not going to reverse in the near future. In the case of Singapore, the MAS expressed concerns about the rise of data localization requirements, which might hinder the ability to aggregate, store, process, and transmit data across borders, especially in the digital age.[227] The regulatory challenge is how to enhance data connectivity while addressing issues of data sovereignty. The U.S. and Singapore recognize the increasing use of data and technology in the financial sector, and in line with their shared policy objectives, the Treasury and the MAS issued a joint statement on financial services data connectivity.[228] This allows financial service suppliers to transfer data, including personal information, across borders and opposes measures that restrict the storage and processing of data, as long as financial regulators have access to data needed for their supervisory mandates.[229]

From a comparative perspective, data localization measures have proliferated in recent years to address legitimate concerns about privacy and cybersecurity, or to ensure data access for law

---

[226] *The Extent and Impact of Data Localization*, FRONTIER ECON. LTD. 65—67 (June 1, 2022), https://assets.publishing.service.gov.uk/media/63a1a2e88fa8f539198d9bb5/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf.

[227] Monetary Authority of Sing., *"Singapore FinTech: Innovation, Inclusion, Inspiration" – Presentation by Mr. Ravi Menon, Managing Director, Monetary Authority of Singapore at Singapore FinTech Festival 2018 on 12 November 2018*, MONETARY AUTH. OF SING. (Nov. 12, 2018), https://www.mas.gov.sg/news/speeches/2018/singapore-fintech.

[228] *United States-Singapore Joint Statement on Financial Serv. Data Connectivity*, MONETARY AUTH. OF SING. (Feb. 6, 2020), https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity.

[229] *Id.*

enforcement and regulatory oversight, as well as more recently as a result of national security, competitiveness, or human rights concerns. Many jurisdictions require certain types of data to be stored on local servers or restrict the free flow of data across borders. These restrictive data policies pose a serious challenge to financial service providers, especially those with global reach, and weaken their multi-jurisdictional risk management practices.[230] While some regulators have bilateral data sharing arrangements, the general trend towards data localization is likely to undermine the benefits of digital finance that increasingly relies on cross-border data access, processing, and transfers. One study found that data localization requirements could lead to considerable economic losses.[231]

As such, a key issue in Open Finance governance is how to facilitate data connectivity in the context of growing cross-border financial activity while protecting data security. This will be particularly important for smaller jurisdictions. Larger jurisdictions (with sufficient data ecosystem scale) are likely to be largely designed with the internal market in mind. Nonetheless, linkages to other markets is a significant aspect of building Open Finance.

C. ASYMMETRY OF OPEN FINANCE DATA

Open Finance aims to foster competition between incumbents and new entrants in financial services by increasing access to and sharing of customer data, both through breaking down barriers to control particularly by incumbents but also by empowering consumer to control and share their own data, wherever it may be held. However, the lack of reciprocity in data sharing frameworks can lead to an asymmetry between market participants.[232] For example, the PSD2 only mandates banks to provide third-party service providers with access to payment account data, but third parties are not subject to the same requirements to share customer data.[233] This asymmetry is very likely to create competitive advantages for third-party service providers, especially for BigTechs

[230] INT'L. REG. STRATEGY GRP., *supra* note 201, at 47—50.
[231] Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, INFO. TECH. & INNOVATION FOUND. 10—17 (Jul. 2021), https://www2.itif.org/2021-data-localization.pdf.
[232] Brad Carr, *From Open Banking to Open Data and Beyond: Competition and the Future of Banking*, in OPEN BANKING (Linda Jeng eds., 2022).
[233] The Second Payment Services Directive, *supra* note 5.

that have large amounts of nonpayment-related data on their customers, such as e-commerce transactions and social media. Given the importance of data in the digital economy, there are growing concerns about asymmetric data sharing and its negative impact on Open Finance.

