Draft Position Paper on Open Finance

FSCA
Financial Sector Conduct Authority

JUNE 2023

Table of Contents

1. Executive Summary

Data may be a powerful enabler of innovation. As such, many countries are implementing an Open Finance regime to foster the benefits that Open Finance can bring, including enhanced value services for customers and increased competition, by encouraging consent-based sharing of customers' financial data with Third Party Providers (TPPs). Although there may be benefits to Open Finance, there are also challenges and risks to overcome. The Financial Sector Conduct Authority (FSCA) has a crucial role to play in ensuring appropriate risk mitigation by a financial institution or service provider that participates in the Open Finance ecosystem, to protect financial customers.

In 2020 the FSCA published an assessment of the Open Finance landscape, including an international review and survey of local industry participants, fostering engagement amongst stakeholders. Drawing on these learnings, the FSCA is aiming for an approach to Open Finance in South Africa that drives sustainable innovation, financial inclusion and competition, while at the same time protecting financial customers. Noting that the FSCA is just one role-player in the Open Finance regulatory ecosystem, a distinction is made between the steps to be taken as a conduct regulator to mitigate conduct and consumer protection risks brought about through data sharing, and national policy decisions relating to mandating Open Finance (or Open Banking). The views of the FSCA on the latter are intended to contribute towards the national policy debate, as coordinated through the Intergovernmental Fintech Working Group (IFWG)[1].

For the purposes of this paper, **Open Finance refers to the practice of consent-based financial data sharing and payment initiation[2], with suitably authorised third parties, safely and ethically.** There are various Open Finance use-cases that leverage consumer financial data to offer innovative and personalised financial services and products.

This draft Position Paper considers five such use-cases intended to illustrate Open Finance, including:

(1) account aggregation, (2) financial management, (3) payment initiation, (4) alternative lending and (5) insurance.

In determining the FSCA's approach to Open Finance, the draft Position Paper considers the following:

- The extent that Open Finance supports the achievement of the FSCA's objectives;
- the regulatory and institutional parameters currently in place to support Open Finance in the South African context;
- the extent that Open Finance will be compelling and sustainable for data holders;
- the availability of a market for the effective use of shared data by innovators; and
- the appetite for Open Finance by consumers and Small and Medium Enterprises (SMEs) and how to optimise their value derived.

Open Finance has the potential of meeting the strategic objectives of the FSCA by providing potential benefits such as:

- supporting financial inclusion and the financial resilience of customers by improving affordability and transparency of financial products and services (including by augmenting or supplementing traditional data sources) and creating products and services that make it easier for consumers and businesses to make improved financial choices; and
- promoting competition by enabling new market entrants to compete with current incumbents and use the available financial data to create personalised products.

1 IFWG comprise representatives from the National Treasury (NT), South African Reserve Bank (SARB), FSCA, National Credit Regulator (NCR), Financial Intelligence Centre (FIC), Competition Commission and South African Revenue Services (SARS).

2 Payment initiation occurs when a consumer instructs a third party to execute a payment via electronic funds transfer.

However, the draft Position Paper also illustrates potential risks emanating from Open Finance. These include risks related to: (1) privacy and protection of personal data, (2) misconduct, (3) operations and cybersecurity, and (4) fraud. Access to Open Finance platforms and technologies rely heavily on digital literacy, internet connectivity and access to reliable devices. These barriers may disproportionately affect marginialised communities, potentially widening the digital divide and leaving vulnerable groups behind. Moreover, Open Finance may have anti-competitive effects if certain providers are excluded from the data sharing regime. Lastly, increased interconnectivity amongst systems both inside and outside of the financial system may ultimately introduce systemic stability risks.

The FSCA acknowledges Data Portability[3] and Open Finance as potentially valuable financial innovations, proposing that these be accommodated within the conduct regulatory framework alongside proportionate regulatory safeguards. This is informed by the statutory mandate of the FSCA together with South Africa's existing data sharing/Open Finance landscape, taking into account current levels of adoption, acceptance and usage. It does however warrant close monitoring of the evolving sector to ensure that the potential benefits to customers sufficiently manifest.

Regulatory proposals in this draft Position Paper relate to: (1) regulatory approach to introducing an Open Finance framework in South Africa, (2) approach to regulatory oversight over participants in Open Finance, (3) informed consent from customers for the use of data, (4) implementation of appropriate risk management and disclosure frameworks, (5) data protection and data sharing standards, and (6) complaints and dispute resolution mechanism for customers that participate in Open Finance.

The FSCA favours an incremental approach to implementation of Open Finance, where prioritisation may focus on particular sectors or use-cases and be shaped by aspects like relative market size and maturity, stakeholder appetite and anticipated positive impact, especially for the poor.

Effective implementation of Open Finance will require proactive collaboration and coordination across the financial sector and amongst regulators to ensure effective oversight while limiting the regulatory burden on those that are regulated. As part of its collaboration effort, the FSCA is participating in the IFWG and Open Finance Integration Working Group (OPI WG). The FSCA Open Finance Position Paper is building on the OPI WG work in line with the FSCA mandate relating to market conduct.

3 To the extent that data portability applies to financial customers, it can be considered a version of Open Finance. Data portability refers to awarding an individual the legal right to obtain their own personal data from data holders, upon request, in a structured, commonly used, and machine-readable format, for their own purposes.

2. Problem Statement and Purpose

This draft Position Paper communicates the FSCA's proposed policy position on Open Finance and provides recommendations in respect of appropriate risk mitigation. Stakeholder feedback received on the policy approach outlined will, in due course, inform regulatory changes in line with these recommendations. This draft Position Paper focuses on financial institutions[4], TPPs[5], and financial customers.[6] It builds on the FSCA's 2020 "Research and Consultation Paper: Regulating Open Finance" (2020 Research Paper), taking into account stakeholder submissions.[7] [8] It should also be read alongside the NPSD's 2020 Consultation Paper on Open Banking activities in the national payment system (the NPSD 2020 Open Banking Consultation Paper)[9].

Customer data is critical to enable Open Finance. Indeed, customers are already sharing online login credentials with TPPs to access innovative financial services. This credential-sharing behaviour exposes customers to various risks, for example, data privacy breaches, breaches of contractual agreements, and fraud. Customers may have little to no control over how their credentials and data are shared, used or handled by third parties. Risks to customers are amplified by them not being fully aware of what practices are taking place. These risks are unpacked further in Section 6.2.

