Regulating Data Markets through Open Banking: Lessons for South Africa

WORKING PAPER CC2021/01

Godknows Giya, Salma Kagee and Tankiso Thibane

Abstract

This research explored the approaches to Open Banking adopted globally and draw lessons for the implementation of Open Banking in South Africa. The research is premised on the fact that despite the existence of potential benefits of Open Banking, South Africa is still lagging in terms of Open Banking implementation. The research found that the key pillars that have a bearing on Open Banking implementation include the type of data involved, data ownership, payment for data, opening of APIs and data privacy and security. As such, for Open Banking implementation to be a success in South Africa regulatory guidance is needed on these aspects. International experiences show that there is no universal approach adopted in Open Banking with countries adopting either a market-led or regulatory led approach while others transition from market led to regulatory led regimes.

In South Africa, this research observes that due to the economic incentives of banks in a highly concentrated market, a regulatory led approach may be appropriate. Notwithstanding, this research notes that whichever approach is pursued in South Africa, i.e., whether a market-led, or regulatory-led approach, relevant regulators including the Information Regulator must provide direction on the main pillars of Open Banking. This research has also observed that while not yet an imminent threat, the Open Banking initiative may invite the entry of BigTech firms and not just Fintech start-ups into the financial system. Given potential systemic risks and potential competition concerns raised by the entry of Bigtechs, a pre-emptive approach must be adopted regarding the involvement of Bigtechs in the South African financial market.

Keywords: Open banking; competition; regulation; data sharing and access; Bigtechs; APIs
1. Introduction

Increased digitalisation has reshaped business interactions in various markets, with data acting as a catalyst for innovation and competition. Open Banking is premised on data access and leveraging of customer data to enable innovation and competition through, inter alia, risk profiling and customer targeting. Open Banking initiatives have increasingly gained traction globally with the technology-driven innovation in the financial services sector (Fintech) and large technology companies (BigTech firms) using technologies to develop new services and business models. These initiatives enable third-party providers (TPPs) to access customer banking and financial data.

Notably, Open Banking is facilitated by Application Programming Interfaces (APIs), which provide real-time secure access to customer data. This is to bridge the gap between established databases and core systems by banks, and other financial institutions and third parties. In Open Banking, there are two distinct third parties i.e., Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).

The approach to Open Banking can either be market-led (i.e., voluntary) or regulatory-led, (i.e., mandatory). A detailed discussion of these approaches is presented in Section 2 below. What is important to note is that whether the approach is market-led or regulatory-led, some rules are required to guide contracting for data access between incumbent banks and third-party firms. Also important to note is that whichever approach may be adopted, it is acknowledged that Open Banking promotes greater competition by enabling Fintechs to innovate and by forcing incumbents to also innovate. The benefits of Open Banking may also be realised by small businesses through quicker turnaround on loan applications and faster decisions based on accurate, personalised

---


4 Monocle Research Team. 2020. OPEN BANKING: DISRUPTION OR DISTRACTION? Accessed at: [https://www.monocle.co.za/ViewPosts.aspx?Art=Open+Banking%3a+Disruption+or+Distraction%3f&Category=Insights&utm_term=banking%20api&utm_campaign=Open+Banking&utm_source=adwords&utm_medium=ppc&hsa_acc=910913260&hsa_cam=12446790664&hsa_gclid=EAIaIQobChMIzfnM49io8gI_vCw2-4k07jTwEAAYASAAEgITV_D_BwE]

5 AISPs are TPPs that are authorised to retrieve account data from banks and financial institutions with consent from the account holder.

6 PISPs are TPPs that are authorized to initiate payments out of or into a user’s bank account using the bank’s own payment systems.
insights. Despite the existence of potential benefits, South Africa is still lagging in terms of Open Banking implementation.

Lessons can be drawn from other countries that are already at the forefront of implementing Open Banking. Notably, Open Banking regimes differ across countries but generally encompass key elements such as implementation timelines, the range of product and service offerings, the type of data and the manner it must be shared, as well as the type of institutions and third parties involved. In some countries, the regulatory frameworks go beyond third-party data access to include provisions on whether third parties can share and/or resell data onward to fourth parties. Another important dynamic is whether data can be utilised beyond the original consent of a consumer and whether financial institutions such as banks or third-party firms must be compensated for sharing data.°

While Open Banking benefits exist, South Africa is lagging as currently there has been no regulatory directive regarding the implementation of Open Banking. Wider access to financial data held by incumbent banks and other financial institutions can go a long way in promoting market entry and economic participation, as new entrants and SMEs can leverage this data and create new products in the market at a lower cost leading to more product diversity. This may also facilitate the switching of providers through expanded choices available to consumers.® By reducing switching costs and promoting multi-homing, it allows firms and consumers to simultaneously enjoy services and products offered by different providers, while stimulating competition between these providers and constraining the market power of incumbents.

Some debates have already commenced between relevant stakeholders regarding Open Banking in South Africa such as on the Intergovernmental Fintech Working Group (IFWG) forum established in 2016.° The IFWG, amongst others, consists of financial sector regulators (i.e., prudential and market conduct authorities), the competition authorities and industry players such as banks.°° However, there is still a vacuum in terms of guidance and rules that are required to move Open Banking forward. Contracting between traditional banks and Fintechs and other players, particularly for data access, is critical for the successful implementation of Open Banking. As with any other market, some guidance and rules are necessary to provide certainty for contracting

---

9 The overall objective of the IFWG is to foster fintech innovation while ensuring a continued efficient functioning of financial markets, financial stability, and protecting the rights and interests of customers and investors.
parties to operate effectively. The nature of contracting depends on the Open Banking approach adopted by a country, i.e., whether the country adopts a market-led or regulatory-led approach.

What seems to be prevalent in other countries is that whichever approach is adopted, regulatory guidance has been provided including recommended standards (i.e., published open API standards and technical specifications)\(^\text{11}\). Thus, even if a market-led approach is adopted, there is a need for supervision on key pillars for Open Banking. Considering experiences in other countries, generally whether a market-led, or regulatory-led regime is adopted, guidance is provided around the following key pillars of Open Banking: type of data involved; ownership of data; payment for data; development of APIs, and; data privacy and security.

This research follows a qualitative approach relying on review of secondary sources of information which include textbooks, journals, unpublished manuscripts, previous studies, legislations and the Internet. The paper is organised as follows: firstly, it highlights the approaches to Open Banking adopted in other jurisdictions. Secondly, it provides lessons that can be drawn from international jurisdictions on Open Banking approach that can be adopted in South Africa, considering the country’s unique economic context and regulatory framework. Thirdly, the research highlights the key pillars for the successful implementation of Open Banking. Fourthly, the research considers that the entry of Bigtech firms in the financial services markets has raised some competition concerns, with implications on data sharing going forward. In this regard, the research also evaluates how Bigtechs can be treated in the South African context. Lastly, the research provides conclusions summarising key observations.

2. APPROACHES TO OPEN BANKING IN INTERNATIONAL JURISDICTIONS

Globally, there is no universal approach adopted in the governance of data access in Open Banking. In Mexico, for example, the 2018 Fintech law establishes data-sharing requirements across all financial sector entities, and forthcoming changes in the national payments system. This is to allow for third parties to initiate payments. India has gone one step further by building an open payments system under the National Payments Corporation of India (NPCI), called the Unified Payments Interface (UPI). The Indian government has further created a new type of institution for sharing customers’ financial data, called an Account Aggregator. Mexico’s new Fintech law is a good example of an effort to widen the data supply. It places a data-sharing obligation upon banks, payment service providers, credit cooperatives, insurance providers, money remitters, and licensed Fintech firms12.

In Africa, most countries are yet to implement Open Banking regimes. However, financial sector regulators (including monetary authorities) have taken the lead in promoting and offering guidelines on the rolling out of these frameworks13. Few countries have enforced clear legislative rules for Open Banking and there are promising developments in some of these countries. For instance, Nigeria recently announced their own regulatory framework establishing principles for data sharing between banks and Fintechs. Their regulations, amongst other things, govern data access, technical and information security standards. However, arising concerns pertain to data protection, dispute management, liabilities, and implications on their services14. Rwanda has already modelled their Open Banking approach on the European Union’s Revised Payment Services Directive (PSD2)15. It covers consumers and SMEs. The Rwandan regulatory framework also addresses the issue of data sharing and security to encourage innovation, efficiency, and new product development.

Although a differentiation can be made between voluntary and mandatory Open Banking regimes, some degree of overlap may exist in practice. A voluntary regime implies that participation is optional, but its rules are usually mandatory once an entity has decided to join. The level of specification set by the government in voluntary regimes may vary from highly detailed

frameworks (in Hong Kong and Singapore) and a specific licensing regime (for account aggregators in India) to high-level guiding principles (in Indonesia, Japan, and Malaysia). Some voluntary regimes are highly prescriptive and may as such border on being mandatory in their implementation. For example, although technically Hong Kong is a voluntary regime, as its policy documentation articulates, when read in conjunction with other policy statements and levels of specification for the framework, it appears to be mandatory. Equally, some voluntary regimes are not highly prescriptive but de facto mandatory because of expectations set by the regulator (e.g., Japan)\(^{16}\). The appropriateness of adopting a voluntary or mandatory approach across jurisdictions depends on the context of the market, particularly the market structure.

Using a voluntary approach, there are no regulations on compulsory Open Banking regime, but countries are introducing voluntary data sharing frameworks in the financial services sector (especially banking). Countries may introduce a range of measures to promote and accelerate the uptake of data sharing frameworks in Open Banking, but without formal or compulsory Open Banking regimes. While a range of measures may be put in place to promote and accelerate the practice of data sharing frameworks in Open Banking, it is not mandatory for banks to publish their open API policies. However, under the mandatory approach, data exchange and sharing are regulated by pieces of legislation and transition from market-led to a regulated framework. Regulators introduce a range of measures to promote Open Banking and data sharing and set compulsory timelines for the implementation of these measures. A summary of approaches to Open Banking undertaken by international jurisdictions is presented in Table 1 below (see detailed case studies in the appendix).

**Table 1: International Open Banking approaches**

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Approach</th>
<th>Type of framework</th>
<th>Regulatory authorities</th>
<th>Timelines</th>
</tr>
</thead>
</table>
| 1. Hong Kong  | Market-led | • Governance framework supervised by the monetary authority.  
• Collaborative and phased approach to implementing the API framework.  
• Transparency in data specifications | Hong Kong Monetary Authority and a proposed Standards Body | Implementation of Phase 1 and 2 within 15 months after July 2018. Phase 3 and 4 implementation process is ongoing. |
| 2. Singapore  | Market-led | • API standardisation  
• Recommendations on APIs for adoption by the monetary authority | Monetary Authority of Singapore | Phased approach beginning in 2013 with no |

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• API standardisation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Voluntary adoption of Open Banking principles facilitated by partnership between industry and the monetary authority.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Registration and authorisation process of third parties to access data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bilateral contracting between banks and third-party firms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. China</td>
<td>Market-led</td>
<td>No regulatory oversight</td>
<td>2019 until to date.</td>
</tr>
<tr>
<td></td>
<td>• Creation of a new FinTech Research Lab to develop an Open Banking framework</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. India</td>
<td>Market-led</td>
<td>The Reserve Bank of India, National Payments Council of India, Account Aggregator and Reserve Bank Information Technology Private Limited</td>
<td>2010 until to date.</td>
</tr>
<tr>
<td></td>
<td>• Governance framework with Open Banking guidelines supported by regulatory authorities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Customer consent-based sharing of financial information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. EU</td>
<td>Regulated framework</td>
<td>European Commission</td>
<td>Data protection reform package starting in 2012 and the process is still ongoing with new regulations being introduced</td>
</tr>
<tr>
<td></td>
<td>• Formal regulations for market players</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Standardisation of data protection and portability rule across the EU</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rights-based approach to the control of personal data of EU citizens</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. UK</td>
<td>Regulated framework</td>
<td>Competition and Market Authority, Financial Conduct Authority, and Information Commissioner's Office</td>
<td>Compliance due date by banks extended to the end of 2021</td>
</tr>
<tr>
<td></td>
<td>• Mandatory development and use of APIs, as well as data sharing by the UK's largest banks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mandatory provision of data access and publication of specific financial information by the UK's largest banks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Australia</td>
<td>Regulated framework</td>
<td>The Australian Competition and Consumer Commission, the Office of the Australian Information Commissioner, and a new Data Standards Body</td>
<td>Implementation of Consumer Data Right in the financial sector completed in 2020</td>
</tr>
<tr>
<td></td>
<td>• Mandatory implementation of open APIs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• API implementation supervised under a multi-regulator model consisting of three bodies with defined mandates.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Type of Framework</td>
<td>Key Initiatives</td>
<td>Regulatory Authority</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
</tbody>
</table>
| Nigeria      | Regulated framework | • Development of a common banking industry API standard  
• Regulatory framework focusing on financial inclusion.  
• Risk-based approach to data access | Central Bank of Nigeria               | Within 12 months from February 2021                  |
| Bahrain      | Regulated framework | • Consumer consent-based approach  
• Customized Open Banking framework for Bahrain  
• Flexible regulatory framework to be updated as and when required | Central Bank of Bahrain               | 6-month compliance period by traditional banks (28 October 2020 to 30 April 2021) |
| Rwanda       | Regulated framework | • Open Banking regime modelled based on the European Union’s regulatory framework.  
• Customer consent-based sharing of financial information | National Bank of Rwanda               | Implementation of technical standards by 2024             |
| US           | Market-led approach with prospects of transition to a regulated framework | • Voluntary development of API-related data sharing agreements  
• Adoption of common standards for Open Banking.  
• Standardisation of state and federal banking regulations | Consumer Financial Protection Bureau and the US Treasury | No specific timelines                                       |