In jurisdictions with a mandatory approach to Open Finance, licensed financial institutions such as banks and payment service providers are required to share their customer data at the direction of consumers with authorized third parties.[234] Under this data sharing framework, third parties are able to access and aggregate customers' financial information, hopefully with sufficient scale to empower datafication and attractive services and business models, thus facilitating entry into financial services, with competition supporting innovation, consumer, economic and societal benefits. However, the data asymmetry is likely to exacerbate the existing problem of market concentration in the hands of a few large FinTech players.[235] According to the FCA's report, the asymmetry of data and data sharing mechanisms between BigTechs and financial service firms could adversely affect how competition evolves in retail financial markets.[236] There are several potential risks associated with the data asymmetry, including barriers to entry and expansion in financial markets, the gatekeeper role of BigTechs in retail financial services, and the concentration of financial services firms' partnerships with a few BigTechs.[237] The existing regulatory framework is not sufficient to mitigate these adverse impacts of the data asymmetry, especially in the context of Open Finance, which allows BigTechs greater access to customer financial data. Despite the original intention to create a level playing field among Open Finance participants, asymmetric data sharing may have the opposite effect on market competition. In addition, the massive amount of data that BigTechs collect from diversified online activities can be used for customer authentication and fraud detection.[238] Nevertheless, due to the lack of data sharing reciprocity,

---

[234] See *supra* note 85, at Part III.A.
[235] *Reciprocity in Customer Data Sharing Frameworks*, INST. INT'L FIN. 2 (Jul. 2018), https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_frameworks_20170730.pdf.
[236] *Potential Competition Impacts from the Data Asymmetry between Big Tech Firms and Firms in Financial Services*, FIN. CONDUCT AUTH. (Apr. 22, 2024), https://www.fca.org.uk/publication/feedback/fs24-1.pdf.
[237] *Id.* at 5—7.
[238] *Id.* at 21—22.

it is difficult for financial institutions to access data exclusively held by BigTechs. Coupled with the fact that many BigTechs operate outside the purview of financial regulators, the data asymmetry may increase the opacity of Open Finance services and pose a threat to the stability of financial markets.

While some jurisdictions have not taken a mandatory approach to Open Finance, the problem of asymmetric data sharing between large FinTechs and financial institutions also exists. For example, in Mainland China, BigTechs such as Ant Group have invested significant resources in building customer databases and technology infrastructure to maintain data-enabled competitive advantages and expand their influence in financial services.[239] These firms' exclusive access to and control of customer data creates a barrier to entry for smaller competitors, reinforcing their monopolistic practices in the market. The PBOC actively supports the establishment of market-based credit reporting agencies to promote information sharing, meaning BigTechs with massive customer data and advanced analytics capability are regarded as important sources of information. However, sharing customer data with other market players can incur high costs and cause BigTechs to lose their competitive advantages. As a result, they have little incentive to provide customer data to financial institutions and other participants in the credit reporting business.[240] In the absence of reciprocity in data sharing, the major concern is that large FinTechs can scale up their operation in financial markets by leveraging customer databases of other institutions involved in the credit reporting system. Open Finance, which encompasses broader sharing of customer financial data on a voluntary basis, is likely to exacerbate this concern.

By comparison, India observed that certain entities eligible to participate in the Account Aggregator ecosystem as financial information providers only registered as financial information users, and thus did not share their customer data.[241] As such, the RBI has modified the open banking rules to ensure efficient and optimal use

---

[239] Robin Hui Huang & Christine Menglu Wang, *Fintech-Bank Partnership in China's Credit Market: Models, Risks and Regulatory Responses*, 24 EUR. BUS. ORG. L. REV. 721, 730 (2023).
[240] Wang et al., *supra* note 117.
[241] *Joining the Account Aggregator Ecosystem as Financial Information User*, RSRV. BANK OF INDIA (Oct. 26, 2023), https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI773109DABBDE4E4E27B93AB7325962E43A.PDF.