Most TPPs are currently not licensed as financial institutions and therefore lie outside of the FSCAs regulatory framework. For financial institutions already participating in the emerging Open Finance and data sharing ecosystem, there is no tailored regulatory framework, meaning that the risks deriving from data-sharing and data-use are not yet specifically addressed. The responding regulatory framework will have to balance enabling Open Finance and mitigating the associated risks.

3. Introduction

The FSCA has observed that while the use of customer data and technology in the financial sector is not new, computing power, data storage capacity, data sources, and financial data created per customer have increased exponentially over time. Data and technology are transforming the financial sector in South Africa and internationally. There is an ever-increasing trend for digital service providers in and out of the financial sector to aggregate, analyse and monetise data.

4 Financial institutions, for the purposes of this paper, means licensed financial sector institutions holding customer's data.
5 TPPs, for the purposes of this paper, means entities that have the consent of a financial customer to access that customer's data and to analyse and offer them innovative products and services safely and ethically.
6 Financial customers, for purposes of this paper means, "financial customer" as defined in the Financial Sector Regulation Act, 2017.
7 "Regulating Open Finance, FSCA Research and Consultation paper 2020," Available at: www.fsca.co.za/Documents/Regulating%20Open%20Finance%20Consultation%20and%20Research%20Paper.pdf
8 Note that the 2020 Research Paper included an international review and survey of the South African market, hereafter referred to as the 2020 Survey.
9 Available on the SARB website: www.resbank.co.za
10 A closed system in which all the operations are controlled by the system operator – see for example the Financial Times article: "Walled gardens versus open markets in payments," June 2020.

A financial ecosystem has developed where financial institutions collect large quantities of customers' financial data resulting in what can be termed "closed data silos". Access to these data silos is often forbidden to third parties, which creates private "walled gardens"[10]. The situation may be aggravated by potential misinterpretation of the protection of personal information legislation and associated penalties and the consequence of these closed data silos is information asymmetry with TPPs. This asymmetric access to customer information is not in the interest of the market nor the financial customer, as it can undermine competition, innovation and financial inclusion.

Since 2018, these closed data silos started to change with the introduction of Open Banking in Europe. **Open Banking can be defined as the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services**, including, for example, those that provide real-time payments, greater financial transparency options for account holders, marketing, and cross-selling opportunities[11]. The term **"Open Finance"** in this Position Paper is wider and refers to the practice of **consent-based financial data sharing and payment initiation[12], to licensed third parties, safely and ethically**.

The scope of this paper to consider Open Finance beyond Open Banking is risk driven – we are considering a proactive response to data sharing that may be already taking place across the sector, and is likely to grow as financial institutions and fintechs adapt their business models to the opportunities of "big data".

This sharing of customers' financial data to TPPs — under conditions of strong control practices — has the potential to enhance customer value, financial inclusion and competition. These benefits have motivated the introduction of Open Banking and exploring Open Finance in multiple countries, including the United Kingdom (UK), Singapore and Brazil.

BOX 1: Data sharing under Open Finance

Financial data shared may be primary and/or secondary data, before enrichment has been performed.

Primary data refers to first-hand gathered data, being a customer's personal registration or identification information at the financial institution, as collected during the initial customer onboarding process, for due diligence or know-your-customer (KYC) processes, including beneficial ownership data (where applicable).

Secondary data refers to data that is already available, such as customer information produced by financial institutions in relation to that customer's financial products. Examples are account statements, balances, movements, loan payment behaviour, investment portfolio changes, insurance claims, etc.

Enrichment, for the purposes of this paper, means data processed to achieve segmentation, scoring, and personalisation. It is excluded from the proposed Open Finance framework.

11 https://www.bis.org/bcbs/publ/d486.pdf
12 Payment initiation occurs when a consumer instructs a third party to execute a payment via electronic funds transfer from their bank account.

The FSCA, as part of the inter-agency OPI WG, is working closely with the National Treasury and other financial sector regulators to understand the Open Banking and Open Finance ecosystem in South Africa, and its role as conduct regulator. Effective implementation of an Open Finance regime will require collaboration and coordination across the financial sector and other regulators, to ensure effective oversight while limiting the regulatory burden on regulated persons.

In responding to the FSCA's 2020 Research Paper, stakeholders provided valuable inputs. A first public workshop in 2021 focused on consent, customer protection, and dispute resolution mechanisms. A second workshop later that year focused on data sharing standards, commercial models and data protection. Stakeholder submissions informed the recommendations in this draft Position Paper.

As the FSCA is just one of the regulatory role-players, a distinction is made between the steps that must be taken to mitigate existing conduct and consumer protection risks brought about through data sharing, for which the FSCA is responsible, and national policy decisions relating to mandating Open Banking or Open Finance, which may be a shared responsibility impacting multiple regulators. The FSCA's views on the latter, as presented in this paper, are exploratory, and intend to contribute towards the national policy debate. A final policy decision in this regard will be developed through the IFWG.

Engagement on the recommendations in this draft Position Paper will support finalisation of the FSCA approach.

4. Global Context

Open Finance complements other policy initiatives to drive improvements in the financial sector. It is still in the nascent stages and might not be ideal for every jurisdiction around the world. Policymakers and regulators have tended to take one of two approaches to Open Banking / Open Finance, namely, the voluntary or mandated approach.

The **voluntary approach** does not compel financial institutions to share customer data. Rather, data holders (often financial institutions) and TPPs enter into an Open Finance arrangement of their own volition, without being required - or mandated - to do so by law. In certain jurisdictions, financial institutions may offer fintech services themselves (explained more fully in Box 2). Others enter into Open Finance arrangements with TPPs, which arrangements are governed by contract and may be subject to data protection laws. In the United States (US), certain financial institutions are voluntarily participating in a range of data-sharing practices such as bilateral data-sharing contracts, wherein individual financial institutions open Application Programming Interfaces (APIs) for use by TPPs for collective data sharing. Here industry bodies may apply a code for their members, e.g. the Financial Data Exchange (FDX)[13] has aligned its member institutions by adopting a standard for Open Banking. The US seems to be an outlier in this regard. More commonly, jurisdictions that have adopted the voluntary approach maintain a strong role for the regulator, which imposes requirements for entities participating in the Open Finance ecosystem in support of fair competition and data and consumer protection. Examples of this approach are Singapore, Japan, Hong Kong, Columbia, and Nigeria.

Alternatively, under the **mandated approach**, regulators have compelled financial institutions and other data holders to participate in an Open Finance ecosystem. In these jurisdictions government mandates (requires) financial institutions to participate and abide by the rules of the Open Banking or Open Finance regime. Implemented through legislation, regulation or court rulings, the regime can be designed to mandate individual entities or specific categories of institutions (e.g., the banking, credit, or insurance sectors), or can apply broadly to a range of financial sector players. Examples of this approach are the UK, European Union, Brazil, Australia and Chile.