Source: Authors’ own compilation based on various sources

2.1 Open Banking regime for South Africa: market-led or regulatory-led?

Several Fintechs are already operational alongside traditional incumbent banks. Telcos have also been playing an important role in reaching a limited range of financial services to the unbanked population in South Africa. This is also true in the African continent where telcos such as M-Shwari, M-Pesa, Tala are providing consumers with some benefits which are associated with Open Banking[17]. Despite the existence of the highlighted market developments, there has been no

---

regulatory directive regarding the implementation of Open Banking or data sharing in the financial sector in South Africa. The onset of Open Banking in South Africa and the need for access to data as a catalyst for innovation and competitiveness require a more proactive approach to ensure that markets remain competitive and eliminate barriers to entry and expansion, particularly by Fintechs and start-ups. Regulatory authorities have also not pronounced whether Open Banking will be voluntary or mandatory. Therefore, a critical question to debate is whether South Africa should adopt a voluntary or mandatory approach to Open Banking.

A review of literature on the approaches to Open Banking, shows that there is a mix of models that have been adopted by different countries depending on the dynamics of the market. Furthermore, Open Banking initiatives have been successfully implemented in jurisdictions that have followed a regulatory-led approach such as in Australia and the United Kingdom (UK). This success has also been witnessed in jurisdictions that followed voluntary regimes such as Hong Kong and Japan. However, what is apparent is that whatever approach is adopted, guidance by relevant regulators is essential. What informs the decision on the sort of guidance to provide is partly whether a market-led approach is leading to actual sharing of data and whether there is an incentive to share data rather than engaging in exclusionary conduct. Incumbent banks are the infrastructure providers that create and manage the marketplace in Open Banking. However, considering the incentives at play, exclusionary conduct such as refusal to supply may occur in an Open Banking environment where a dominant firm can exclude its competitors from accessing valuable data, and thus deprive them of a source of product and/or service innovation in the market.

International experiences on the suitable approach to Open Banking indicate that the adoption of market-led approach may not achieve the desired results largely because the approach may potentially be susceptible to abuse by firms that possess market power. Preliminary evidence shows that a market-led approach may not be in the interest of traditional banks and therefore unlikely to succeed in South Africa. This is corroborated by a survey conducted by the Financial Sector Conduct Authority (FSCA) that suggests that Fintechs are likely to be the big winners of open finance in South Africa. This may provide little incentives for incumbent financial institutions to provide open consumer data access to Fintech firms and other start-ups that seek to compete with them for either the customers, or certain financial services provided to the customer. There is also

---


evidence that banks share APIs with Fintechs and other players that collaborate rather than compete with them as it is more likely that banks agree to complementary as opposed to competing offerings\(^{21}\). Therefore, even if South Africa starts with a market-led approach, it is likely to gravitate towards a more mandatory approach. Given these observations, a regulatory-led approach may be appropriate for South Africa based on the following:

- The banking sector is highly concentrated with only five major banks and if left to the market, it is likely that the pace of Open Banking will be slow;

- The self-interest motive or economic incentives of banks in a highly concentrated market may lead to further delays and decisions on the API specifications would naturally consider their financial incentives;

- The role of data is important to drive innovation and therefore banks may feel short-changed by promoting “competitors” or potential competition; and

- There may be some reluctance among many consumers to share their data especially if the initiative is driven by banks themselves.

A regulatory approach will also assist incumbent banks to further innovate which may lead to consumer benefits. It also limits the artificial “hold-up” placed by incumbent banks.

3. **KEY PILLARS OF OPEN BANKING REGIME AND TREATMENT OF BIGTECHS**

3.1. **What data is involved?**

One of the key pillars in the implementation of Open Banking is what type of data can be shared and which parties can get access to the data. In Open Banking, contracting generally takes place between traditional banks and Fintechs and other players. The types of data that the traditional banks and other financial institutions typically keep broadly consist of customer data, transaction data, and value-added customer data. Customer data encompass information provided directly to the bank, such as employment information and tax filings. Transaction data includes records of payments, withdrawals and other account activities and value-added customer data is the data generated by banks and financial institutions to gain specific insights on a consumer, such as credit scores\(^{22}\). We present in the appendix section more detail on different types of data.

What is important in Open Banking is that Fintechs and other players need to combine consumer data (i.e., transactional information including banking transactions and payments) with other types of data to innovate products and services. Therefore, customer data derived from transactional interactions is critical in the implementation of Open Banking.

3.1.1. **Data sharing in other countries**

We observe from experiences in other countries that access to consumer data is central to the implementation of Open Banking with slight variations across jurisdictions. For example, in Australia, consumer data that can be shared include savings and credit card data, mortgage data, personal loan information, and joint bank account data (AT, 2020). A noteworthy variation is observed in India where the perimeter of data subjects is broader than in most other jurisdictions. The Indian approach extends this to also include SMEs, who can participate in the payments and data layers of the stack and gain access to improved financial services and access to funding\(^{23}\).

In Nigeria, data is categorised according to risk and access is not open to all participants. Under a regulatory framework for Open Banking, there is certain data that may be exchanged and not every participant has access to all the categories of information made available. There are four access levels by data and service category and applicable Risk Management ("RM") Maturity Levels. These


are (i) Product Information and Service Touchpoints (ii) Market Insight Transactions (iii) Personal Information and Financial Transaction and (iv) Profile, Analytics and Scoring Transaction. The first and second information categories are considered low and moderately risk and are accessible by participants. The Personal Information and Financial Transaction category is considered high risk information and cannot be accessed by participants without regulatory license. The Profile, Analytics and Scoring Transaction category of information is considered high risk and sensitive and can only be accessed by licensed payments service providers and other financial institutions²⁴.

The CMA has been explicit about data to be shared in Open Banking in the UK. This followed its market investigation into the retail banking sector, where it ordered the largest banks to make data available through open APIs including prices, charges, terms, and conditions together with customer eligibility criteria in the case of loans, for all personal current account and business current account products and all SME lending products. Banks were also compelled to share reference data such as branch and ATM location, branch opening hours as well as data on service quality indicators (i.e., customer recommendation scores) as specified by the CMA²⁵.

Lessons from jurisdictions such as Australia and Hong Kong also provide insights with regards to what type of data should be covered at a minimum in Open Banking implementation. This primarily comprises of data on product and services, transactions, and account information. Notably, Hong Kong’s Open Banking framework comprehensively dealt with the format or way each type of data can be shared or accessed. Data sharing on products and services was to be “read-only” information offered by banks on details of their products and service offerings, while the sharing of transactional and account information would involve the retrieval and alteration (where applicable) of account information of authenticated customers for stand-alone or aggregated views²⁶²⁷.

### 3.1.2. Way forward on data sharing in South Africa

In South Africa, Fintechs and other start-ups that collaborate with traditional banks already have access to customer data. The experiences of Fintechs and other start-ups in terms of the type of


data they require is important for regulators to come up with guidance on what data can be shared. This will eventually filter down to which players can be given access to which type of customer data. The Nigerian experience is interesting for South Africa as it considers riskiness of the data types and the type of data that can be shared with the different participants in Open Banking\textsuperscript{28}. What is apparent is that the experiences of Fintechs and other start-ups in the selective data access that is currently taking place, is key to the formulation of guidance on the types of customer data that can be shared with different participants.

Owing to the increased sensitivity of data some countries have also adopted a phased approach where data is shared gradually depending on the risks involved with each category of data. From international experiences, it is also clear that data sharing in Open Banking has generally commenced with less sensitive information such as information on products and services provided by banks and ending with classified consumer information on transactions and payments\textsuperscript{29}. This approach can be a consideration for South Africa.

3.2. Who owns the data?

The decision on who owns customer data is critical in formulating direction on data access in Open Banking. There are distinct stakeholder interests with respect to customer data given its implications for competition and innovation; including data domains which are personal, private, and public. These data domains are detailed in the appendix. While the domains of the data provide some insights into the different stakeholder interests in the data, it does not determine who owns the data. It is generally purported that data collected about an individual belongs to the individual and the individual should be able to determine how this data is used and who can use it\textsuperscript{30}.

Banks and financial institutions have traditionally been the primary holders of consumer financial data and access to this data has consequently been controlled by these banks and subject to substantial regulatory oversight\textsuperscript{31}. The control of customer data by traditional banks and vested


interest imply that the question of data ownership should be resolved to determine how customer data can be shared in Open Banking.

3.2.1. Data ownership in other countries

There seems to be some convergence that consumer data collected and processed by banks and financial institutions is owned by the consumer. Legislations on data privacy and security in several countries reviewed in this research other than the Asia-Pacific region, consumer protection is central. Examples of countries with such an approach include the EU through the GDPR, India through the fiduciary, a financial data aggregator, Singapore through personal data protection legislation and Personal Data Protection Amendments (PDPA), Australia through the Consumer Data Right (CDR) and in Nigeria through the Nigerian Data Protection Regulations (“NDPR”). Placing customers at the centre of Legislations on data privacy and security and emphasis on customer consent seem to suggest that customer data collected and processed by banks and financial institutions is owned by the consumer.

In Australia, consumers are effectively custodians of their financial data as they are in control of how and when they share their data. Since 2020, Australian bank customers could permit accredited third parties to access their financial data. As such, consumers are empowered through the CDR to use their data for their own benefit. In the EU, the question of who owns the data has also emerged in the context of the GDPR. While the GDPR does not provide clarity on data ownership, it provides consumers with control and easier access to their personal data.

3.2.2. Way forward on data ownership in South Africa

In South Africa, the provisions of the Protection of Personal Information (PoPI) Act do not explicitly address the issue of data ownership, but they encompass a broader framework governing the rights of a data subject. A data subject refers to the person (i.e., consumer) to whom the

---

32 See: https://gdpr.eu/what-is-gdpr/.
personal data relates. However, the specific provisions of PoPI Act which appear to confer data subjects with some degree of control over personal data state that personal information can only be processed, *inter alia*, subject to a valid consent by the data subject. Data subjects are also empowered to object to the processing of their personal information or withdraw their consent contingent on reasonable grounds. The Act also includes provisions for data subjects to establish institutions that possess their personal data and the right to access this data, as well as to request for destruction of their personal information held by a data holder where reasonable.40

While the provisions of the PoPI Act do not explicitly address the issue of data ownership, it was anticipated that the decision in a case deliberated by the South Gauteng High Court in the insurance industry, wherein Discovery (Ltd) (“Discovery”) contended that the Liberty Group Ltd (“Liberty”) had “made unlawful and unfair use of the Vitality programme, its reputation and the “back-office” that it entails”41, would have provided much needed clarity on the balancing between consumers’ rights and copyright laws in South Africa. In May 2019, Liberty introduced a feature to its Liberty Lifestyle Protector Plan (which is a life insurance product) called the “Wellness Bonus”, wherein customers could elect to disclose to Liberty whether they had an existing membership in an external wellness programme, in order to qualify for a rebate on a portion of their premiums depending on their status on the external wellness programme. In its decision, the Court found that Liberty’s conduct was not wrongful, because members of the public had paid for their Vitality membership and status and are, therefore, entitled to use this for whatever lawful reason they wish. Furthermore, the Court ruled that it was in the interest of consumers and competition in the insurance industry that Vitality members are able to exercise their choice in how they wish to use their Vitality status.42

While the PoPI Act and the Liberty decision seem to suggest that there is consumer ownership of data, there is still some ambiguity. The Liberty decision creates uncertainty in instances such as Open Banking where the consumer may not have paid for their data to be processed and insights generated. This uncertainty may incentivise the incumbents to take advantage of the status quo to exclude Fintechs and other start-ups from accessing consumer data. For Open banking to move forward, some guidance is required in this regard, or determination must be made by the Information Regulator to provide certainty on data ownership in the market.