of the Account Aggregator network, requiring regulated entities joining as financial information users to also provide specified financial information. [242] Likewise, reciprocity is one of the principles of Brazil's Open Finance regime and therefore all participating institutions that receive financial data must also share their data and services.[243]

As a jurisdiction adopting mandatory Open Finance rules, Australian regulators have emphasized creating a level playing field among participating institutions through reciprocal data sharing. During the consultation process on the CDR rules, the ACCC considered incorporating a principle of reciprocity into the legislation, under which participants receiving data through the CDR would be obliged to also provide equivalent data at the direction of a consumer.[244] Under the existing regulatory regime, reciprocal obligations may arise if an accredited data recipient is requested to disclose some or all of the CDR data within the scope of any designation instrument.[245] Given the growth of participation in the CDR ecosystem, it is recommended to extend the cross-sectoral application of reciprocal requirements and issue guidelines on the identification of equivalent data.[246] Despite some concerns about the expansion of reciprocity, this data sharing rule has been critical to the development of Australia's Open Finance framework.[247]

Reciprocity in data sharing between financial institutions and third parties, especially large FinTech firms, must be an important principle in building Open Finance governance.

The implementation of Open Finance in many jurisdictions

---

[242] Master Direction – Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, *supra* note 129, art. 7.7.

[243] *See Open Finance*, BANCO CENT. DO BRAZ., https://www.bcb.gov.br/en/financialstability/open_finance (last visited Jul. 23, 2024).

[244] *Consumer Data Right Rules Framework*, AUSTL. COMPETITION & CONSUMER COMM'N 21 (Sep. 2018), https://www.accc.gov.au/system/files/ACCC%20CDR%20Rules%20Framework%20%28final%29.pdf?ref=0&download=y.

[245] Competition and Consumer Act 2010, *supra* note 58, s. 56AJ. Competition and Consumer (Consumer Data Right) Rules 2020, *supra* note 59, rules 4.7(A)-(B).

[246] *Treasury Laws Amendment (Consumer Data Right) Bill 2022 Explanatory Memorandum*, H.R. OF THE PARLIAMENT OF AUSTL. 64-65 (2022), https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6950_ems_8554d9e8-6126-4d11-ac3c-0ef16cec05ce/upload_pdf/JC008246.pdf;fileType=application%2Fpdf.

[247] Francesco De Pascalis, *The Journey to Open Finance: Learning from the Open Banking Movement*, 33 EUR. BUS. L. REV. 397, 416 (2022).

aims to facilitate the entry of more market players into financial services through greater access to customer data. However, the eventual outcome of this initiative may be unfair competition, as BigTechs with advanced technology can make better use of customer information than smaller third-party service providers and reap the benefits of asymmetric data sharing by financial institutions.[248] The lack of reciprocal rules in Open Finance poses a serious challenge to the policy objective of creating a level playing field between incumbents and new entrants in financial services. In addition to traditional financial information, the data collected by BigTechs from a broad range of online activities can also reveal additional insights into customers' risk profiles, and therefore is valuable for the provision of financial services. Due to the data asymmetry, it is difficult to ensure the accessibility of non-traditional financial information in Open Finance, which has a negative impact on regulatory transparency.

V. FROM OPEN FINANCE TO OPEN DATA

Open Finance is seen as potentially bringing significant benefits to finance, through empowerment, inclusion, competition, and datafication, and also through broad participation of service providers and increased access to customer data. However, a number of clear issues have emerged with governance approaches to building Open Finance, including regulatory fragmentation, data localization requirements, and asymmetric data sharing. A major challenge is how to improve the existing regulatory framework to maximize the value of Open Finance data, while addressing the complex interplay of financial regulations, data protection laws, technical standards, and other infrastructure. More importantly, as the economy has become increasingly digitalized, it is worth considering a shift from sector-based Open Finance towards a broader Open Data framework.