13 FDX is a non-profit organisation that is dedicated to unifying the financial industry around a common, interoperable, and royalty-free standard for the secure access of user permissioned financial data. FDX has an international membership that includes financial institutions, financial data aggregators, fintechs, payment networks, consumer groups, financial industry groups and utilities and other permissioned parties in the user permissioned financial data ecosystem.

BOX 2: Voluntary approach – Open Banking / Open Finance in Singapore, the US, and Nigeria

Singapore follows a voluntary approach to Open Finance with the **Monetary Authority of Singapore (MAS)** playing an active enabling role. The regime covers the banking, insurance, and payments industries and was initiated to provide a market environment that would reduce barriers to entry for fintech innovators. Licensed TPPs can access the data according to private agreements entered into with financial institutions.

APIs are standardised by MAS and the cost is borne by the regulator, TPPs and financial institutions, who pay fees to utilise the APIX sandbox set up for this purpose. MAS fulfils the role of implementing agency. It has created an API Playbook to set out the rules for participation, as well as a Finance Industry API Registry. The Personal Data Protection Commission is also an active participant, given the role of the Personal Data Protection Act in the enabling environment for Open Finance.

In **Nigeria**, the Central Bank of Nigeria published a regulatory framework for Open Banking in 2021. Banks are not mandated to participate in the Open Banking regime, but once they opt to participate they will need to comply with the data sharing and API standards being developed by Open Banking Nigeria. The regulatory framework provides a risk management maturity level and data services access levels that determine who can access certain types of data; industry participants will need to comply with different requirements depending on which type of data they want to access.

In the **US**, there are currently no regulatory standards around APIs and financial data sharing. However, in 2022 the US Consumer Financial Protection Bureau indicated it will be moving forward with an Open Banking rule to require financial institutions that offer transactional accounts to set up secure methods for data sharing, as well as requirements aiming to limit the misuse and abuse of financial data[14]. In the meantime, various private sector initiatives are driving the adoption of Open Banking and APIs, for example, the Clearing House Payments Company created a Model Agreement that banks and TPPs can use as a guide in developing API-related data-sharing agreements; the FDX has aligned its member institutions in adopting a standard Open Banking regime; the National Automated Clearing House Association (NACHA) and the Financial Services Information Sharing and Analysis Centre (FS-ISAC) have also developed APIs to enable the safe transfer of data between parties.

Other countries that have engaged the voluntary approach include Columbia, Hong Kong, and Japan.

Mandated approach - Open Banking / Open Finance in the UK, European Union and Brazil,

The **European Union** implemented a mandatory version of Open Banking in September 2019 with the aim to increase pan-European competition and level the playing field. It covers the whole banking and payments industry across the European Union. The regime was implemented under the auspices of the European Commission and the European Banking Authority, with the latter established as the implementation agency. It is established across three regulatory frameworks: Payment Services Directive 2 (PSD2), the Regulatory Technical Standards on Strong Customer Authentication (RTS-SCA), and the General Data Protection Regulation (GDPR). APIs are not standardised, and banks, as mandated financial institutions, bear the cost for the implementation of the regime in each country, as well as for creating their own APIs.

14 Reuters, US consumer agency to move ahead with "open banking" rule this week, 25 October 2022.

BOX 2 (Continued)

The **UK** launched Open Finance services in 2018. This followed the Competition and Markets Authority 2017 order, requiring the UK's nine largest banks to share their customer data with licensed TPPs. The banks were sanctioned for anticompetitive behaviour and were required to participate in the Open Banking regime as a penalty[15]. The Financial Conduct Authority (FCA) plays a lead role alongside the Competition and Markets Authority. After the banks were ordered to share their data they were consulted in the setting of the rules of the regime. An Open Banking Implementation Entity (OBIE) was set up in to create software standards and industry guidelines for Open Banking. The regime was modelled on the three core EU regulatory frameworks under development at the time: the PSD2 was transposed into the Payment Services Regulations 2017, the RTS-SCA became the UK Regulatory Technical Standards (UK-RTS), and the GDPR rendered into the Data Protection Act of 2018. APIs are also standardised by the OBIE.

Brazil implemented its version of Open Finance in 2021. The regulations require participation of the 12 most dominant banks in Brazil, which are part of financial conglomerates, as well as all authorised payment entities. Participation is voluntary for other financial institutions, like small(er) banks, cooperatives, fund managers, etc.), subject to reciprocity in data sharing for actors and provided they satisfy the technical requirements of API data transmission. They must also be registered in the participant directory. The Central Bank has the authority to make participation mandatory for other institutions.

Other countries that have embraced the mandatory approach include Australia and Chile.

5. How Open Finance can Empower Consumers

There are various Open Finance use-cases that leverage consumer financial data to offer innovative and personalised financial services and products. We consider five of these to reflect a spectrum of possible offerings[16]. Use cases 5.1 through 5.4 have tended to see traction internationally. The final use case 5.5 is seeing increased international interest and may be the next frontier. Implemented in the right way, these use cases align to the FSCA's mandate to protect and empower financial consumers and SMEs[17].

5.1. Account aggregation

TPPs aggregate financial data related to a single customer into a single location for that customer. The financial data can relate to transactional, credit, investment, mortgage and savings accounts (including retirement fund accounts). This serves as a critical enabler to Open Finance, to provide online visibility of a customer's financial data in a consolidated format for one or more accounts. It forms the basis for the use cases outlined in 5.2 to 5.5.

15 The Competition and Markets Authority investigated the supply of personal accounts (PCAs) and of banking services to SMEs, publishing findings and recommendations in 2016, including relating to Open Banking.

16 These use-cases are not exhaustive and should not be viewed as priority cases for the FSCA at this stage. Rather, they rather indicative of opportunities available to financial customers. Any move towards a mandated approach will require closer scrutiny of preferred use-cases for prioritisation.

17 The FSCA's 2020 Survey revealed "Account Information Service Providers" - use case 5.1 - as the leading benefit expected to arise from Open Finance. Respondents indicated that customers will most likely value "seeing all their financial relationships in a single view" to better inform their financial decisions through a holistic view. Other benefits were reflected in equal measure from "enhanced credit scoring" to "new payment methods". Many of the respondents suggested however, that it might be too soon to predict which use-cases will ultimately dominate, as it also depends on market forces.

South African experience: Innovative account aggregators are offering solutions (apps) which allow customers to view their money in one place by linking customers bank accounts, credit and store cards, investments, and loans, thereby enabling customers to get a better understanding of their expenses and the behaviours that might be sabotaging their efforts to budget and invest. The apps can integrate with different financial institutions.