---

40 See: section 5 (a-d) and section 11 (1)(a), section 11 (2)(b) and section 11 (3)(a) of PoPI Act.
41 See: Discovery Ltd and Others v Liberty Group Ltd (21362/2019) [2020] ZAGPJHC 67; [2020] 2 All SA 819 (GJ); 2020 (4) SA 160 (GJ) (15 April 2020)
3.3. Payment for data?

In formulating guidance on Open Banking, one of the key issues to consider is whether Fintechs and other smaller players will pay financial institutions such as banks or third-party firms to get access to customer data. Even though data may be owned by the consumer, sometimes financial institutions incur costs to process and store the data. Payment for data access is meant to level the playing field between data holders and third-party firms by compensating for processing and storing of consumer data. The argument is that if compensation for data processing is not allowed, it disincentivises the processing and storing of data. Furthermore, when data sharing involves data that required significant investments to obtain or transform, free access to such data may have negative implications of discouraging investments and adversely affecting the development of a market. In some markets, these investments generally occur when raw data is collected to derive value from it. For instance, market players may expend significant resources to add value and store a dataset\(^{43}\).

However, there may be risks concomitant with the sale of customer data if payment is allowed. The risks include exploitative conduct such as excessive pricing and constructive refusal to supply. Consumer data may be sold by incumbents at excessive prices or on unfavourable commercial terms\(^{44}\). The resultant effect is that instead of achieving access as envisaged with Open Banking objectives, the sale of data may create barriers to data access thereby inhibiting innovation and competition. Direction is therefore required regarding compensation to banks or third-party firms for processing and storing consumer data.

3.3.1. Payment for data in other jurisdictions

Some jurisdictions have approached the issue of compensation for processing and storing of consumer data differently. Notably, data holders incur costs in processing and storing consumer data. Competition agencies such as the European Commission have taken a strong stance on the sale of data, allowing banks to receive compensation only amounting to a maximum of the efficient costs incurred to arrange access for other third-parties or competitors\(^{45}\). Australia adopted a staged approach to the sale of consumer data. During the first phase of the initial Open Banking

---


implementation, data was transferred at no charge, at the consumer’s direction. However, with the adoption of the Consumer Data Right (CDR) system in May 2018, there was flexibility to provide for charging for access to data. This was required in relation to access to value-added data or in instances where making data available for free would disincentivize the collection and storage of such data in the market.\footnote{Australian Treasury. 2019. CONSUMER DATA RIGHT OVERVIEW. Accessed at: https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf.}

In India, responsibility is placed on the fiduciary, a financial data aggregator, to manage the subject’s data and rights and seek consent for data processing. The fiduciary is allowed to charge fees to offer the service.\footnote{Rao, R. 2021. Open banking in India. Accessed at: https://www.bis.org/review/r210419a.pdf.}

\subsection*{3.3.2. Way forward on payment for data in South Africa}

In South Africa, like other jurisdictions, incumbent banks possess hordes of consumer data relative to Fintechs and other third-party players. Customer data is processed by the incumbent banks through the deployment of technology. The PoPI Act does not preclude data holders from levying a fee when data subjects request access to their data. Data holders can therefore charge a fee for services provided when responding to a data request from the data subject.\footnote{See also: https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?id=3142.} The current status quo in South Africa may provide incentives for exploitative conduct such as excessive pricing and constructive refusal to supply. For instance, when banks were allowed to charge fees in order for third parties to access data in South Africa, they provided consumer data required for credit checks in a pdf format at R30-R40 per consumer.\footnote{Section 23 (1)(b) read with section 23 (3)(a-b) of PoPI Act.}

Given the need to compensate financial institutions to incentivise processing and storing of consumer data and associated risk of potential exploitative abuse, guidance is required on whether financial institutions can charge fees for data access and what type of data can attract a fee when shared as well as the permissible magnitude of compensation. This is key in an Open Banking environment to ensure that compensation for consumer data does not create a barrier for access to data and restrict competition. At most, compensation must be equal to the costs incurred for sharing data.\footnote{IFWG Working Group Discussions.}
3.4. Open APIs or not?

Open Banking is facilitated by Application Programming Interfaces (APIs), which provide real-time secure access to customer data. Whilst screen scraping technology provides a substitute for the lack of APIs, this is less desirable as it cannot scrape a lot of the customer information and is a more expensive or less efficient means of acquiring data\(^{51}\). The facilitation of Open Banking using APIs implies that the large traditional banks are the infrastructure-providers that create and manage the marketplace in Open Banking. Therefore, API specification is one of the key pillars that require guidance in the implementation of Open Banking. Guidance may be required on interoperability of APIs, API standardisation and specifically on whether to open APIs or not. This is because lack of interoperability may be used by incumbents as an artificial barrier to prevent new market entrants and with a clear tactic to monopolise a market\(^{52}\).

3.4.1. Development of APIs internationally

A review of international experiences on API specifications shows that countries have adopted diverse approaches in the development and implementation of API standards. The European Commission’s PSD2 Regulation requires banks to develop APIs that meet the following minimum standards: (i) allow account information services providers (AISPs) and payment initiation services providers (PISPs) to identify themselves to the bank; (ii) permit AISPs and PISPs to communicate securely to request and receive accounts and payments information; and (iii) allow PISPs to initiate payment orders from customer’s payment accounts as well as receive all information on the initiation and execution of the payment transactions (Lexology, 2020). PSD2 mandates that banks share extensive user financial data with Fintechs, who are not required to reciprocate by sharing their user data with the banks.

In the UK, APIs are standardised for the largest banks. The CMA require the use of open API standards and data sharing by requiring that the largest banks in the UK, namely, RBSG, LBG, Barclays, HSBCG, Nationwide, Santander, Danske, Bol and AIBG to adopt and maintain similar API standards. This was meant to enable the standardisation and ease of data sharing with third-party service providers including price comparison websites (PCWs), account information service providers (AISPs) and payment initiation service providers (PISPs). Important to note is that only


18
institutions accredited by the Financial Conduct Authority (FCA) were eligible to be provided with access to open APIs. Further, customers are required to opt-in to share data\(^{53}\).

The Hong Kong Monetary Authority (HKMA) adopted a collaborative and phased approach to implementing the API framework. The framework was designed to provide guidance in the market and ensure flexibility, rather than prescribing how banks should implement it. The scope of the API framework consists of, *inter alia*, the deployment timeframe; technical standards on architecture, security, and data; governance model; facilitation measures; and ongoing development\(^{54}\).

The Japanese FSA also obliged banks to publish their open API policies and encouraged them to contract with at least one TPP by 2020\(^{55}\). The deadline for implementation of APIs was initially set for 31 May 2020. However, progress has been rather sluggish owing to an incident where customer money was stolen from bank accounts which were breached in September 2020\(^{56}\).

In India, the government played an active role in the development and implementation of APIs. These include the introduction of the IndiaStack\(^{57} \, ^{58}\) which developed a set of APIs (Aadhaar, eKYC, Digilocker and eSign), the launch of the Unified Payments Interface (UPI) and the issuing of prescribed Account Aggregator (AA) guidelines on acceptable activities and API specifications\(^{59}\).

In Australia, implementation of open APIs is mandatory. API implementation supervised under a multi-regulator model consisting of three bodies, namely, the Australian Competition and Consumer Commission (ACCC), the Office of the Australian Information Commissioner (OAIC), and a new Data Standards Body, with defined mandates. The Consumer Data Right (CDR) governing Open Banking is the first Open Banking legislation to introduce the concept of reciprocity in data sharing. The reciprocity implies that those who wish to become accredited and receive designated


\(^{57}\) A set of APIs that allows governments, businesses, start-ups and developers to utilize a unique digital infrastructure to solve India’s hard problems towards presence-less, paperless, and cashless service delivery.

\(^{58}\) See: Indiastack.org. 20 February 2017

data at a consumer’s request, must be willing to share equivalent data, in response to a consumer’s request\textsuperscript{60}.

Nigeria issued a regulatory framework for Open Banking in February 2021 that makes provisions on API access requirements and principles for API specifications. The Risk Management (“RM”) Maturity Level of participants determines API services that may be implemented by and used by participants. The RM Maturity Level ranging from tier 0 to 3 and participants categories. The CBN commits to regulate the development of a common banking industry API standard with technical design standard, data standard, information security standard and operational rules. The CBN is required to develop Common Banking Industry API Standards within twelve (12) months of the issuance of the Framework and maintain an Open Banking Registry\textsuperscript{61}.

3.4.2. Way forward on APIs in South Africa

In South Africa, banks are already creating APIs for Fintechs that collaborate with them implying limited and exclusionary access. While most banks provide API-based access to data, there are no agreed standards and access is limited to certain Fintechs that banks are prepared to provide access to. To provide many standard offerings, Fintechs must negotiate across different banks separately and if some banks do not agree, it creates coverage gaps in the offering provided. In addition, it is more likely that banks agree to complementary as opposed to competing offerings\textsuperscript{62}.

Another competition concern is that incumbent banks may manipulate the functionality of their systems in order to limit third-party users from retrieving their data from the platform and use it on another. Such conduct may lead to dominant firms possessing exclusive control over valuable data which cannot be replicated. A highly concentrated banking sector in South Africa implies that large traditional banks have incentives to selectively determine what data to share or not to share with third-party payment providers. Therefore, a decision must be made on whether there must be standardisation of APIs or to maintain the existing status quo of selective API provision. Lessons from other jurisdictions show that there are some countries such as Singapore with no specific data


sharing or Open Banking legislation, but provide a guideline for Open Banking APIs, which are defined via a publicly available infrastructure\(^{63}\).

Since APIs are already in existence, the focus at this stage may be to ensure wider access and not necessarily standardised access. Further, to ensure that certain APIs are available at a minimum. Either way, guidance is still required on interoperability of APIs and on whether to implement open APIs or not.

### 3.5. How is data privacy and security addressed in Open Banking?

A key feature of Open Banking is that a lot of data, particularly customer data, is consent driven. While customers may give consent, data privacy and security considerations may pose difficulties to compel dominant players such as the larger banks to provide data access to SMEs and start-ups. The concerns that have emerged in the context of Open Banking relate to incumbent banks refusing third-party access to data on grounds of data security, although some refusals may relate more to limiting competition from third parties\(^{64}\). Therefore, given the role of data as a source of market power, how data privacy and security are addressed has a significant bearing on the successful implementation of Open Banking.

#### 3.5.1. International data privacy and security measures

Many countries have enacted legislations to ensure data privacy and security in the implementation of Open Banking. In enacting data privacy and security legislations, some countries ensured that these legislations would not hinder access to customer data required by third-party players to compete in the market. Notably, there are diverse positions internationally about consumer data ownership and, as a result, the concomitant regulations that would apply to consumer data in terms of openness and privacy. For instance, in Europe, consumers have strong data protections and rights to the data access, whereas in the United States data protection is not a fundamental right and laws and regulations in respect of data focus more on preventing physical and economic harm. Countries in the Asia-Pacific region do not have a strong focus on consumers’ data rights and are concerned more with weighing up economic development and financial inclusion considerations\(^{65}\).

---


The EU has taken a rights-based approach to individuals' control of personal data through the adoption of the General Data Protection Regulation (GDPR). The GDPR imposes obligations on the data controller and processor to ensure that the rights of the data subject are respected when data is transferred for analysis and value extraction. In practice, the approach has involved data controllers issuing GDPR-compliant checklists for data subjects to complete in order to gain access to services. There is a single set of rules on data protection adopted amongst EU countries. The right to data portability is aimed at fostering competition in the market where consumers will have easier access to their data and be able to transfer it from one service provider to another more effortlessly.

In India, responsibility is placed on the fiduciary, a financial data aggregator, to manage the subject’s data and rights and seek consent for data processing. The fiduciary may not access or store the data being shared but will be allowed to charge fees to offer the service. This limit on access to the subject’s data by the fiduciary marks a unique approach than in other jurisdictions, where aggregators offer their services in exchange for access to the data that can be used to offer other financial services. The fiduciary also acts as a consent manager as it can authenticate the data subject using their digital ID to verify their information.

Singapore has personal data protection legislation which was amended. For instance, the amendments were passed by Parliament in November 2020 and began to take effect in phases beginning on 1 February 2021. These amendments enhance consumer protection and strengthen accountability of organizations. Key changes include (i) new mandatory data breach notification (ii) penalties for new offenses should personal data be mishandled (iii) increased financial penalty cap for breaches, and (iv) additional rules on telemarketing and spam control.

In Australia, data privacy and security are governed by the Consumer Data Right (CDR), aimed at providing consumers with the right to securely access certain data about them held by financial institutions including banks. The CDR also permits consumers to share their data with whichever authorised third parties they may choose. All customers (individuals; or small, medium, or large...