A. HARMONIZING OPEN FINANCE REGULATIONS AND STANDARDS

Building Open Finance involves multiple regulators that prioritize different policy objectives, including financial regulatory objectives, data security and consumer protection, market efficiency and competition, and competitiveness. This raises the need to

[248] Arner et al., *supra* note 4.

address fragmentation of Open Finance regulations. As discussed earlier, data protection is a key component in the broad Open Finance framework, and there is sometimes a trade-off between financial and data regulatory objectives. In some jurisdictions that adopt a mandatory approach, such as the EU, the UK, and Australia, the coordination failure between financial regulation and data protection requirements presents a serious challenge to Open Finance governance. This coordination failure may restrict access to customer financial data or increase the complexity of regulatory compliance, thereby impeding the development of Open Finance.[249]

Due to multi-disciplinary features of Open Finance, a series of regulators must coordinate their efforts to address issues related to data sharing between financial institutions and third-party service providers.[250] For example, with the introduction of the UK's data protection legislation, the Information Commissioner's Office (ICO) plays an important role in overseeing data-related businesses such as Open Finance, thereby having more intersections with other regulators.[251] To avoid potential regulatory conflicts, the Digital Regulation Cooperation Forum (DRCF) was established to ensure greater coordination between the ICO, the CMA, and the FCA.[252] As a voluntary cooperation forum, the DRCF facilitates engagement between these member regulators on emerging digital issues of mutual concern, but does not provide them with formal advice. Where regulatory regimes intersect, the ICO may face resource constraints or have a different understanding of Open Finance services than other regulators, in which case the DRCF helps pool expertise and tools needed to fulfill their supervisory mandates and promote coherent policy development and enforcement.[253] Through regular meetings between different regulators, this initiative can establish harmonization of Open Finance regulations, achieving greater certainty and consistency in the application of related but

---

[249] *See supra* Part IV.A.

[250] BANK FOR INT'L SETTLEMENTS, *supra* note 16, at 5.

[251] *Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues*, ORG. FOR ECON. CO-OPERATION AND DEV. 20-21 (Feb. 2023), https://www.oecd-ilibrary.org/docserver/6c872949-en.pdf?expires=1721896631&id=id&accname=guest&checksum=5428647CD1CE6BCC1B1F3A10A87B44A1.

[252] *See About the DRCF*, DIGITAL REG. COOPERATION FORUM, https://www.drcf.org.uk/about-us (last visited Jul. 23, 2024).

[253] Competition & Mkt. Authority, *DCRF Terms of Reference (ToR)*, GOV.UK (Sep. 5, 2022), https://www.gov.uk/government/publications/drcf-terms-of-reference/terms-of-reference.

different rules.

Likewise, in March 2022, the ACCC and three other Australian regulators responsible for media and broadcasting, data and privacy protection, and online safety formed the Digital Platform Regulators Forum (DP-REG) to share information and collaborate on cross-cutting issues related to the regulation of digital platforms.[254] These regulators face many of the same challenges, such as balancing data-driven innovation and consumer protection, and limiting harms from the market power of large platforms. Through collaboration on research and consultation with stakeholder groups, the DP-REG aims to build a broad consensus on innovative technologies and business models and minimize unnecessary regulatory overlaps.[255] Open Finance governance needs to consider the intersection of multiple regulatory objectives and the involvement of different market players. It is difficult for a single regulator to examine and address cross-sectoral risks associated with Open Finance services. The collaborative forums in the UK and Australia provide an important reference for jurisdictions seeking to develop and implement proportionate, coherent, and responsive Open Finance regulation.