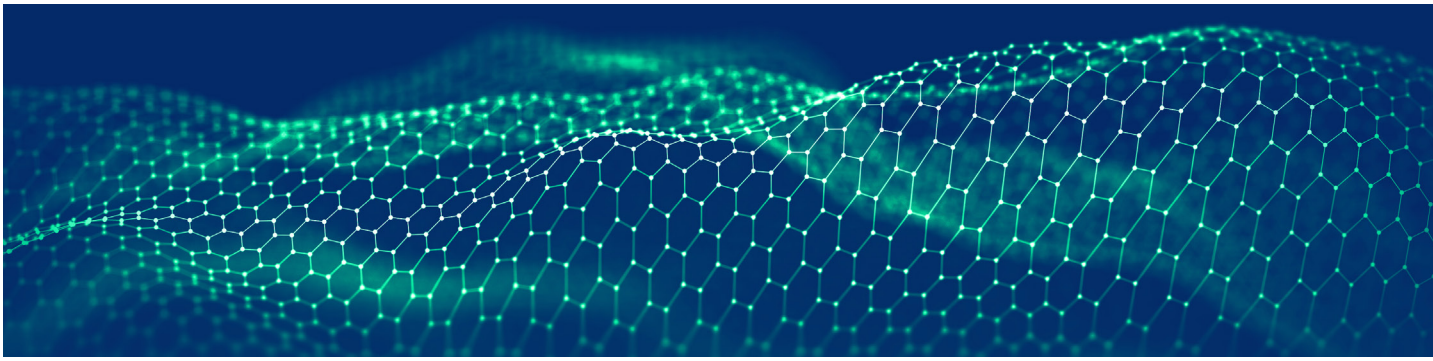
5.2. Financial management

This use-case deals with personal and business financial management tools using holistic management dashboards enabled by Open Finance. Open Finance, in respect of this use-case, also facilitates the automation of financial management by enabling applications to make financial-related decisions based on customer preferences and information. The process begins with a TPP aggregating the financial accounts into a single view, as referred to in the account aggregation use-case 5.1 and enriching the data to provide guidance and steer customers to better manage their finances. The aggregated financial data is presented to users in a user-friendly and easily understandable manner. This may include features like interactive dashboards, graphs, categorisation of expenses, spending analysis, budgeting tools and personalised insights. The guidance can take the form of intermediary services and advice, which is a regulated activity[18].

South African experience: *There is an emergence of solutions that are helping consumers to budget, track their spending on all their accounts, and invest for their life goals. In a single interface, consumers can link to different accounts to get a better understanding of their expenses and the behaviours that might be sabotaging their efforts to budget and invest. The solutions can also help customers to decide which investments to keep their money in and how much they need to save to reach their personal financial goals on time. This gives users the ability to track what they have, owe and what they can borrow.*

5.3. Payment initiation

In Open Finance payment initiation, authorised TPPs can initiate payments on behalf of the account holder with their explicit consent. This enables users to initiate payments directly from their accounts without relying solely on their bank's infrastructure. Authorised TPPs can access and initiate payments from a user's bank or other financial account. The payment process becomes frictionless and user-centric for the customer by automating the capturing of the seller's bank details, payment instructions, interbank transfer, and payment confirmation. Thus customers can schedule recurrent payments like subscriptions, set up payments or automatic transfers between accounts to avoid interest or overdraft fees, make payments to merchants' accounts at a lower cost than other electronic payments systems, and avoid having to enter their payment data every time they make an online purchase.



18 Advice and intermediary services are regulated activities in the Financial Advisory and Intermediary Services Act 37 of 2002.

These services allow merchants to increase their payment alternatives available to customers. Additionally, with the security of knowing that the electronic transfer has been initiated, merchants can trust that they will receive their payment, so they can deliver the goods or service without delay.

South African experience: *Innovative payments companies are offering online transactions and what other companies in South Africa call instant Electronic Funds Transfers (EFTs). An instant EFT is a payment method offered by a third party, in partnership with e-commerce stores, which automates the initiation of payments for consumers to e-commerce stores and provides immediate confirmation of payment to the e-commerce store to enable them to dispatch the goods or services purchased.*

Instant EFT payments use a method called 'screen scraping', which makes it possible for third parties to access bank account data and automate actions on behalf of a consumer using that consumer's online banking access credentials[19]. The access to the consumer's screen data is then used to facilitate payments. This provides a convenience for sellers and buyers not to wait for the funds to be reflected before goods or services can be delivered.

5.4. Alternative lending

This process involves the TPP securely connecting to one or more financial institutions to retrieve financial data. Once retrieved, the financial data is enriched by the TPP, for example by creating credit scores of the customers. This credit scoring is personalised and usable by lenders, brokers, and banks. The solution enables lenders to make more informed decisions on alternative data points, like irregular income received when working in the informal sector and how reliably the borrower makes their rent payments. This in turn supports growth in emerging lending markets like peer-to-peer lending, crowdfunding, merchant cash advances and digital wallet-based lending. Benefits include increased access to funding, streamlined application and approval processes, customised and flexible loan offerings and enhanced transparency and competition.

In South Africa: *Innovators are using online interfaces to securely connect to multiple financial institutions and to retrieve transactional data using APIs. The innovators then consolidate the financial data retrieved into a useable format for lenders to generate a personalised credit score. Affordability checks can be done efficiently which ultimately results in a quicker credit decision for customers.*

5.5. Insurance

From a financial customer perspective, Open Insurance can be defined as accessing and sharing consumers' insurance services data (e.g., their insurance policies data, such as an insured object, coverage, claims history, and Internet of Things data etc.) between insurers, intermediaries or TPPs to build applications and services[20].

19 Screen scraping is a technique in which a computer programme extracts data from human-readable output coming from another programme.

20 https://www.eiopa.europa.eu/document-library/consultation/open-insurance-accessing-and-sharing-insurance-related-data_en

The insurance use-case for Open Finance occurs when the TPP aggregates insurance services data into a single location to perform financial projections, risk assessments, and cash flow projections. These calculations are used to assist with identifying the appropriate insurance products and the appropriate duration of these products, based on the consumers' specific needs. For insurers, greater availability of data could lead to improved risk monitoring and assessment, a better customer experience and increased fraud detection. Increased access for insurers to data generated by both public and private sectors on a cross-sectoral basis could also provide the opportunity to increase innovation and competition in the insurance sector.

From a technical perspective, this use-case uses a combination of open API architectures that are embedded into insurance-based applications.