---

66 See: https://gdpr.eu/what-is-gdpr/
68 See: https://gdpr.eu/what-is-gdpr/
businesses) will be entitled to exercise the right concerning the classes of data covered by the CDR. The CDR is a sectoral policy initiative as it will initially apply to the financial sector (i.e., banks) and then later rolled-out to other sectors including energy and telecommunications, with the possibility of being applied to any sector in the future. In Nigeria, compliance with data privacy laws and regulations including the Nigerian Data Protection Regulations (“NDPR”) requires institutions to obtain consent of the end-user on each action that may be performed on the account of the end user as specified by the provider. There are also additional requirements imposed by the framework. Notably, the requirement that agreements presented to the customer by the participant should be simple, explicit and in the customer’s preferred language and form including written, electronic, video or audio. A copy of the customer’s consent should moreover be made available to the consumer and preserved by the participant. The provisions of the framework also require that the consent of the customer be revalidated annually and where the customer has not used the service of the provider for a maximum of 180 days.

3.5.2. Way forward on data privacy and security in South Africa

In South Africa, like other jurisdictions, there are existing legislations to ensure data privacy and security. The Constitution of 1996 (Constitution) is the overarching legal framework governing data privacy in South Africa. Section 14 of the Constitution makes provisions for the right to privacy for every South Africa citizen, “which includes the right not to have-(a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed”. However, the PoPI Act is the primary data protection legislation in South Africa. The Act obliges organisations to apply specific data protection principles and conditions when processing, storing, and disposing of personal information. PoPI Act also places a legal duty on all data holders to deal with customer information with far more diligence than ever before. This has in effect intensified the need to reduce the risk of personal information being compromised, misused, and stolen. Data security measures put forward by PoPI are also intended to prevent unauthorised access to and processing of restricted personal information.

---

Notwithstanding the presence of general data privacy and security legislation, targeted legislation on data privacy and security is non-existent in the context of Open Banking. It is also imperative to provide guidance on how data privacy and security will be enhanced in without compromising on data access required for successful implementation of Open Banking. Further, lessons can be drawn from other jurisdictions where data protection and security is the responsibility of all the participants in the Open Banking ecosystem.

3.6. Treatment of Big Techs

A fundamental aspect of Open Banking regulations and initiatives is to enable, but also control by way of regulatory oversight, the disruption of the business models currently employed in banking. This disruption is intended to facilitate open innovation platforms, the like of which has been witnessed across multiple industries. The platform business model is the mainstay of BigTech firms. As such, this model has enabled these firms to capture dominant positions in the markets they have disrupted by leveraging their core offering as multi-sided platforms. This core offering allows these firms to exploit network effects and scale and scope economies, which allows for the tipping of markets in their favour.

The banking sector already resembles the platform business models of today, with services and products bundled on top of a current account platform to create scale and scope economies. As with modern platform markets, the unbundled entrants, or Fintechs, seeking to compete for the provision of banking products and services on top of the current account platform, may find it difficult to compete with incumbent banks that have the benefit of operating and controlling access to the current account platform. Further barriers are erected, particularly in erecting a competing platform ecosystem to the current account platform, by the regulatory context of the banking and financial industry that are meant to ensure the resilience of sector.

Open Banking initiatives seeking to encourage disruptive innovation in the banking sector may facilitate the entry of Fintechs providing a rich product and service diversity and expanding the banked population. These initiatives will also facilitate the entry of BigTech firms that are particularly suited to disrupting markets using a platform business model into the banking industry, an industry that is particularly suited to the use of platform business models. There are indications that BigTech firms are already entering banking-related product and service markets and are also developing larger ambitions of disruption at the platform level of banking, as demonstrated in the Figure 1 below.
Most of the activity of the BigTech firms in the banking sector has centred around payments, as it is less heavily regulated compared to other banking and finance-related activities. Furthermore, the data potential around payments provides BigTech firms with a new dimension over which they may observe consumer behaviour, which is at the core of these firms’ monetisation strategies. However, according to the announcements made by some of these firms, it is evident that broader envelopment of the ecosystem is envisaged in future.

If the broader participation of BigTech firms in banking services follows the disruption path executed in other sectors of the economy, then there is the potential for these firms to follow a path towards market domination and platform envelopment due to the larger data advantages these firms have as compared to traditional banks. It appears that at the very least Alphabet (Google) appears to be headed in this direction given the firm’s intention to launch current accounts, the core platform of traditional banks over which services are bundled, in 2021.

Thus, it seems apparent that BigTech firms, at least in principle, can compete directly with incumbent banks either by becoming banks themselves or by continuing to operate as a multi-sided
platform that focuses on the most profitable banking products and services. The incumbent banks can respond by either trying to match the offering of BigTech firms or by partnering with other banks and third parties, which is unlikely as it may be difficult for banks to match BigTech firms in bundling products and services over their platform. This is due to the dominant position of BigTech firms in non-financial products and services which will also be bundled with their financial offering, or the incumbent banks may seem to partner directly with the BigTech firms, which may reduce the profitability of the incumbent banks as the BigTech firms erode their margins. Figure 2 below presents these strategies alongside their predicted outcomes.

**Figure 2: Strategic outcomes of the potential strategies of traditional banks and BigTech firms**

<table>
<thead>
<tr>
<th>Incumbents</th>
<th>BigTech firms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodate • Cooperate with partnerships • Provide specialised unique banking products and services</td>
<td>Accommodate • Partnerships</td>
</tr>
<tr>
<td>Fight/compete head-to-head by becoming platform/marketplace • Profit from superior trust (?) from customers and data security • Better regulatory navigation skills and similar lobby power than BigTech firms • Cannot match BigTech firms’ bundling/cross-subsidization strategy with complementary financial and nonfinancial products (despite enjoying some network effects)</td>
<td>Compete head-to-head • Become banks/intermediaries bundling their offerings and exploiting economies of scope - Opt not to accept deposits to avoid regulation • Multisided platform (marketplace) - Platform envelopment - Gatekeeper: monopolise interface with consumers</td>
</tr>
</tbody>
</table>

**Source:** (OECD, 2020)⁷⁷

Initially, the entry of BigTech firms into financial services was likely to lead to an expansion in the bankable population and a reduction in the margins of incumbents as competition increases. However, in the long-run and depending on the extent of the entry by BigTech firms, these firms may either envelope the financial sector, or appropriate the profits of the incumbents by monopolising the interface with consumers or providing key services.⁷⁸

Under each of these scenarios, there is a heightened systemic risk in the financial services industry as BigTech firms become increasingly pervasive in the financial system and essentially become too big to fail. While regulatory oversight may prove sufficient if BigTech firms choose to become banks themselves and are, thus, subjugate to existing banking regulations, this is not the case for the other potential future strategies of these firms and there is a strong incentive to avoid costly regulation. Partnerships with incumbents at various levels of the value chain and gatekeeping the

---


customer interface, while remaining encumbered by regulatory oversight, introduces systemic risk into the financial system due to their interconnectedness with the system\textsuperscript{79}.

Furthermore, asymmetries in the regulation of incumbent institutions and BigTech firms can have a significant impact on the type of competition that will materialise between these firms in the future. If regulation is designed in such a way as to ensure that there is a level playing field between BigTech firms and incumbent financial institutions, then there is a higher likelihood that these firms will engage in head-to-head competition. However, if incumbents are more strictly regulated compared to BigTech firms, for instance, if the same regulatory leeway provided to Fintechs to encourage their entry and participation is provided to BigTech firms, it will result in an initial increase in competition but with a long-term risk of monopolisation or gatekeeping by BigTech firms\textsuperscript{80}. As such, it is recommended that a bespoke policy approach be developed for BigTech firms separate from the approach applied to Fintechs more generally\textsuperscript{81}.

3.6.1. Experiences of Bigtech and Fintech in other countries

China is a prime example of the significant impact that the fintech sector and especially BigTech firms can have on the banking sector. The Chinese mobile-based connectivity ecosystem and regulatory framework that is conducive for innovation has provided scope for the large tech companies to increase their market shares in terms of customer base. For instance, Alibaba, which is China's largest e-commerce company introduced Alipay in 2003 as a third-party online payment platform. Alipay has been an integral part of Alibaba's success which currently offers a bouquet of services including payments, wealth management, lending, insurance, and credit scoring services. Another tech giant, namely, Tencent (which owns the social network app WeChat) is used to make payments (both online and in physical stores and to settle utility bills). It is estimated that the two Chinese tech firms account for over 90% of the market\textsuperscript{82}\textsuperscript{83}.

In China, most Fintechs are affiliated with Chinese BigTech firms, and all the products and services previously supplied by traditional banks are offered within the ecosystem of the BigTech firms, as


demonstrated in the figure below. As such, it is apparent that China already exists in a banking landscape characterised by dominant BigTech firms.

However, it appears that China’s banking and market regulators have recently intensified supervision of these BigTech firms. Late in December last year the People’s Bank of China imposed certain requirements on Ant Financial, such as improving trading transparency; refraining from unfair competition; complying with laws, regulations, and licensing regimes for their personal credit reporting business; protecting the privacy of personal data; improving corporate governance; complying with the regulatory requirements for lending, insurance, wealth management, and securities; and creating a holding company for financial services that implements the regulatory requirements for capital adequacy and compliance with related party transactions. These impositions followed changes in the competition framework for internet companies in China to curtail the monopolistic behaviour of BigTechs and protect consumers. Furthermore, the People’s Bank of China imposes a stringent 100% reserve requirement for customers’ balances held in payment institutions that are not banks, such as AliPay and WeChat Pay.

Figure 3: Fintechs contained within the broader ecosystems of Chinese BigTech firms

<table>
<thead>
<tr>
<th>Europe &amp; US</th>
<th>China</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payments</td>
<td></td>
</tr>
<tr>
<td>PayPal</td>
<td>Alipay</td>
</tr>
<tr>
<td>Stripe</td>
<td>Tenpay</td>
</tr>
<tr>
<td>Wealth</td>
<td></td>
</tr>
<tr>
<td>management</td>
<td></td>
</tr>
<tr>
<td>Betterment</td>
<td>Yu'e Bao</td>
</tr>
<tr>
<td>Wealthfront</td>
<td>Li Cal  Tong</td>
</tr>
<tr>
<td>Financing</td>
<td></td>
</tr>
<tr>
<td>LendingClub</td>
<td>Ant Check Later</td>
</tr>
<tr>
<td>SoFi</td>
<td>WeSure</td>
</tr>
<tr>
<td>Insurance</td>
<td></td>
</tr>
<tr>
<td>Oscar Metromile</td>
<td>Zhong An Insurance</td>
</tr>
<tr>
<td>Metromile</td>
<td>WeBank</td>
</tr>
<tr>
<td>Banking</td>
<td></td>
</tr>
<tr>
<td>Atom</td>
<td>MYbank</td>
</tr>
<tr>
<td>Credit scoring</td>
<td></td>
</tr>
<tr>
<td>Credit Karma</td>
<td>Zhima Credit</td>
</tr>
</tbody>
</table>

Source: (Jones, & Ozcan, 2021)

In India the introduction of *Unified Payments Interface (UPI)* has included the exponential increase in online payment adoption and redefined customer sentiment\(^86\). The development of the “India Stack” – a set of APIs, open standards, and components of infrastructure necessary to allow customers to obtain a range of digital services – has facilitated the high rates of penetration. There have been some concerns raised that while interoperability has facilitated entry into UPI system, the inherent network scale advantages of BigTech firms could allow them to acquire a dominant position in the market. As such, regulators stipulate that in order to participate in the Stack, entrants are subject to regulatory oversight or their services must be linked through a regulated bank. A special category of banking license was introduced called the “payments bank” license with fewer regulatory requirements and a limit on the types of services that can be provided\(^87\).

### 3.6.2. Regulation of Bigtech in South Africa

Currently, the BigTechs have had limited activities in Open Banking in South Africa. Notwithstanding, regulators must be proactive in anticipation of potential entry. An imminent question pertains to whether BigTech firms may fall within the South African regulatory framework or not. If currently Apple and Facebook offer limited services in South Africa, e.g., loading credit card in the phone and tap with the phone, regulation may not be necessary but when they become registered, a pre-emptive decision must be made regarding what governs their involvement in the South African financial market, if registration will be compulsory. For example, it may become necessary to develop a bespoke set of regulatory requirements for BigTech firms distinct from the permissive environment provided to independent start-ups, or clear limitations on the degree of unregulated penetration permissible by BigTech firms to ensure that these firms do not expose the financial system to systemic risks.

---


4. CONCLUSION

This research examined the approaches to Open Banking adopted globally. Considering experiences in other jurisdictions, the research explored whether a market-led, or regulatory-led approach may be adopted in South Africa. We found that the key pillars that have a bearing on Open Banking implementation include: the type of data involved, data ownership, payment for data, opening of APIs and data privacy and security. As such, for Open Banking implementation to be a success in South Africa regulatory guidance is needed on these aspects. Furthermore, international experiences also show that whichever approach is pursued in South Africa, i.e., whether a market-led, or regulatory-led approach, relevant regulators including the Information Regulator must provide direction on the main pillars of Open Banking identified. This is where multi-stakeholder forums such as the IFWG which includes the Commission can serve a useful purpose of advancing discourse in this field.