Alternatively, an independent body could be established to issue general guidance, such as guidelines, recommendations, and best practices, to promote a common understanding of relevant laws and ensure consistency in regulatory action. In the EU, there is a divergence between the provisions on data processing under general data governance and those under Open Finance regulation. Specifically, the European Data Protection Board has raised concerns about the interpretation of rules related to data protection and the interplay between the GDPR and the PSD2.[256] In response, it provides clarification on the relationship between relevant regulatory requirements, such as different notions of explicit consent, the processing of special categories of personal data, and the application of main data protection principles. [257] These

---

[254] *DP-REG Terms of Reference*, DIGITAL PLATFORM REGS. FORUM (Sep. 16, 2022), https://dp-reg.gov.au/publications/dp-reg-terms-reference.

[255] Gina Cass-Gottlieb, the ACCC chair, delivered a speech on 'Regulatory Intersections between Competition, Consumer and Privacy Laws' at the Asia Pacific Privacy Authorities 60th Forum (Nov. 30, 2023), https://www.accc.gov.au/about-us/media/speeches/regulatory-intersections-between-competition-consumer-and-privacy-laws-speech.

[256] Arner et al., *supra* note 160, paras. 1-3.

[257] *Id.*

guidelines are useful for financial institutions and third-party service providers to determine their compliance with Open Finance regulations, especially when facing complex regulatory intersections.

Internationally, different Open Finance governance frameworks have been developed, including mandatory, collaborative, ecosystem, and market-led approaches. Given the growing cross-border data transfers, differences in these regulatory frameworks may create uncertainty and inconsistency for global financial service providers. While there is so far no one-size-fits-all approach to Open Finance, an international organization could initiate a dialogue among regulators in different jurisdictions to reach an agreement on minimum governance principles.[258] For example, in the context of finance, the Bank for International Settlements (BIS) has a well-developed framework for international cooperation and responsible information sharing. By collaborating with several central banks and monetary authorities, the BIS Innovation Hub launched Project mBridge to tackle some of the key inefficiencies in cross-border payments and settlement.[259] This project has established a multi-central bank digital currency platform shared among participating institutions and created a bespoke governance framework tailored to match the platform's unique nature.[260] Inspired by such experience, international organizations such as the BIS can consider designing a strategic framework for global digital economy cooperation to mitigate the fragmentation of Open Finance regulations.[261] The involvement of data protection, competition authorities, and industry is also needed. The global dialogue on Open Finance issues will strengthen engagement with regulators across jurisdictions to share best practices on governance approaches and gather insights on how to create interoperability between regulatory regimes.

Furthermore, the lack of common technical standards for Open Finance data sharing has led to multiple networks between financial institutions and third-party service providers, which increase

---

[258] ORG. FOR ECON. CO-OPERATION AND DEV., *supra* note 251, at 22.

[259] Bank for Int'l. Settlements, *Project mBridge Reaches Minimum Viable Products Stage and Invites Further International Participation*, BANK FOR INT'L. SETTLEMENTS (Jun. 5, 2024), https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.

[260] *Id.*

[261] *Strategic Framework for Digital Economic Cooperation: A Path for Progress*, INST. OF INT'L FIN. (Apr. 2022), https://www.iif.com/portals/0/Files/content/PathForProgress_Final.pdf.

regulatory complexity and costs.[262] Some jurisdictions, such as the UK, Australia, Brazil, and India, have developed a set of technical specifications to improve the consistency and compatibility of APIs. In Singapore, Hong Kong, and Mainland China, there are recommended API standards and relevant industry practices. As the use of APIs is essential to facilitate secure access to and the sharing of customer data, the adoption of different technical standards across the market may pose challenges to data interoperability and system compatibility among financial service providers.[263] Thus, a minimum level of standardization and harmonization is required to provide the technical foundation for Open Finance. Given the rapidly evolving nature and complexity of APIs, regulators may have limited skills and expertise in understanding relevant technical details. It is worth considering collaborating with the private sector and standard-setting bodies to establish common technical specifications for API and data interoperability.[264] The BIS launched a consultative group to promote greater cooperation in the area of innovation and the digital economy, with the aim of developing public technological infrastructures and key APIs for Open Finance.[265] This group has published a series of reports to provide minimum technical requirements for the central validator API architecture[266] and present technological considerations for API implementation, such as design patterns, protocols and standards, and security mechanisms.[267] Although nonbinding, these technical initiatives can serve as a useful reference for jurisdictions to harmonize API and data sharing standards among Open Finance participants.