In South Africa: *At present there is relatively lower experience and understanding of Open Insurance in the South African context. More research is needed to understand this local market as it develops.*

6. Opportunities and Risks of Open Finance

6.1. Open Finance opportunities

Globally, the adoption of Open Finance, and in particular Open Banking, has been rapid and continues to grow. Country approaches may be informed by national policy emphasis on financial inclusion, financial innovation and competition.

Financial innovation can support financial inclusion

For the customer, Open Finance can offer innovative and personalised products and services by TPPs, as granular financial data is shared. This in turn leads to an in-depth consumer profile, with the limited use of [what can be more risky] screen scraping practices. This data can lead to products and services being offered that were not previously possible due to closed data silos. These personalised offerings can provide more efficient risk ratings and need analyses, lowering costs for providers and resulting in better price points. Moreover, customers can more effectively control their financial data by determining who can access it, with the right to be forgotten[21]. Better value for customers of more suitable and trusted products and services promotes financial inclusion. In their review of 12 Open Banking regimes, Consultative Group to Assist the Poor (CGAP) found that access to bank account data is not a primary driver of financial inclusion in terms of account openings. However, Open Banking can help increase the number of relevant services and improve the quality of those services for people who already have a bank account but are underserved[22]. CGAP also emphasises the role of Open Data in driving financial inclusion, meaning that non-financial entities like telcos and utility providers are similarly compelled to share their data; however, this lies outside of the jurisdiction of the FSCA and beyond the scope of this paper.

Where jurisdictions like Japan and Hong Kong are driving Open Banking for innovation, Brazil, Mexico, India and Indonesia are examples of countries prioritising financial inclusion in the design of their Open Banking / Open Finance systems[23].

21 Financial institutions are required to delete or destroy information at consumers requests.
22 Plaitakis and Staschen, 2020, "Open Banking: How to design for financial inclusion," CGAP Working Paper 10.
23 Plaitakis and Staschen, 2020, "Open Banking: How to design for financial inclusion," CGAP Working Paper 10; and Montoya and Celedon, 2021, "Guidelines for the Development of an Open Finance Framework in Chile, with a Focus on Competition and Financial Inclusion".

Competition can bring positive disruption

Fintechs often depend on financial institutions for their infrastructure, regulatory licenses and customer/ product data, thereby raising their barriers to entry and generating significant informational rent for the incumbents. Open Finance aims to level the information playing field, bringing new financial product and service providers and an enhanced range of products and services on offer. This is good for competition and customer value. New entrants may challenge incumbents to assess what it means to be customer-centric, motivating them to improve their customer offerings and in some instances rethink business models[24].

There are also benefits to incumbent financial institutions, which can leverage their client base to facilitate a platform-type business model, specialising in products and services that they have core competencies in and relinquishing other offerings to TPPs. This dynamic type of ecosystem can drive market development by expanding services and revenue lines.

The UK, European Union and Australia are examples of countries that have prioritised competition in the design of their Open Banking systems[25].

BOX 3 Open Finance/ Open Banking UK experience

Given the relative "newness" of Open Banking and Open Finance, beyond the hype there remains much to learn about its impact. As the Open Finance ecosystems evolve worldwide, the FSCA will continue to monitor and learn from tested successes and shortcomings.

The UK is an important case study as it was the first country to implement a mandated Open Banking system. In January 2023 7 million consumers and SMEs used Open Banking services, including 1.2 million new users[26]. Of these, SMEs range between 14% and 25%[27]. The OBIE's March 2023 Impact Report finds that:

- There were 159 fully regulated firms as of December 2022, which has been broadly flat since March of that year.
- The market is dominated by propositions addressing improved financial decision making, expanded payments choice and better borrowing.
- While the availability of services continues to expand, growth is increasingly coming from participants that are not regulated as TPPs, such as agents.
- Adoption continues to grow, with 10-11% of digitally enabled consumers now estimated to be active users, up from 7-8% in December 2021.
- This is surpassed by SME penetration of 16%
- The split between types of usage is 64% data, 30% payments, with 6% of customers using both.
- SME demand is dominated by data usage and cloud accounting propositions are driving growth.
- In the six months to March 2022 there were 21.1m Open Banking payments, compared with 6.1m in the same period of the previous year. Month on month growth is around 10%, with a total of 68m payments made for 2022 overall.

24 A recent Doctoral thesis of Open Banking for example argues that the current structure of banks business models may be unsustainable under consumer-led pressure for innovative and convenient, independent mobile based products, and therefore motivates for bank and FinTech collaboration - "The Benefits of Open Banking to Consumers, Banks and FinTech companies," by Danete Zandamela.

25 In terms of the 2019 Consumer Data Right legislation, the Australian approach anchors in giving more control to banking customers of their own data, in support of more choice and convenience – visit www.cdr.gov.au.

26 Data reported to Open Banking Limited, otherwise known as the Open Banking Implementation Entity (OBIE), which was established by the banks and building society mandated by law to implement Open Banking in the UK – www.openbanking.org.uk

27 See for example www.statista.com and OBIE reporting (including annual reports and impact reports).

An earlier 2019 study "Consumer Priorities for Open Banking"[28] showed that Open Banking has had an impact on financial inclusion in the UK, providing evidence that people "on the margins" (who do not have an account or only have a basic account) will probably pay lower commissions in an Open Banking system, with savings equivalent to 0.8% of their income. In the case of people who are "over-stretched" (who have one or more accounts and are heavily indebted), the study showed that Open Banking allows them to save the equivalent of 2.5% of their income.

A 2021 report however cautions that benefits cited may be over-stated, especially relating to consumers and competition[29].

The Joint Regulatory Oversight Committee (JROC)[30] - comprising His Majesty's Treasury, the FCA, the Payment System Regulator and the Competition and Markets Authority - has prioritised the following five themes to be progressed over two years[31]:

- levelling up availability and performance
- mitigating the risks of financial crime
- ensuring effective consumer protection if something goes wrong
- improving information flows to TPPs and end users
- promoting additional services, using non-sweeping variable recurring payments (VRP) as a pilot

The JROC also committed to establishing a new body to replace the OBIE and expand the existing Open Finance framework.

6.2. Open Finance risks

To date there have been no scandals relating to Open Finance abuse or customer losses, and Open Finance participants are generally focused on the advantages and gains rather than the potential risks. But there are sizable risks that must be considered[32].