The phenomenon of data ownership is of paramount importance in Open Banking. Banks have historically served as custodians of customer data. However, over the last few years, a paradigm shift globally has seen customers take ownership and consent of handling of their data to institutions of their choice. In South Africa, the research has pointed to shortcomings in the current regulatory framework especially the provisions PoPI Act in so far as they relate to who owns the data. Therefore, clarity on data ownership must be prioritised and speedily addressed by regulators in order to guide industry on what is permissible when Open Banking is implemented.

Data sharing can sometimes involve costs that may effectively be borne by data holders when providing access to other market players. From a competition perspective, concerns have been raised that the incumbents may engage in conduct that may harm competition such as excessive pricing. To address these concerns, regulatory guidance is also required to clarify on what grounds can compensation be permitted to access data. This is to ensure that compensation for data access does not create a barrier and thereby restrict competition. The question on whether to implement open APIs in the financial sector must further be addressed. This is to provide industry with a clear direction on an appropriate API framework for South Africa. Lessons can be drawn from jurisdictions that have already developed APIs for the financial sector to make Open Banking possible.

Another key feature of Open Banking explored in this research pertains to data privacy and security. Notwithstanding the regulatory framework which empowers consumers to give consent in order for their personal data to be shared, data privacy and security considerations may pose difficulties to compel dominant players such as the larger banks to provide data access to SMEs
(i.e., Fintechs). In the context of Open Banking, targeted legislation on data privacy and security may be necessary to establish acceptable data privacy and security standards. Therefore, supervision is required on how data can be shared without compromising data privacy and security.

This research has also observed that while not yet an imminent threat, the Open Banking initiative does invite the entry of BigTech firms and not just Fintech start-ups into the financial system, which, while increasing competition and the penetration of financial services in the short run, may create a long-term risk of monopolisation or gatekeeping by BigTech firms. Furthermore, as BigTech firms become more pervasive in the financial system without regulatory oversight, systemic risk in the system will likely escalate. A pre-emptive decision must be made regarding their involvement in the South African financial market if registration will be compulsory. For example, it may be necessary that bespoke regulation be developed for BigTech firms with limitations on the allowable penetration by these firms into the financial system before systemic risk exposure requires regulatory oversight.
5. **APPENDIX**

5.1 **Types of data**

Banks and financial institutions have traditionally been the primary holders of consumer financial data and access to this data has consequently been controlled by these banks and subject to substantial regulatory oversight. The types of data that these financial institutions typically keep broadly consist of data in the following three broad categories: customer data, transaction data, and value-added customer data. Customer data is information provided directly to the bank, such as employment information and tax filings; transaction data includes records of payments, withdrawals and other account activities; and value-added customer data is the data generated by banks and financial institutions to gain specific insights on a consumer, such as credit scores.

Increasingly, customer data in the financial sector has grown to include real-time electronic data without the traditional barrier of banking and financial institutions that have strong regulatory oversight. This customer data varies in terms of the data type, how the data is collected and how the data is used. **Figure 4** below describes and compares traditional and emerging types of customer data that may be used in the financial sector.

**Figure 4: Traditional and emerging forms of customer data used by financial firms**

<table>
<thead>
<tr>
<th>Traditional forms</th>
<th>Emerging forms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity</strong></td>
<td>Fingerprint, photographs, iris scan, digital ID</td>
</tr>
<tr>
<td>Public records, tax filings</td>
<td>Fitness tracking, sleep/eating habits</td>
</tr>
<tr>
<td><strong>Health</strong></td>
<td>Medical records, insurance claims</td>
</tr>
<tr>
<td><strong>Financial</strong></td>
<td>Bank statements, credit scores</td>
</tr>
<tr>
<td><strong>Social</strong></td>
<td>Organization registries</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Telephone books</td>
</tr>
<tr>
<td><strong>Media behaviour</strong></td>
<td>Library checkout histories</td>
</tr>
</tbody>
</table>

*Source: (WEF, 2018)*

---


The way data is collected or created demonstrate how different stakeholders contribute to data co-creation\(^91\). Customer data can be volunteered by the customer, observed in terms of the behaviour displayed by the customer, derived by the firm, or acquired from third parties\(^92\).

- **Volunteered** data is when the customer explicitly shares information with the firm about themselves or others,
- **Observed** data is created by the firm where the activities of the customer are captured and recorded,
- **Derived** data is created by the firm using data analytics, such as data that is created mechanically using simple reasoning and basic mathematics to detect patterns, and;
- **Acquired** data is either purchased from third parties on a commercial basis using commercial licensing contracts or on a non-commercial basis such as through open government initiatives\(^93\).

The way that the data will be used also has implications for how it can be shared. Customer data may simply be used internally by the firm for core business processes, to improve products and services, managing risk and marketing; or it may be shared with third parties. Specific data may be used for one or multiple purposes, both internally and with the third parties for monetisation or otherwise, and some data uses are mandated by law, for example, to prevent fraud\(^94\).

**Figure 5** below provides a useful overview of the different sources data that may be used in financial services, where they are collected from and how they may be used by firms.

---


When it comes to the way data access is conducted, there are two additional considerations; namely, the degree of identifiability (when it comes to personal data), which dictates the degree to which the data may be made openly available and the legal and technical protections that may be required, and the domain of the data, which dictates the legal rights that may apply to the data and reflect stakeholder interest.

The degree of identifiability of the data can be distinguished into five categories:

- **Identified data** can explicitly be linked to a specific person, because the information contained in the data is personally identifiable,
• **Pseudonymised data** is when the personal identifiers of the data have been **substituted** with aliases that cannot be reasonably reversed except by the person that assigned the aliases,

• **Unlinked pseudonymised data** is when the personal identifiers of the data have been erased or substituted with aliases that even the party assigning the aliases cannot reverse,

• **Anonymised data** is where the data and subject are unlinked and the attributes have been changed, so that there is reasonable confidence that a specific individual cannot be identified directly or indirectly with the data or in combination with other data, and

• **Aggregated data** does not include data entries at the individual level and is instead combined with information with enough other individuals that individual-specific identifiers cannot be discerned.

There are three domains of data, which may overlap when reflecting different stakeholder interests:

• **Personal** domain refers to data that is related to an identified or identifiable individual that has a privacy interest in the data,

• **Private** domain refers to proprietary data that is protected by intellectual property rights or access control rights and where there is an economic incentive to withhold access to others, and

• **Public** domain refers to data that is not protected by intellectual property rights or access control rights, and the data is free for access and re-use.

Overlapping domains may occur in instances when the data is generated, created, collected, processed, preserved, maintained, or disseminated by the private sector, but is funded by the public sector. In this instance, there is both a private interest and public interest in the data, which may create a conflict in interests as public sector data typically lies in the public domain, whereas privately produced data typically lies in the private domain.

---


5.2 OPEN BANKING APPROACHES

5.2.1 Market-led approaches

5.2.1.1 Hong Kong

From January to March 2018, the Hong Kong Monetary Authority (HKMA) conducted public consultations on the draft Open Application Programming Interface (API) framework. The release of open API framework is part of the endeavors announced by the HKMA to transition Hong Kong to a new era of smart banking. The API is a computer programming approach developed to enable the exchange of information. It also allows third parties to access information of an organization securely.\(^{100}\)

The HKMA received commentary from several stakeholders on its draft API framework including from banks, technology/fintech firms, industry associations, consulting firms, payment card scheme operators, individuals, and other relevant organisations. The HKMA’s policy direction in developing an open API framework has been widely welcomed by the industry, although some stakeholders required further details or clarification.\(^{101}\)

A collaborative and phased approach to implementing the API framework was adopted. The framework is designed to provide guidance in the market and ensure flexibility, rather than prescribing how banks should implement it.\(^{102}\) It also applies to the retail banking market segment which covers the services offered to the largest group of customers. However, it is noted that banks are not precluded from extending it to other banking segments they see fit. Its three main policy objectives are to (i) ensure the competitiveness and relevance of the banking sector; (ii) provide a secure, controlled, and convenient environment to allow banks and third-party service providers, to collaborate and develop innovative or integrated banking services that improve customer experience; (iii) and to keep up with international best practice and standards in the provision of banking services.\(^{103}\)

The scope of the API framework consists of, inter alia, the deployment timeframe; technical standards on architecture, security, and data; governance model; facilitation measures; and ongoing development. The open APIs are classified into four main categories starting with

\(^{100}\) https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/open-application-programming-interface-api-for-the-banking-sector/#:~:text=the%20Banking%20Sector


information sharing on products and services (i.e., the information offered by banks on details of their products and services) and ending with sharing of transactional information including banking transactions and payments. However, it is acknowledged that data protection is key for the successful implementation of the API framework at each level where data is shared between parties.104

In July 2018, the HKMA issued the final Open API framework following extensive consultations with stakeholders. The framework proposed a phased approach to the introduction of the open APIs given the sensitive nature of data and the risks concomitant with each category or type of data shared. In this regard, the HKMA proposed a four-phased approach of implementation following the publication of the final API framework as reflected in Table 2 below.

Table 2: Timelines of Open API implementation in Hong Kong

<table>
<thead>
<tr>
<th>Phase</th>
<th>Categories of Open Banking</th>
<th>Timeline after the publication of Open API framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Product and service information</td>
<td>6 months</td>
</tr>
<tr>
<td>II</td>
<td>Subscription and new applications for product/service</td>
<td>12-15 months</td>
</tr>
<tr>
<td>III</td>
<td>Account information</td>
<td>To be set out within the next 12 months</td>
</tr>
<tr>
<td>IV</td>
<td>Transactions</td>
<td>To be set out within the next 12 months</td>
</tr>
</tbody>
</table>


There is, however, leeway for banks to develop their timeframes to advance the implementation of open APIs. Banks are further required to adhere to sound industry security standards by adopting controls on information and cybersecurity based on a risk- and principle-based approach in order to protect the banks’ systems as well as bank and consumer data. To expedite the introduction of open APIs banks are, moreover, permitted to determine their own data specifications which should be made public.105

A proposal has been made to establish a body responsible for reviewing the architecture, security, and data standards on an ongoing basis. The body may also take on other industry-related tasks, such as coordination and consumer education. Lastly, the HKMA has committed to work closely with the banking industry in the implementation process to ensure an effective, secure and smooth process.106

5.2.1.2 Singapore

Singapore is among the pioneer countries to implement Open Banking in the Asian region. The implementation is premised on its digital ecosystem, ideal for fintech companies and the adoption

of APIs.\textsuperscript{107} The Monetary Authority of Singapore (MAS) had anticipated way before others the indispensability of APIs in bringing radical improvement in financial services area. Thus, way back in 2013, the MAS introduced the “Finance-as-a-Service: API Playbook” and the Finance Industry API Registry. \textsuperscript{108} The purpose of the Playbook is to support data exchange and communication between banks and fintechs as well as for the design and usage of APIs by relevant stakeholders. The Playbook has also been developed with the ambition that it will be a reference guide that can be adopted in the wider Association of Southeast Asian Nations (ASEAN) region, especially by countries who are embarking on similar API programmes.\textsuperscript{109}

As of November 2019, 470 APIs were published in the API Register by the financial institutions operating in Singapore. Both the MAS and the financial institutions in Singapore are unanimous on the fact that opening up of customer data lead to innovations. Despite proliferation of APIs, their standardisation is a task that remains to be fulfilled.\textsuperscript{110}

The MAS’ approach is slightly different to that seen in the UK. Normally the MAS will create a new system that banks, and other financial institutions could use, but they do not mandate companies. The MAS creates API recommendations that the banks can choose to use or not.\textsuperscript{111} Open Banking in Singapore is the use of open APIs that enable third-party developers to build applications and services around the financial institution. This enables greater financial transparency options for account holders, allowing them to direct the use of their financial data where they see appropriate.\textsuperscript{112}

Currently in Singapore there is no specific data sharing or Open Banking legislation. However, the government provide a guideline for Open Banking APIs, which are defined via a publicly available infrastructure. In 2018, the MAS was the first to provide guidance and a legal framework for Open Banking when it launched the APIX, a new digital innovation ecosystem with APIs related to data regulation. The APIX is an open-architecture API marketplace and sandbox platform for collaboration between fintechs and financial institutions in which participants can integrate and test solutions with each other via a cloud-based architecture.\textsuperscript{113} So far, it has registered more than 120 transactional APIs and almost 200 informative APIs.\textsuperscript{114} Several financial institutions and leading

\textsuperscript{108} http://www.jcreview.com/fulltext/197-1606458428.pdf
\textsuperscript{109} https://abs.org.sg/docs/library/abs-api-playbook.pdf
\textsuperscript{110} http://www.jcreview.com/fulltext/197-1606458428.pdf
\textsuperscript{112} https://uploads-ssl.webflow.com/5f09129bc08517c75c0103d5/5f0a3631c0851727f502bdc3_aot-globalopenbankinglandscapev1-200621043820-compressed.pdf
\textsuperscript{113} https://uploads-ssl.webflow.com/5f09129bc08517c75c0103d5/5f0a3631c0851727f502bdc3_aot-globalopenbankinglandscapev1-200621043820-compressed.pdf
banks rely on APIX to scale their products. For instance, at least 50 financial institutions and 140 fintech companies now rely on APIX technology to scale their financial products in a secure digital environment. In addition, large Singaporean banks, such as DBS, OCBC, and UOB, are already working with these technology companies or Third-Party Providers (TTPs) to launch apps that use their APIs.  