B. TOWARDS OPEN DATA

In addition to the harmonization of Open Finance regulations, some jurisdictions have expanded the scope of data sharing beyond the financial sector to other industries, thus moving towards a broader Open Data framework. For instance, Australia imposes data

---

[262] *See supra* Part IV.A.
[263] Borgogno & Colangelo, *supra* note 19, at 591.
[264] INST. OF INT'L FIN., *supra* note 235, at 10.
[265] *See Consultative Council for the Americas – Consultative Group on Innovation and the Digital Economy*, BANK FOR INT'L. SETTLEMENTS, https://www.bis.org/about/repoffice_americas/cca.htm (last visited Jul. 23, 2024).
[266] BANK FOR INT'L. SETTLEMENTS, *supra* note 194, at 11-17.
[267] *API Standards for Data Sharing (Account Aggregator)*, BANK FOR INT'L. SETTLEMENTS 19-26 (Oct. 2022), https://www.bis.org/publ/othp56.pdf.

sharing obligations on CDR data holders, which currently covers the banking, energy, and nonbank lending sectors (as mentioned, the roll-out of the regime in telecommunications has been temporarily put on hold); in India, the data sharing system, while initially implemented in the financial sector, is expanding into healthcare and e-commerce; data exchange platforms built in Singapore and Hong Kong connect data providers and users in different areas, such as finance, payment, trade, and supply chain. [268] Under these frameworks, data interoperability is central to facilitating access, transfer, and use of customer data across digital services.

The arguments for Open Data are similar to those for Open Finance. However, the challenge is that, while finance is one of the most heavily regulated industries around the world, other sectors are relatively less regulated and therefore less subject to the direction of the financial regulator, finance ministry, or central bank in the context of building Open Data as compared to building Open Finance. As highlighted above, other regulated sectors (such as energy, telecommunications, or health) may be one approach. Another is to focus on enabling data infrastructure, as has been done in India or in Singapore (with MyInfo).

The trend towards data localization in many jurisdictions has posed a major challenge to free flows of customer data. Despite the importance of protecting data sovereignty, [269] the localization measures have incurred economy-wide costs, such as reducing connectivity of digital trade, undermining cybersecurity best practices and fraud prevention, and hindering data-driven innovation. [270] One possible solution to this issue is to focus regulation on data access, rather than its location.[271] Coupled with the use of new technologies for data storage and processing, regulators can take steps to increase data sharing across sectors and borders, as long as they have access to data needed for law enforcement and supervisory mandates. This approach has great potential to maximize the value of data in growing cross-border

---

[268] *See supra* Part III.

[269] Emily Wu, *Sovereignty and Data Localization*, BELFER CTR. FOR SCI. AND INT'L AFFS. 5-8 (Jul. 2021), https://www.belfercenter.org/sites/default/files/2021-07/SovereigntyLocalization.pdf.

[270] *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy*, INST. OF INT'L FIN. 4 (Dec. 2020), https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.

[271] INT'L. REG. STRATEGY GRP., *supra* note 201, at 58.

digital services while addressing regulatory concerns about data sovereignty. In the absence of global frameworks, Singapore provides an example for developing compatible and interoperable data sharing mechanisms. The MAS, in collaboration with domestic industry groups and overseas regulators, has implemented a number of data exchange initiatives, such as the SGFinDex[272] and the joint statement with the Treasury on financial data connectivity.[273] Singapore has also signed digital economy agreements with Australia and the UK, covering the areas of artificial intelligence, data innovation and protection, and digital identities.[274] These arrangements establish rules to support data access and transfer for digitally enabled activities, including financial services.[275] In the increasingly digitalized economy, an Open Data framework that involves a broader range of participants and data can coordinate cross-sectoral efforts to overcome the fears motivating data localization policies.