28 Reynolds and Chidly, 2019, "Consumer priorities for Open Banking," available on www.openbanking.org.uk.
29 Reynolds and Chidley, with Jenkinson, 2021, "The Consumer and Small Business Blueprint for Open Banking."
30 The JROC was established in March 2022 to ensure that open banking supports innovation and drives greater competition, delivering benefits to consumers and businesses in the form of new and improved products and services, as well bringing benefits to the wider economy.
31 "Recommendations for the next phase of open banking in the UK", available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1150988/JROC_report_recommendations_and_actions_paper_April_2023.pdf
32 Various reports have unpacked expected and experienced risks, for example:
- "The Future Development of Open Banking in the UK," Final report for the Joint Regulatory Oversight Committee published in 2023.
- "Report on open banking and application programming interfaces," by Bank of International Settlements in 2021
- "The Consumer and Small Business Blueprint for Open Banking" by Reynolds and Chidly, with Jenkinson, in 2021
- Guidelines for the Development of an Open Finance framework in Chile, with a Focus on Competition and Financial Inclusion, by Montoya and Celedon for the Ministerio de Hacienda in 2021.
- "Call for Input: Open Finance," by the FCA in 2019.

Table 1: Open Finance risks, identified for each participant in the ecosystem

Participant	Risk	Description	Remedy
Customers	Financial exclusion	Open Finance may entrench financial exclusion for offline population segments or those who may still be deemed to be too high risk or cost based on the data analysis. Although digital financial solutions are growing, many customers still have low digital capabilities and may not take advantage of Open Finance opportunities.	An Open Finance regulatory framework should contemplate conditions and safeguards against potential exclusionary practices that may disadvantage certain customers or groups of customers. Efforts should monitor digital access by customers and consider whether this may be improved. Financial education is crucial to support sustainable take-up and usage.
	Privacy and Protection of personal data	Given the potential increase in the volume of data being shared in an Open Finance system, there will inevitably be an increase in the risk of a data leak or misuse of information, which can impede a customers' right to privacy.	It is imperative to have adequate standards of information protection and to incorporate safeguards to ensure the customer's explicit consent and full understanding of the scope of the authorisation given to third parties to access their information. South Africa's POPI Act is therefore a fundamental foundation (see section 7.3).

Participant	Risk	Description	Remedy
Customers	Financial Literacy and Awareness	Consumers and SMEs may not understand the risks involved when sharing their personal data, including the limited liability accepted by many TPPs.	Targeted financial education and enhanced disclosure should be considered.
	Customer Recourse	Given the complexity of the Open Finance ecosystem and the multiple role players, identifying which entity is responsible and which to complain to when something goes wrong is challenging.	The Open Finance regime should make it easier for customers to hold providers accountable, including by promoting complaints and dispute resolution mechanisms. A clear liability framework in the event of erroneous or fraudulent transactions may be considered.

Participant	Risk	Description	Remedy
TPPs	Market exclusion	The risk of anti-competitive practices can arise in relation to data access requirements for new entrants.	The Open Finance regulatory framework should be designed to be proportionate to observed risks, to minimise market exclusion through undue barriers to entry. Under a mandatory approach, consideration should be given to which entities are included into the shared system and when. This includes considering the interoperability and standardisation of APIs, that may impact access[33].
	Operational risk and cybersecurity	The interaction between providers sharing information via technology platforms or interfaces and the greater flow of data can increase operational and cybersecurity risks, that can in turn compromise information security and the security of the participants' systems. A high degree of interconnection or dependency on third-party technology providers can also lead to contagion risk.	Participants in the Open Finance system must prioritise cybersecurity and information security management. Financial stability effects should be identified and monitored.

33 Giya, Kagee and Thibane, 2021, "Regulating Data Markets through Open Banking: Lessons for South Africa," Paper presented at the 15th Annual Competition Law, Economics & Policy Conference.

Participant	Risk	Description	Remedy
TPPs	Fraud	Unethical employees of TPPs may use or sell customer data to unscrupulous parties.	TPPs should be brought under the regulatory net. TPPs should be subject to the same or similar consumer protection requirements as financial institutions, to the extent that providing financial products or financial services.
Financial Institutions	Reputational Risk	Potentially fraudulent/ rogue TPPs and unauthorised use of customer data can have a negative impact on trust in financial institutions and the financial system.	Underscores importance of suitable regulatory and risk management framework for TPPs; strong governance required by financial institutions in respect of any partnerships or outsourcing arrangements with TPPs.
	Limited oversight and monitoring of TPPs	Financial customers may engage TPPs directly, so that there is no contractual relationship between the financial institution and the TPP, even where the TPP has no regulatory authorisation.	TPPs should be brought under the regulatory net. TPPs may need to be subject to the same or similar consumer protection requirements as financial institutions, to the extent that providing financial products or financial services.

Participant	Risk	Description	Remedy
Financial Institutions	Disintermediation	TPPs may reduce the role of financial institutions as the main conduit for financial intermediation, potentially leading to a partial loss of customer relationships. Financial institutions may lose market share, revenue and ultimately profitability.	Financial sector regulators to ensure a level and fair regulatory playing field amongst market participants. Fair competition should be promoted and not be impeded; financial institutions will need to promote value to customers. Changes in the market structure should be monitored over time to minimise sector instability.
	Change in business model	Facilitation of Open Finance with various technologies has a cost associated with the development and a need for the technology to be interoperable with the various systems. This could increase costs for participating financial institutions[34].	An Open Finance approach should balance fair access to data with ensuring proportionate and fair costs to incumbent financial institutions.

7. Regulatory Considerations for Open Finance in South Africa

7.1. Assessing the extent to which Open Finance is suitable for the South African Financial Sector requires consideration of the following[35]:

7.1.1. Will Open Finance serve the FSCA's objectives?

7.1.2. Are the regulatory and institutional parameters in place to support Open Finance in South Africa — or can they be created?

7.1.3. Will Open Finance be compelling for data holders and can it be sustainably implemented?

34 There can be substantial costs in the implementation of Open Finance. The costs consist mainly of infrastructure costs in the form of the development and maintenance of the standardised APIs and the fees in respect of access/transmission of the data. Based on assessing cost models international, the FSCA proposes that should Open Finance be mandated, that financial institutions share consumers' financial data with TPP without charging a fee to the customer. Any transmission costs should be borne by the TPP. Transmission costs can take the form of connection or data costs. The volume and frequency of consumer free data requests may need to be limited to a daily maximum to limit the web portal pressure on financial institutions. Further technical work should be undertaken to determine whether a regulated fee structure or set maximum fees needs to be implemented. Consideration should also be given to whether value-added data sets can be sold to TPP on a commercial basis. In this instance, the data sharing technology, contractual obligations, and fees should likely be determined between the financial institution and the TPP.