Further, Singapore has also recently launched a fintech aid package considering the COVID-19 pandemic. The aid package includes 6 months free access to APIX for startups, as well as financing and training grants for their employees.

In November 2020, Personal Data Protection Amendments (PDPA) were passed by Parliament and began to take effect in phases beginning on 1 February 2021. The amendments enhance consumer protection and strengthen accountability of organizations. Key changes include (i) new mandatory data breach notification (ii) penalties for new offenses should personal data be mishandled (iii) increased financial penalty cap for breaches, and (iv) additional rules on telemarketing and spam control.

Amendments to take effect in future phases include data portability and increased financial penalties, which are currently capped at S$1 million (approximately US$742,500). For organizations with annual revenues in Singapore of more than S$10 million, the new maximum financial penalty will be increased to 10% of annual revenues (S$1 million minimum). Maximum penalties for organizations with less than S$10 million have been changed with the new maximum financial penalty will be S$1 million.

5.2.1.3 Japan

The Banking Act of Japan (as amended) is the overarching piece of legislation that governs the banking sector. The Financial Services Agency (FSA) is the regulatory authority responsible for ensuring the stability of the Japanese financial system as well as user protection and convenience and market fairness and transparency.

The process of Open Banking introduction in Japan was associated with the issuing of the “Principles for Customer-Oriented Business Conduct” by the FSA in 2017. The purpose was to encourage financial institutions to voluntarily adopt these principles and publish their policy and
achievements in this regard in the public domain. This was to enable consumers to compare financial institutions’ customer-oriented initiatives and select financial institutions that would satisfy their financial needs.\textsuperscript{120} The customer-orientated principles included, \textit{inter alia}, the necessity to clarify fees and provide easily understandable product sales information.\textsuperscript{121}

During June 2018, Japan also amended its Banking Act to promote Open Banking by facilitating collaboration between banks and third-party firms.\textsuperscript{122} As part of the amendments, a new regulatory framework for electronic payment service providers (EPSPs) was introduced, which applies to both payment initiation service providers (PISPs) and account information service providers (AISPs) along with a registry process of EPSPs that is managed by the FSA. An authorization process was, therefore, established for TPPs, because the amended Act makes provision for TPPs to be allowed access to specific data as a right if licensed or authorized, whilst at the same time ensuring user protection.\textsuperscript{123}

The Japanese FSA also obliged banks to publish their open API policies and encouraged them to contract with at least one TPP by 2020.\textsuperscript{124} The deadline for implementation of APIs was initially set for 31 May 2020. However, progress has been rather sluggish owing to an incident where customer money was stolen from bank accounts which were breached via FTSP accounts in September 2020.\textsuperscript{125} It is further noted that some criticisms emerged that the Japanese regulatory framework lacks clarity on data portability. The implementation of Open Banking components further remains voluntary\textsuperscript{126}, and depend on the Japanese Banking Association (JBA) to define broad and high-level data-sharing policies whilst banks continue to contract bilaterally with third-party firms.\textsuperscript{127}

5.2.1.4 China

China is a prime example of the significant impact that the fintech sector and especially BigTech firms can have on the banking sector. The Chinese mobile-based connectivity ecosystem and regulatory framework that is conducive for innovation has provided scope for the large tech companies to increase their market shares in terms of customer base. For instance, Alibaba, which is China’s largest e-commerce company introduced Alipay in 2003 as a third-party online payment platform. Alipay has been an integral part of Alibaba’s success which currently offers a bouquet of

\textsuperscript{120} \url{https://www.fsa.go.jp/en/news/2020/202007fd/201909fd.html}
\textsuperscript{121} \url{https://www.oecd.org/finance/financial-education/Effective-Approaches-FCP_Principles_Digital_Environment.pdf}
\textsuperscript{122} \url{https://www.fsa.go.jp/en/newsletter/weekly2018/296.html}
\textsuperscript{123} \url{https://www.cgap.org/sites/default/files/publications/2020_10_Working_Paper_Open_Banking.pdf}
\textsuperscript{124} \url{https://www.oecd.org/finance/financial-education/Effective-Approaches-FCP_Principles_Digital_Environment.pdf}
\textsuperscript{125} \url{https://talkingtech.cliffordchance.com/en/industries/fintech/payments-trends-2021--continued-expansion-of-open-banking-and-o.html}
\textsuperscript{126} \url{https://www.frbsf.org/banking/asia-program/pacific-exchanges-podcast/open-banking-apis-japan/}
\textsuperscript{127} \url{https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-open-banking-report-noexp.pdf}
services including payments, wealth management, lending, insurance, and credit scoring services. Another tech giant, namely; Tencent (which owns the social network app WeChat) is used to make payments (both online and in physical stores and to settle utility bills). It is estimated that the two Chinese tech firms account for over 90% of the market.\footnote{https://www.oecd.org/daf/competition/digital-disruption-in-banking-and-its-impact-on-competition-2020.pdf; https://www.fljs.org/sites/default/files/migrated/publications/Alibaba%20and%20the%20Threat%20to%20China%22%20-%20Whitepaper.pdf}

In March 2019, Tencent and WeBank announced the creation of a new FinTech Research Lab. The aim of the Lab is to develop an Open Banking framework to support banks in implementing an Open Banking regime. However, there are still no tangible plans for an introduction of a regulated Open Banking in China. In this regard, the development of open APIs will continue to be spearheaded by market players and customer needs.\footnote{https://www.openbankingexpo.com/wp-content/uploads/2019/09/ndgit-Open-Banking-APIS-worldwide-Whitepaper.pdf}

5.2.1.5 India

The Indian financial landscape is like other developing countries in that access to financial services is very low. There have been numerous initiatives undertaken by the government to address this issue including the introduction of the IndiaStack which developed a set of APIs (Aadhaar, eKYC, Digilocker and eSign), the launch of the Unified Payments Interface (UPI) and the issuing of prescribed Account Aggregator (AA) guidelines on acceptable activities and API specifications.

IndiaStack

Beginning in 2010, the Indian government launched the Aadhaar identification system to which all citizens are entitled. This system was initially developed to improve the delivery of government services by enabling biometric checks for verification of the identity of the holder, thus reducing the chances of false identities and fraudulent claims to state benefits. It is noted that the introduction of a low-cost digital ID facilitated a large expansion in the user base, which has been crucial for the success of Open Banking implementation in India to date. The introduction of the digital ID was instantly followed by its linking with several public sector services, including banking services. For instance, to facilitate access to the banking system, the Reserve Bank of India (RBI) enabled the holder of the Aadhaar ID to authorize a bank to obtain an electronic verification of their identity through the Unique Identification Authority of India (UIDAI) in 2013. The UIDAI is an
an independent entity responsible for facilitating the collection of demographic and biometric data for verification purposes and stores this information on a central identity repository.\textsuperscript{130}

\textit{Unified Payments Interface (UPI)}

Other set of APIs include the pilot of the launched UPI system\textsuperscript{131} in 2016 by the National Payments Council of India (NPCI).\textsuperscript{132} In order to participate in the UPI system, fintech firms are required to operate, either through an institution with a banking license or by obtaining a special payment bank license that would ensure that they are regulated. The regulation of fintech firms allows the RBI to promote financial inclusion while fulfilling its objective of ensuring the system’s stability and resilience. The design of the system has proven sufficiently flexible to facilitate entry of many new tech-based payment service providers into the UPI, increasing competition and user choice.\textsuperscript{133}

Interoperability of the payments system has been operationalized through open APIs, available to banks and to fintechs who leverage links to existing banks. This has created an environment for greater competition in the provision of a broad range of financial services that leverage data collected via the payments interface.\textsuperscript{134} Other positive outcomes realised from the introduction of the UPI in India have included the exponential increase in online payment adoption and redefined customer sentiment.\textsuperscript{135} However, there have been some concerns raised that while interoperability has facilitated entry into UPI system, the inherent network scale advantages of BigTech firms could allow them to acquire a dominant position in the market.\textsuperscript{136}

\textit{Account Aggregator}

India’s implementation of an Open Banking regime was reinforced when the RBI announced the establishment of the Account Aggregator (AA) in September 2016. The AA is an independent entity entrusted with, \textit{inter alia}, ensuring the sharing of personal financial information provided that there is consent by a customer and appropriate authorisations between the AA, the customer, and

\textsuperscript{131} Unified Payments Interface (UPI) is a system that powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing & merchant payments into one hood.
\textsuperscript{132} https://www.npci.org.in/what-we-do/upi/product-overview
the financial services providers. The AA is also responsible for ensuring data security, resolution of customer complaints and transparency in the pricing of services.\textsuperscript{137}

Further, in order to facilitate transfer of data and consent-based sharing of financial information the RBI prescribed Account Aggregator (AA) guidelines. A set of core technical specifications were framed by Reserve Bank Information Technology Private Limited (ReBIT), a wholly owned subsidiary of the RBI for adoption by all regulated entities, acting either as Financial Information Providers (FIP) or Financial Information Users (FIU) in November 2019. The customers are also provided a functionality to revoke consent post which a fresh consent would have to be obtained. Explicit onus has also been placed on Financial Information provider (FIP) to verify the validity of the consent, specified date and usage of it and the credentials of the AA.\textsuperscript{138}

5.2.2 Regulatory-driven approaches

5.2.2.1 Europe

The European Commission proposed a comprehensive data protection reform package starting in 2012. This was intended at strengthening the European Union's (EU) 1995 data protection rules on online privacy rights and boost Europe's digital economy. The proposed reforms included, inter alia, streamlining of rules by ensuring that there is a single set of rules on data protection adopted in the EU and right to data portability to foster competition in the market where consumers will have easier access to their data and be able to transfer it from one service provider to another more effortlessly.\textsuperscript{139}

In 2015, the European Parliament adopted the Revised Payment Services Directive (PSD2) Regulation, which was published in the Official Journal of the EU.\textsuperscript{140} This Regulation replaced the first Payment Services Directive (PSD1) of 2007.\textsuperscript{141} The PSD2 Regulation acknowledges the increase of payment-related fintechs and one of its objectives is to create a level playing field for all payment service providers while ensuring security and customer protection in the process. In this regard, the PSD2 provides the legal framework within which the Open Banking regimes can be implemented in Europe by making it an obligation for all payment account providers across the EU

\textsuperscript{137} https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?id=3142
\textsuperscript{138} https://www.bis.org/review/r210419a.pdf
\textsuperscript{139} https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46
\textsuperscript{140} https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366
to provide third-party access. This can also be considered as an effort to shape how Open Banking standards should be executed in the EU.¹⁴²

Under the PSD2 Regulation, banks are required to develop APIs that meet the following minimum standards: (i) allow account information services providers (AISPs) and payment initiation services providers (PISPs) to identify themselves to the bank; (ii) permit AISPs and PISPs to communicate securely to request and receive accounts and payments information; and (iii) allow PISPs to initiate payment orders from customer’s payment accounts as well as receive all information on the initiation and execution of the payment transactions.¹⁴³

During May 2018, the EU passed another regulation into law, the General Data Protection Regulation (GDPR), replacing the Data Protection Directive 95/46/EC. The GDPR is applicable to organisations around the world that collect data related to people in the EU. The Regulation also imposes certain obligations on these institutions in upholding the prescribed privacy and security standards.¹⁴⁴ The GDPR is viewed an example of a rights-based approach to the control of personal data where data controllers and processors are obliged to ensure data security when data is transferred for analysis or value extraction. For instance, in reality, this method has involved data controllers issuing GDPR compliant checklists for data subjects in order to gain access to services.¹⁴⁵

5.2.2.2 United Kingdom (UK)

The UK formally introduced the Open Banking Standard in 2016 outlining how Open Banking data should be created, shared and used.¹⁴⁶ The implementation of the Standard was guided by recommendations from the Open Banking Working Group, that comprised of banks and industry groups and co-chaired by the Open Data Institute and Barclays.¹⁴⁷ However, in the UK, the collection and use of personal data are primarily governed by the Data Protection Act 1998 (DPA),¹⁴⁸ which the Information Commissioner is responsible for enforcing and overseeing. Before the exit of the UK from the EU, it was subjected to two other main pieces of legislation including the EU Revised Payment Services Directive (PSD2) of 2015 and Privacy and Electronic Communications Regulations of 2003 (PECR). The PECR Regulations were intended to complement

¹⁴² https://www.pwc.co.uk/financial-services/assets/open-banking-report-web-interactive.pdf
¹⁴³ https://www.lexology.com/library/detail.aspx?g=c287a1d01-8536-47dc-ba2a-7854f4f2456a7
¹⁴⁴ https://gdpr.eu/what-is-gdpr/
¹⁴⁶ https://www.pwc.co.uk/financial-services/assets/open-banking-report-web-interactive.pdf
¹⁴⁷ https://www.pwc.co.uk/financial-services/assets/open-banking-report-web-interactive.pdf
the DPA and made provisions for rules applicable to direct marketing activities through electronic means (e.g., fax, email, and telephone).  