Furthermore, the lack of reciprocity in data sharing between financial institutions and third-party service providers has led to an unlevel playing field. With greater access to customer financial information, BigTechs leverage their competitive advantage in data analytics to rapidly expand into finance and create a barrier to entry for other market players.[276] Given the adverse impact of asymmetric data sharing on competition, there is a need to incorporate the principle of reciprocity into Open Finance governance. Under this principle, third parties benefiting from financial information shared through the Open Finance system are obliged to make their data available at the direction of customers. However, differing views on the definition of equivalent data in the sector-based Open Finance

---

[272] MONETARY AUTHORITY OF SING., *supra* note 227.
[273] U.S. Dep't of the Treasury, *United States – Singapore Joint Statement on Financial Services Data Connectivity*, U.S. DEP'T OF THE TREASURY (Feb. 5, 2020), https://home.treasury.gov/news/press-releases/sm899.
[274] Singapore has concluded negotiations on four digital economy agreements, two of which, signed with Australia and the United Kingdom respectively, have entered into force. *See Digital Economy Agreements*, MINISTRY OF TRADE AND INDUS. SING., https://www.mti.gov.sg/trade/digital-economy-agreements (last visited Jul. 23, 2024).
[275] *See Singapore-Australia Digital Economy Agreement*, MINISTRY OF TRADE AND INDUS. SING., <https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement (last visited Jul. 23, 2024); *UK-Singapore Digital Economy Agreement*, MINISTRY OF TRADE AND INDUS. SING., https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/UKSDEA (last visited Jul. 23, 2024).
[276] *See supra* Part IV.C.

context are very likely to increase the complexity and uncertainty of introducing reciprocal sharing requirements.[277] In response, it is worth considering extending the application of reciprocity rules beyond Open Finance data to cross-sector data sharing. This more open system can aggregate troves of non-financial data from BigTechs' digital activities, such as e-commerce transactions and social networks, enabling all participating institutions to access the same data pool.[278] The shift to Open Data would alleviate the problem of unfair competition caused by asymmetric data sharing, while facilitating customer authentication and financial fraud detection.

In terms of public infrastructure, a digital identity and consent management system lays the foundation for the implementation of Open Data involving different industry players. For example, India Stack generates important synergies of a digital identity system, an interoperable payments network, and regulatory mechanisms for data sharing, which allows it to authenticate individuals for a wide range of businesses and expand access to financial services.[279] As part of the consent manager mechanism, the establishment of Account Aggregators in India facilitates the secure transfer of customer data and improves interoperability between financial service providers. This digital infrastructure enables customers to easily prove their identity and separately manage consent for data sharing across sectors, thus reducing the cost of complying with e-KYC and privacy protection requirements.[280] Moreover, in Singapore, the national digital identity (Singpass) empowers customers to grant consent for data sharing and access online services ranging from finance to healthcare, education, and transportation.[281] Building on the underlying system for individual identity verification, sector-based data infrastructure has been developed to aggregate customer information spread across multiple

---

[277] H.R. OF THE PARLIAMENT OF AUSTL., *supra* note 246, at 66.
[278] INST. OF INT'L FIN., *supra* note 235, at 3.
[279] Carriere-Swallow et al., *supra* note 77, at 16-18.
[280] *The Ecosystem Imperative: Digital Transformation of Financial Services and Moving From Open Banking to Open Data*, INST. OF INT'L FIN. & DELOITTE 13 (Jun. 2023), https://www.iif.com/portals/0/Files/content/32370132_final_report_-_open_data_22_june.pdf.
[281] *National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX*, THE WORLD BANK & GOV'T TECH. AGENCY OF SING. 5-6 (Oct. 2022), https://documents1.worldbank.org/curated/en/099300010212228518/pdf/P171592079b3e50d70a1630d5663205bf94.pdf.

government agencies and participating institutions.[282] Given the adoption of common standards and formats, Singpass ensures access to authoritative databases and builds trust in digital services. Inspired by these experiences, the establishment of public infrastructure for digital identity and consent management is needed to move towards Open Data.