35 Open finance: Prerequisites and considerations for fit-for-context implementation in Africa. Retrieved from: https://cenfri.org/wp-content/uploads/Open-Finance-Prerequisites-and-considerations-for-fit-for-context-implementation-in-Africa_April-2022.pdf

7.1.4. Is there a market for the effective use of shared data by innovators?

7.1.5. The appetite for Open Finance by consumers and SMEs and how to optimise their derived value.

7.2. Consistency of Open Finance benefits with FSCA objectives

The legislated responsibility of the FSCA is to enhance the efficiency and integrity of financial markets, promote fair customer treatment by financial institutions, provide financial education and promote financial literacy, and assist in maintaining financial stability[36]. The FSCA's strategic objectives and their associated outcomes are outlined below in Table 2:

Strategic Objectives	Intended Outcome
1. Improve industry practices to achieve fair outcomes	• Good conduct and Treating Customers Fairly (TCF) principles embedded consistently across the financial sector • Conduct risk mitigated
2. Act against misconduct to support confidence and integrity in the financial sector	• Trust in the financial sector maintained
3. Promote the development of an innovative, inclusive and sustainable financial system	• Transformation in the financial sector supported • Financial inclusion of low-income households and small business deepened • Greater competition and contestability in the financial system enabled • Sustainable finance and investment in the financial sector fostered
4. Empower households and small business to be financial resilient	• Financial customers able to make better and more informed financial decisions
5. Accelerate the transformation of the FSCA into a socially responsible, efficient and responsive organisation	• Operational excellence embedded across all functions of the FSCA • FSCA is recognised and trusted by financial institutions, financial customers, financial sector ombuds and other financial sector regulators in South Africa and internationally

Source: FSCA Regulatory Strategy document 2021-2025[37].

36 As set out in Section 57 of the Financial Sector Regulation Act, 2017 (Act 9 of 2017)
37 FSCA Regulatory Strategy 2021-2025. Available at: www.fsca.co.za/News%20Documents/FSCA%20Regulatory%20Strategy%202021-2025.pdf

The potential benefits of competition and more personalised service offerings suited for a wider range of financial customers aligns comprehensively with Strategic Objectives 1, 3 and 4. The opportunity for digital innovation to support the financial resilience of customers renders Open Finance an exciting opportunity for more effective financial inclusion. Over 80% of those living in South Africa already have a bank account, the next imperative is to drive monetary transactions increasingly through the financial system rather than cash[38].

In its recently published Statement on Sustainable Finance and Programme of Work[39], the FSCA identified disclosure and market development as two critical pillars of work. Open Finance has the potential to create products and services that make it easier for consumers and businesses to make more sustainable financial choices and help retail investors to understand the environmental impact of their investment portfolios through web and mobile applications[40 41].

But participants in Open Finance must also be compelled to operate fairly, responsibly and in the interests of customers. Consistent with Strategic Objective 1 and 4, Open Finance offerings will require a targeted regulatory and supervisory focus to suitably manage risks, so that the potential gains are realised. These include ensuring safeguards for financial customers' rights protection, privacy protection, and information security, as well as ensuring the maintenance of the stability and resilience of the financial system[42]. South Africa's regulatory system is already well developed. Discussed more fully in section 7.3 to follow, the Information Regulator has made good progress in developing privacy and information protection, while the FSCA – alongside the SARB, PA, NCR and FIC - continues to embed a regulatory and supervisory approach towards protecting financial customers and the integrity and safety of the financial system. This means that there is a well-established regulatory backbone for conduct and privacy to tailor for Open Finance.

Ultimately the responsible and sustainable acceptance of Open Finance will also require users being equipped with the knowledge and confidence to understand the product offerings and make informed decisions. Building awareness of the benefits and risks of Open Finance through financial education should therefore be prioritised. Effectiveness of financial education interventions will rely in turn on the quality of disclosure by market participants.

7.3. Regulatory and institutional parameters currently in place in South Africa

South Africa has strong and enabling personal data and privacy laws in place, however, innovation and market developments have prompted a discussion around possible gaps, especially around TPPs and APIs, because they lie outside of the regulatory perimeter . Furthermore, effective mechanisms and structures for coordination among relevant regulators, to create and implement the frameworks noted below, would need to be embedded.

38 NPSD Vision 2025 available: at https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/Vision%202025%20-%20Action%20Plan.pdf

39 Available at: www.fsca.co.za/Regulatory%20Frameworks/Temp/FSCA%20sustainable%20finance%20statement%20Final%20March%202023.pdf

40 https://www.openbankingexpo.com/features/what-role-is-open-banking-playing-in-sustainable-finance/

41 Sugi is the UK's first platform enabling investors to check their carbon impact and compare with industry benchmarks. The platform aims to help investors build greener investment portfolios, currently displays impact data for roughly 95% of the listed equity market, over 3500 exchange traded funds (ETFs) and certain actively managed funds. Sugi uses Open Finance technology through its partner Moneyhub to enable users to link their investment portfolio to the app and access their personalised impact data.

42 Guidelines for the Development of an Open Finance Framework in Chile, with a Focus on Competition and Financial Inclusion 2021. Available at: https://biblioteca.digital.gob.cl/bitstream/handle/123456789/3818/2021.12.06%20-%20Lineamientos%20Informe.pdf?sequence=1&isAllowed=y

Financial sector laws

The current financial sector legislation empowers the FSCA and PA to regulate and supervise all financial institutions in South Africa. The FSCA was established by the FSR Act on 1 April 2018, as a dedicated conduct authority replacing the Financial Services Board (FSB) and the FSR Act extends the jurisdiction of the FSCA to include oversight of financial products and services not previously overseen by the FSB. These include, amongst other things, banking, services related to credit, and the buying and selling of foreign exchange. It also dictates a shift in approach from a compliance-driven model to one that is proactive, pre-emptive, risk-based, and outcomes focused. Crucially, the FSR Act includes financial inclusion, competition and transformation of the financial sector in its overall objectives.

Although some of the current financial sector legislation already addresses certain themes that overlap with risks identified in the Open Finance environment such as risk management, data confidentiality, dispute resolution and disclosures, these requirements are not tailored to address Open Finance specific risks in the context of these themes. These laws will require reshaping to ensure that they consider identified Open Finance risks.

Looking to the future, the Conduct of Financial Institutions (CoFI) Bill, through consequential amendments to the FSR Act, proposes a new licensing schedule for all persons that are regulated by the FSCA and that will be licensed by the FSCA in the future. The CoFI Bill aims to significantly streamline the conduct requirements for financial institutions that are presently found in several different financial sector laws. The proposed CoFI Bill will not only replace conduct provisions in existing financial sector laws but will build a consistent, strong, and effective market conduct legislative framework for the financial sector. Going forward, an Open Finance regime would need to be accommodated under this framework.