The interventions by the UK Competition and Markets Authority (CMA) in the banking sector have also created a fertile ground for the adoption of Open Banking in the financial sector. For instance, in 2014, the CMA undertook a market investigation into the supply of retail banking services to the personal current account (PCA) and business current account (BCA) customers and small and medium-sized enterprises (SMEs) in the UK. The purpose of this inquiry was to assess the state of competition in the relevant markets and to propose remedies to address any findings on adverse impact on competition. The investigation focused on PCA services in the provision of an account marketed to individuals rather than businesses, offering facilities to hold deposits, to receive and make payments by cheque and/or debit card, to use ATM facilities and to make regular payments by direct debit and/or standing order.

The CMA’s final report that was released in August 2016, found that several features of the market had adverse effects on competition. The same concerns that were identified in the provision of PCAs, BCAs and SME lending in the UK, overlapped across these three market segments. For instance, the CMA found that an incumbent bank with a large established base of PCA customers would benefit from that established base, but also in the provision of BCAs, because of the commonalities between the two products. As a result, these market dynamics render a competitive advantage on such incumbent banks when competing in the provision of SME lending.

Another finding was that costs to customers, due to ineffective competition in PCAs and SME banking were likely to be high. The CMA further found significant variation in prices between banks and that the larger banks which benefit from the stronger incumbency advantages generally have higher prices (and lower quality) than smaller ones.

To address the competition concerns identified, the CMA proposed remedies aimed at driving innovation and improving products and service offerings as well as disrupting the status quo. The remedies included customer access to transactions history, customer awareness and confidence, competition to develop SME comparison tools, standardisation of information requirements for BCA and sharing of SME information ‘soft’ searches.

The CMA also announced measures to develop and require the use of open API standards and data sharing by requiring that the largest banks in the UK, namely; RBSG, LBG, Barclays, HSBCG,

---

150 https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf
Nationwide, Santander, Danske, BoI and AIBG to adopt and maintain similar API standards. This was to enable the standardisation and ease of data sharing with third-party service providers including price comparison websites (PCWs), account information service providers (AISPs) and payment initiation service providers (PISPs). The focal point of this remedy was further to ensure that the largest banks in the UK make data available using open API standards. As such, enable consumers and SMEs to identify products that suit their needs more easily and to create an environment where they can manage their finances better.

Another remedy imposed by the CMA was to require these largest banks in the UK to release and make data available through an open API including (i) The prices, charges, terms and conditions together with customer eligibility criteria, in the case of loans, for all PCA and BCA products (including overdrafts) and all SME lending products and (ii) the Reference Data such as branch and ATM location, branch opening hours as specified by the CMA (iii) data on service quality indicators (i.e., customer recommendation scores) as specified by the CMA. These remedies in totality were seen as a vehicle to potentially stimulate fierce competition in PCA and SME banking markets in the UK, by alleviating several barriers to accessing and assessing product and provider information.

However, it is noted that only institutions accredited by the Financial Conduct Authority (FCA) were eligible to be provided with access to open APIs. Further, customers are required to opt-in in order to share data. The CMA’s compliance due date of Open Banking implementation in the UK following its investigation was set for January 2018.151 The evolution of the COVID-19 pandemic has, however, impacted on the timing of implementation by industry. In this regard, the CMA has extended the deadline for Open Banking implementation to the end of 2021.152 Other recent developments to note in the UK include the formation of the Digital Regulation Cooperation Forum given the interface between competition and data protection in digital markets. The Forum consist of the CMA, Information Commissioner’s Office and the FCA.153

Outside the EU, other jurisdictions that have implemented a regulatory-driven approach are Australia, Bahrain, and Rwanda.

**5.2.2.3 Australia**

151 https://www.pwc.co.uk/financial-services/assets/open-banking-report-web-interactive.pdf
The plans for the introduction of Open Banking regime was announced by the Australian Government during the 2017-18 Budget. This process was aimed at empowering consumers to have greater access to and control over their banking data. For instance, Open Banking legislation compels banks to share product and consumer data with customers and third parties with the consent of the consumer.\textsuperscript{154}

The Open Banking regulatory framework in Australia focused on the scope of the banking data sets to be shared, the parties which will be required to share the data sets, and the parties to whom the data sets will be provided. Further, to determine existing and potential technical data transfer mechanisms including customer consent mechanisms. Data security and privacy issues as well as the costs and funding models of implementing an Open Banking regulatory model were considered.\textsuperscript{155}

After the conclusion of the Australian government’s review process on Open Banking rules, it was agreed in May 2018 that the Consumer Data Right (CDR) should be adopted.\textsuperscript{156} The CDR is established primarily through amendments to the Competition and Consumer Act of 2010 and the Privacy Act of 1988. According to the regulations, the CDR operates under a multi-regulator model, which consists mainly of three bodies, namely, the Australian Competition and Consumer Commission (ACCC), the Office of the Australian Information Commissioner (OAIC), and a new Data Standards Body.\textsuperscript{157}

It is noted that the CDR aimed at providing consumers with the right to securely access certain data about them held by businesses including banks. This Right would also permit consumers to share their data with whichever authorised third parties they may choose.\textsuperscript{158} As of 1 July 2020, Australia’s bank customers could permit accredited third parties to access their savings and credit card data, whilst as of 1 November 2020, they could also give consent to accredited third parties in accessing their mortgage, personal loan, and joint bank account data. This is viewed to yield benefits for consumers where they will be able to access data in a usable form and convenient manner. Consumers will also be empowered to search for better deals on banking products or to easily monitor their banking activities.

These benefits can also extend to SMEs since through data-sharing arrangements SMEs will be able to identify better business lending products, by considering historical borrowing needs. It is also noted that all customers (individuals; or small, medium, or large businesses) will be entitled to

\textsuperscript{154} https://treasury.gov.au/review/review-into-open-banking-in-australia
\textsuperscript{155} https://treasury.gov.au/review/review-into-open-banking-in-australia/terms-of-reference
\textsuperscript{156} https://treasury.gov.au/consumer-data-right
exercise the right concerning the classes of data covered by the CDR as reflected in Figure 6 below.159

**Figure 6: CDR applicable datasets in the financial sector**


During the first phase of the initial Open Banking implementation, it is noted that data sets are to be transferred, at the consumer’s direction, without charge. However, the CDR system will have the flexibility to provide for charging for access to data. This flexibility may be required in relation to access to value-added data or in instances where making data available for free, may disincentivize the collection and storage of such data in the market going forward. It is also worth pointing out that Australia has adopted a cautious approach where data sets will not all be subject to the CDR at the commencement of the Open Banking regime.160

The application of the Australian CDR is unique compared to other jurisdictions in that it applies to financial services but is also a sectoral data policy initiative. For instance, it will initially apply to banks, and then later rolled-out to other sectors including energy and telecommunications, with the possibility of being applied to any sector in the future. The CDR is also the first Open Banking legislation to introduce the concept of reciprocity. The reciprocity implies that those who wish to become accredited and receive designated data at a consumer’s request, must be willing to share equivalent data, in response to a consumer’s request.161 It is noted that the Treasury Laws Amendment (Consumer Data Right) Bill of 2019 allows the reciprocity arrangements to be established.162

---

Finally, the ACCC, OAIC and Data Standards body are responsible for overseeing the enforcement of the CDR by undertaking shared accountabilities. The ACCC will amongst other things take enforcement action in relation to serious or systemic breaches of the CDR in line with its mandate, whilst the OAIC will undertake the function of dealing with complaints from consumers. The Data Standards Body is envisaged to set technical standards relating to transmission of data, data format and security.\(^{163}\)

### 5.2.2.4 Nigeria

Banks in Nigeria are sitting on big data which is growing exponentially when considering that Nigeria has over 73,2 million active bank customers.\(^{164}\) This data can serve a useful purpose in the context of Open Banking.\(^{165}\) In February 2021, Nigeria issued a regulatory framework for Open Banking to ensure the simplification and integration of multiple and complicated financial services. The framework is fundamental in driving innovations in the financial services sector. Prior to the issuing of the framework, banks operated in a closed ecosystem, with exclusivity of access to customer information, locking out innovators; and forcing customers to rely solely on the digital channel offerings of their respective banks. The purpose of the framework is to enhance financial inclusion, foster the sharing and leveraging of data with third-party financial services firms to build solutions and services that provide efficiency, greater financial transparency, synchronization and options for account holders across Nigeria.\(^{166}\) In tandem with international best practices adopted in other jurisdictions in relation to Open Banking, the framework seeks to achieve ease of accessibility of data to third parties and innovators. The framework applies to the following financial services:\(^{167}\) payments and remittance services; collection and disbursement services, deposit-taking; credit; personal finance advisory and management, treasury management, credit ratings/scoring; mortgage; leasing or hire purchase and other services as may be determined by the Central Bank of Nigeria (CBN).

The framework makes several provisions including data and API access requirements, principles for API, data, technical design, and information security specifications.

#### Data exchange

Under the Framework, there is certain data that may be exchanged and not every participant has access to all the categories of information made available. The Risk Management (“RM”) Maturity Level of

---


\(^{164}\) [https://techcabal.com/2021/03/25/open-banking-nigeria/](https://techcabal.com/2021/03/25/open-banking-nigeria/)

\(^{165}\) [https://techcabal.com/2021/03/25/open-banking-nigeria/](https://techcabal.com/2021/03/25/open-banking-nigeria/)


\(^{167}\) [https://www.aelex.com/regulatory-framework-for-open-banking-in-nigeria/](https://www.aelex.com/regulatory-framework-for-open-banking-in-nigeria/)
participants determines API services that may be implemented by and used by participants. The RM Maturity Level ranging from tier 0 to 3 and participants categories are presented in Table 3 below.

**Table 3: RM maturity level and participants categories**

<table>
<thead>
<tr>
<th>RM maturity level</th>
<th>Participant's category</th>
<th>Risk rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 0</td>
<td>Participants without regulatory license</td>
<td>Low</td>
</tr>
<tr>
<td>Tier 1</td>
<td>Participants through CBN Regulatory Sandbox</td>
<td>Moderate</td>
</tr>
<tr>
<td>Tier 2</td>
<td>Licensed payments service providers and other financial institutions</td>
<td>High</td>
</tr>
<tr>
<td>Tier 3</td>
<td>Deposit money banks</td>
<td>High and sensitive</td>
</tr>
</tbody>
</table>


There are four access levels by data and service category and applicable RM Maturity Levels as presented below.

**Table 4: Description of access levels by data and service category and applicable RM maturity levels**

<table>
<thead>
<tr>
<th>Access levels by data and service category</th>
<th>Description</th>
<th>Applicable RM maturity levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Information and Service Touchpoints (“PIST”)</td>
<td>Information shared under this category has a low-risk rating and includes information on products provided by participants to their customers and access points available for customers to access services including ATM/POS/Agents locations, channels (website/app) addresses, institution identifiers, service codes, fees, charges and quotes, rates, and tenors.</td>
<td>Information accessed by participants across all the Tiers (0-3)</td>
</tr>
<tr>
<td>Market Insight Transactions (“MIT”)</td>
<td>Information shared under this category has a Moderate-risk rating and includes statistical data aggregated on basis of products, service, segments, etc. The information is not associated to any individual customer or account. These data could be exchanged at an organizational level or at an industry level.</td>
<td>Information accessed by participants across all the Tiers (0-3)</td>
</tr>
<tr>
<td>Personal Information and Financial Transaction (PIFT)</td>
<td>Information shared under this category has a High-risk rating and includes data at individual customer level either general information on the customer (e.g., KYC data, total number or types of account held, etc.) or data on the customer’s transaction (e.g., balances, bills payments, loans, repayments, recurring transactions on customer’s accounts, etc.)</td>
<td>Information accessed by participants across all Tiers excluding Tier 0 participants (1-3)</td>
</tr>
<tr>
<td>Profile, Analytics and Scoring Transaction (“PAST”)</td>
<td>Information shared under this category have a High and Sensitive-risk rating and includes information on a customer which analyses, scores, or gives an opinion on a customer e.g., credit score, income ratings etc.</td>
<td>Information only available to Tiers 2 and 3</td>
</tr>
</tbody>
</table>


It is noteworthy that under this framework, the CBN commits to regulate the development of a common banking industry API standard with technical design standard, data standard, information security
standard and operational rules. Participants who include providers, consumers, fintechs, developer community and the CBN may assume different roles under the framework. Overall, participants are required to adhere to the Risk Management principles including but not limited to having information technology and information security policies; and a risk management framework that address APIs; a designated chief risk officer who shall be responsible for implementing effective internal control and risk management practices; updated API risk catalogues and API process control mapping and risk control matrix. The different roles of the participants under the Framework are summarized below.168

**Provider**

A provider is a participant that mainly uses APIs to avail data or service to another participant. The role of the provider is to publish the APIs and define the requirements and technical guidelines as well as the data and services accessible through the APIs.