VI. CONCLUSION

Over the past decade, the building of Open Finance in a number of major jurisdictions is beginning to have a significant impact on financial services by improving access to customer data, empowering consumers, breaking incumbent data control, and bringing new entrants to finance. As the financial sector has become increasingly digitalized, Open Finance presents a potentially important opportunity for innovation and market competition. In building Open Finance, governance, design, and infrastructure are central. Different governance frameworks for Open Finance are evolving around the world, including mandatory requirements, collaborative arrangements, ecosystem approaches, and voluntary initiatives. The EU led in mandating Open Banking, with the introduction of PSD2. Following this approach, other jurisdictions such as the UK, Australia, Brazil, and the UAE have established regulatory regimes for Open Finance, addressing scale of participation, scope of data sharing, and degree of technical standardization. In contrast, financial regulators in Singapore and Hong Kong have collaborated with industry to actively support the development of Open Finance and publish recommended API standards. China and India have both developed comprehensive mandatory data aggregation strategies. In the US, industry associations have promoted Open Finance practices and regulatory involvement has been limited, mainly by issuing nonbinding guidance. More recently, the CFPB has proposed a mandatory rule governing personal financial data rights.

Despite the potential benefits of Open Finance, the governance frameworks required to build it involve a complex interaction between laws and regulations focusing across different objectives including financial regulation, data security and customer protection, competition, and national security, and thus raise a range of concerns. First, since rules governing financial data sharing in Open Finance

[282] *Id.* at 48-49.

are implemented by multiple authorities, there is a serious issue of regulatory fragmentation. The lack of common technical standards and the economic cost of API development also challenge Open Finance governance. Furthermore, some jurisdictions have strengthened the implementation of data localization measures to maintain digital sovereignty. However, this restricts the free flow and sharing of customer data, especially in growing cross-border financial activities, which conflicts with the development of Open Finance. In addition, the asymmetry of data sharing between financial institutions and third-party service providers can lead to an unlevel playing field, exacerbating the risk of market concentration in the hands of a few large participants.

Based on a comparative analysis of regulatory experience, we highlight several ways to address the complex interplay of financial regulations, data protection laws, technical standards, and infrastructure necessary to build Open Finance. Due to the multi-disciplinary nature of Open Finance services, coordination is necessary between regulators and industry to ensure policy coherence and to create interoperability between different governance frameworks within and across jurisdictions. In most cases, a combination of a law on general data protection combined with specific legislation for Open Finance (and other sectors in the context of Open Data) will be most effective. It is increasingly clear that mandatory approaches to Open Finance are more successful than those which are industry led. It is also clear that approaches which cover not only banking but all aspects of finance are likely to yield the greatest eventual impact. There are clear lessons for the US in this respect. Where financial and data regulatory regimes intersect, it is important to establish a forum to share information and collaborate on cross-cutting issues of Open Finance governance. This is a clear area where more could be done in the US, with significant lessons from the ecosystem and systemic approaches of India, Brazil, the EU, Australia, and China. In addition, guidance such as guidelines and best practices can promote a common understanding of Open Finance rules and improve consistency in regulatory action. A minimum level of API standardization and harmonization is also required to build the technical foundation for Open Finance. This can often be supported and enabled through digital infrastructure including credit registries, digital identity, and other mechanisms to enable sharing. More importantly, in response to the increasing digitalization of the economy, there is a great need

to expand the scope of data sharing from the financial sector to other industries, in most cases focusing initially on other regulated industries such as energy, telecommunications, transport, and health, and thus move towards a building not only Open Finance but also Open Data.