**Consumer**

A consumer is a participant that uses APIs released by the providers to access data or service. In compliance with data privacy laws and regulations including the Nigerian Data Protection Regulations (“NDPR”), the consumer, inter alia, is required to obtain the consent of the end-user on each action that may be performed on the account of the end user as specified by the provider.

**Fintechs**

These include companies that provide innovative financial solutions, products, and services. The framework recognises that fintechs may either be consumers or providers of APIs and are required to assume the responsibilities of either consumer or provider depending on the role played at the relevant time. In addition, fintechs are required to leverage APIs to innovate products and solutions that are interoperable and comply with data privacy laws and regulations.

**Central Bank of Nigeria**

The CBN has the oversight of the implementation and operations of Open Banking. Further to review and enforce the Open Banking framework. It also arbitrates disputes among participants before any litigation or commencement of a judicial process. The CBN is required to develop Common Banking Industry API Standards within twelve (12) months of the issuance of the Framework and maintain an Open Banking Registry.

Another aspect of the Nigerian Open Banking framework is that of consumer rights. The protection of the customer is the responsibility of all the participants in the Open Banking ecosystem. Participants are

therefore required to adhere to the provisions of the Consumer Protection Framework of the CBN in their dealings with customers as well as data privacy laws and regulations; particularly the NDPR. There are additional requirements imposed by the framework notably the requirement that agreements presented to the customer by the participant should be simple, explicit and in the customer’s preferred language; and in the customer’s preferred form including written, electronic, video or audio form. A copy of the customer’s consent should be made available to the customer and preserved by the participant. The specific rights which the customer will be granting to the participant as well as the implication of granting those rights to the participant should be listed for the customer to consent to separately. The provisions of the framework also require that the consent of the customer be re-validated annually and where the customer has not used the service of the partner for a maximum of 180 days.169

5.2.2.5 Bahrain

Bahrain was the first country in Middle East and North Africa (MENA) to introduce regulations that stipulated the adoption of Open Banking by all retail banks. The Central Bank of Bahrain (“CBB”) launched the Bahrain Open Banking Framework (Bahrain OBF) to ensure holistic implementation of Open Banking services by the industry. The Bahrain OBF sets the stage for the practice of sharing financial information electronically, securely, and only under conditions that customers agree to. The framework includes detailed operational guidelines, security standards and guidelines, customer experience guidelines, technical open API specifications and the overall governance framework needed to protect customer data.170

The Central Bank of Bahrain gave the traditional banks six months to comply (starting on 28 October 2020 and ending on 30 April 2021) before going live. Bahrain learnt a lot from the EU experience and prior to the launch of the Bahrain OBF, the CBB had issued rules relevant to Open Banking in December 2018 which were aligned to the European Payment Services Directive (PSD2).171 However, in contrast to other jurisdictions, the framework has been customized for Bahrain and every bank in Bahrain has had to open up their APIs, as CBB required banks to publish every piece of data they hold on customers through these APIs.172

The first company to receive an Open Banking license in Bahrain was Tarabut Gateway (TG) which is the first and only licensed Open Banking provider in the Middle East and North Africa.173 It took the startup three years to plug in all the financial institutions in the country. TG is a common infrastructure API base

171 https://thepayers.com/online-mobile-banking/bahrain-based-banks-are-ready-for-open-banking--1249118
173 https://www.thebuzzbusiness.com/bahrain-leads-way-to-open-banking/
that connects every single financial institution on a single platform aggregating data from all the financial institutions to create a marketplace between financial institutions.\textsuperscript{174}

The framework entails the provision of two broad categories of services i.e., account information service and payment initiation service. Account information service provides customers with access to all bank account information in an aggregated manner through a single platform. Payment initiation service allows licensed third parties to initiate payments on behalf of customers while allowing seamless transfers between different customer accounts through a mobile based application.\textsuperscript{175} The customer can choose when, for what purpose and for how long, to give access to their data and only third-party providers regulated by the CBB can provide Open Banking services in the country.\textsuperscript{176}

There is an added uniqueness in the Bahrain OBF in that it is the first in the world to include Islamic banking licensees. The framework is also not rigid in the sense that it will continue to be revised and updated periodically, based on inputs from the industry and changing global trends.\textsuperscript{177}

\textbf{5.2.2.6 Rwanda}

The National Bank of Rwanda (BNR) has acknowledged that fintech and more particularly increasing the availability of digital customer data can revolutionise financial markets.\textsuperscript{178} Rwanda’s approach towards Open Banking has been based on European Union’s PSD2. Provisions were made in the legislation for new types of payments providers and regulatory sandbox design.\textsuperscript{179} The Open Banking regulation in Rwanda covers individual consumers and small businesses and addresses data sharing and portability with a view to encourage innovation, efficiency, new product development and facilitate entry. The aim is to use consumers’ digital data strategically to generate economic advantage.\textsuperscript{180} As in the UK and Europe, informed customer consent is required.

It is significant to note that telcos (telecom companies) are playing important role in fintech development in the country, which is a key requirement for the success of Open Banking. It is, therefore, critical that Rwandan legislation and policy should apply to and require participation by telecommunications companies and mobile banking providers in addition to traditional banks.\textsuperscript{181}

\textsuperscript{174} https://www.wamda.com/2020/11/issue-open-banking-part-two
\textsuperscript{175} https://www.cbb.gov.bh/media-center/cbb-launches-the-bahrain-open-banking-framework/
\textsuperscript{176} https://www.fccib.net/news/n/news/bahrain-launches-open-banking-framework.html
\textsuperscript{177} https://www.fccib.net/news/n/news/bahrain-launches-open-banking-framework.html
\textsuperscript{179} http://www.jcreview.com/fulltext/197-1606458428.pdf
\textsuperscript{181} https://thepaypers.com/expert-opinion/open-banking-a-very-global-business--1240033
In alignment with the country's aspiration to transform its economy into one which is both service oriented and knowledge-based, the umbrella of financial services has been fast spreading. As per Rwanda's Vision 2020, the country has a target for 90% financial inclusion by 2020. Considering the rapid spread of financial inclusion and rather early initiatives taken with regard to introduction of Open Banking, Rwanda makes for an interesting case in the African continent.\(^{182}\)

The introduction of APIs in the financial sector is included within the framework, which also supports the implementation of (technical) standards by 2024.\(^{183}\)

### 5.2.3 Transition from market-led growth to a regulated framework

#### 5.2.3.1 United States (US)

The US has also elected for a market-led approach with prospects of transitioning to a regulated framework. This because of the limited government initiatives to support the development of Open Banking products and services. It is notable that there are several private sector initiatives driving the adoption of Open Banking and APIs in the US. For instance, The Clearing House Payments Company's (TCH) created a Model Agreement that banks and third-party firms (fintechs) can use as a guide in developing API-related data sharing agreements. Use of the Model Agreement is entirely voluntary and may require modifications where feasible. The Model Agreement has been established to be consistent with relevant US regulations and polices including the Consumer Financial Protection Bureau (CFPB's) Consumer Protection Principles.\(^{184}\)

In 2018, financial sector stakeholder groups in the US have further created frameworks to develop common standards for Open Banking to promote interoperable and royalty-free standards for financial data sharing. The Financial Data Exchange (FDX) has aligned its member institutions in adopting a standard Open Banking regime. The FDX members include financial institutions, financial data aggregators, fintechs, payment networks, consumer groups, financial industry groups and utilities and other stakeholders. It is noted that as of the beginning of 2021, FDX increased its membership base to 186 organizations with an addition of 18 new members.\(^{185}\) The National Automated Clearing House Association (NACHA) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) have also developed APIs to enable safe transfer of data between parties in the US.\(^{186}\)

---


\(^{185}\) [https://financialdataexchange.org/FDXNews/Press-Releases/FDX_Adds_18_New_Members.aspx](https://financialdataexchange.org/FDXNews/Press-Releases/FDX_Adds_18_New_Members.aspx)

\(^{186}\) Federal Reserve Bank of Boston. 2021. “Modernizing U.S. Financial Services with Open Banking and APIs”.
The transaction where Mastercard was approved by the US Department of Justice to acquire Finicity in 2020 is another recent development that will enhance opening banking activities in the US. For instance, the transaction is envisaged to assist Mastercard to strengthen its Open Banking services given that Finicity is a leading North American provider of real-time access to financial data. This will also allow customers to determine how and where third parties such as fintechs or other financial institutions can access their personal financial information.187

However, some interventions by the CFPB and the US Department of Treasury in accelerating momentum to move towards a more connected and Open Banking cannot be undermined. The CFPB issued voluntary “Consumer- Authorized Financial Data Sharing and Aggregation” guidelines in 2017 focusing on amongst other things consumer control and transparency, informed consent, and data privacy. This was following an instruction from the US Congress that the Bureau must implement and enforce consumer financial law for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive. Further, the Bureau was mandated with exercising its authorities so that markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation.188

In November 2020, the CFPB published an Advance Notice of Proposed Rulemaking (ANPR) for consumer-authorized access to financial records for public comment. For instance, section 1033 of the Dodd-Frank Act of 2010 makes provisions for consumer access to financial records subject to the rules prescribed by the CFPB.189 With the publication of the Notice, the Bureau was therefore inviting comments from the public to assist it in developing regulations to implement section 1033. 190

The US Treasury Report in 2018 also recommended developing regulatory approaches to enable secure data sharing in financial services.191 The report highlights the challenges with the state and federal regulatory frameworks due to the highly fragmented and state-based nature of banking and banking regulation in the US. For instance, in respect of lending and servicing, there are concerns that because different states in the US set varying maximum loan interest rate requirements, this can materially impact which products are available to consumers. In this regard, emphasis is placed on the harmonization of

189 https://www.govinfo.gov/content/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf
190 https://www.govinfo.gov/content/pdf/2020-23723.pdf
regulatory frameworks and the adoption of a common federal policy on Open Banking to address these challenges.\(^{192}\)

5.2.4 **The Cegedim Case\(^{193}\): Refusal to sell medical information database**

The Cegedim Case shows how competition agencies have dealt with anti-competitive conduct in data markets, which can be relevant to Open Banking. In July 2014, the French Competition Authority imposed a fine on Cegedim for having abusively refused to sell its medical information database to certain pharmaceutical laboratories.

**Euris’ complaint**

Euris accused Cegedim, among other things, of abusing its dominant position by refusing to sell its database to laboratories that were using or intending to use it with Euris management software. For instance, Cegedim refused to sell its OneKey database – the benchmark for the sector – to laboratories that were using software marketed by Euris, although it had agreed to sell it to laboratories that were using other competing software.

**The medical databases market:**

To optimise the work of their sales forces, pharmaceutical laboratories use two tools, namely, databases containing medical information, mainly for collecting the names and address details of doctors and any information useful to medical sales representatives (addresses, conditions and visiting hours, etc.), and customer management software that makes it possible to use this information. Cegedim is leader in the medical database information market and enjoys a dominant position. It offers both databases and management software to laboratories, whereas Euris only produces customer management software.

**Competition effects:**

This abusively discriminatory treatment – caused Euris to lose any possibility of expansion in the management software market. The laboratories that used its software or that were interested in its software solution could not access the leading database in the market and consequently were deterred from working with Euris. This practice, which was instituted in October 2007, despite the fact that Cegedim was fully aware of the illegal nature thereof, had a seriously harmful effect on Euris, which lost


\(^{193}\) https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/8-july-2014-health-medical-information-databases
70% of its customers between 2008 and 2012, and restricted the laboratories in their choice of customer management software.

**Conclusion:**

The French Competition Authority found that Cegedim’s conduct lasted from April 2007 to April 2013. It also ordered Cegedim ceases to discriminate between its customers according to the software they are using.

-End-