Protection of personal information laws

There is a Constitutional right to privacy contained in Section 14 of the Bill of Rights of the Constitution of South Africa. This right to privacy means that everyone has the right to privacy, including the right not to have the privacy of their communications infringed.

The Protection of Personal Information Act, 2013 (Act 4 of 2013) (POPI Act) was signed into law in November 2013, with the remaining provisions of the Act fully enacted on 1 July 2021. The POPI Act makes the right to privacy contained in the Constitution enforceable from a personal information perspective, which responsibility falls within the legislative mandate of the Information Regulator[44].

44 The Information Regulator is, among others, empowered to monitor and enforce compliance by public and private bodies with the provisions of the Promotion of Access to Information Act, 2000 (Act 2 of 2000), and the POPI Act. The Information Regulator (South Africa) is an independent body established in terms of Section 39 of POPI Act. The POPI Act aims to :

- promote the protection of personal information processed by public and private bodies;
- introduce certain conditions so as to establish minimum requirements for the processing of personal information;
- provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000;
- provide for the issuing of codes of conduct;
- provide for the rights of persons regarding unsolicited electronic communications and automated decision making;
- regulate the flow of personal information across the borders of the Republic; and
- provide for matters connected therewith.

Both in terms of common law and in respect of the POPI Act, the duty owed to confidentiality is not absolute. In respect of common law, the courts in decisions such as GS George Consultants and Investments (Pty) Ltd v Datasys (Pty) Ltd 1988(3) SA 726(W) noted as a qualification of this duty, for instance, that where the disclosure is made with the express or implied consent of the customer, the disclosure does not clash with the duty of confidentiality.

The POPI Act contains strict privacy requirements in respect of the processing of personal information, which includes both the collection and retention of personal information. Personal information, in its essence, is any information relating to the identity of a person. The POPI Act grants data subjects[45] substantial rights, which include their rights to the right to access personal information, the right to withdraw consent where processing relies on it, and the right to erasure and to be forgotten. From a financial institution's perspective, there is a duty owed to the financial customer to protect the customer's information and in terms of common law an implied term in respect of confidentiality exists within the contract between the financial institution and the customer.

The POPI Act provides and recognises sharing of personal information through obtained consent, which must be a voluntary, specific, informed expression of a lawful justification for the processing of personal information. Open Finance requires the use of customer data, and this data can only be shared in line with the POPI Act, and the framework provided therein.

Cybersecurity laws

There is a cybersecurity framework currently in place in South Africa. The President of South Africa proclaimed the commencement date of certain sections of the Cybercrimes Act, 2020 (Act 19 of 2020) (Cybercrimes Act) to be effective from 1 December 2021[46]. The Cybercrimes Act is aimed at criminalising certain cyber-related activities and establishing jurisdiction for the South African courts and law-enforcement agencies over certain cybercrimes[47].

Further to the Cybercrimes Act, the FSCA and the PA published on 15 December 2021 a draft Joint Standard for Cybersecurity and Cyber Resilience Requirements (draft Cyber Joint Standard). The draft Cyber Joint Standard sets out the minimum standards for sound practices and processes of cybersecurity and cyber resilience for categories of specified financial institutions[48]. It seeks to ensure that these financial institutions implement processes and have tools and technology which will prepare them for cyber-attacks and respond to and recover from such attacks.

Because the financial sector is a prominent target for cyberattacks, financial institutions need to strengthen their ability to continue to carry out their activities, even when under attack or threat of attack, by anticipating and adapting to cyber threats and other relevant changes in the environment, and by withstanding, containing, and rapidly recovering from cyber incidents.

45 Data subject means the person to whom the data relates.

46 Cybercrimes Act 19 of 2020 available at: https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000

47 The Cybercrimes Act intends to, amongst other things:
- create offences that have a bearing on cybercrime;
- criminalise the disclosure of data messages which are harmful and to provide for interim protection orders;
- regulate jurisdiction in respect of cybercrimes;
- regulate the powers to investigate cybercrimes;
- regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes;
- impose obligations to report cybercrimes;
- provide for capacity building; and
- provide that the Executive may enter into agreements with foreign states to promote measures aimed at the detection, prevention, mitigation, and investigation of cybercrimes.

48 At a high level, the proposed Joint Standard seeks to:
- ensure that financial institutions establish sound and robust processes for managing cyber risks;
- promote the adoption of cybersecurity fundamental and hygiene practices to preserve confidentiality, integrity, and availability of data and information technology systems;
- ensure that financial institutions undertake systematic testing and assurance regarding the effectiveness of their security controls;
- ensure that financial institutions establish and maintain cyber resilience capability, to be adequately prepared to deal with cyber threats; and
- provide for notification of material cyber incidents by the regulated entities to the Authorities.

In the Open Finance environment, there is a high degree of interconnection or dependency on third-party technology providers which could lead to contagion risk, meaning that cyber risk management is critical. The draft Cyber Joint Standard should support robust cyber risk management practices across financial institutions, thereby promoting the safety of financial customer data. As such, the draft Cyber Joint Standard is important in the Open Finance context.

Coordination amongst regulators is a critical enabler

Effective implementation of an Open Finance regime will require proactive coordination between relevant authorities, specifically the FSCA and other financial sector regulators and the information regulator. For example, the SARB published its 2020 Open Banking Consultation Paper to develop an NPS policy position on Open Banking. In 2021 the Competition Commission made recommendations regarding data markets[49]. The FSCA will therefore continue to collaborate with the NPSD and other relevant regulators to ensure alignment on various Open Finance matters (use-cases, API standards etc.). Furthermore, the FSCA is participating in the IFWG OPI WG. The OPI WG outputs to date include internal notes or papers which aim to provide recommendations for members to consider as part of any regulatory framework for Open Finance in South Africa. The FSCA is building on the OPI WG work in line with the FSCA mandate relating to market conduct.

The South African government has also embraced a pro-innovation stance, working across agencies to develop harmonised approaches to fintech, and clarifying the regulatory stance on emerging technologies and products. The goal is to benefit the market and provide clarity, while effectively managing the risks. For example, the 4th Industrial Revolution South Africa partnership (4IRSA) — an alliance between partners from the public and private sectors, academia and civil society — launched in 2019, reaffirms a national push towards promoting the digital economy for growth. This reinforces the IFWG agenda.

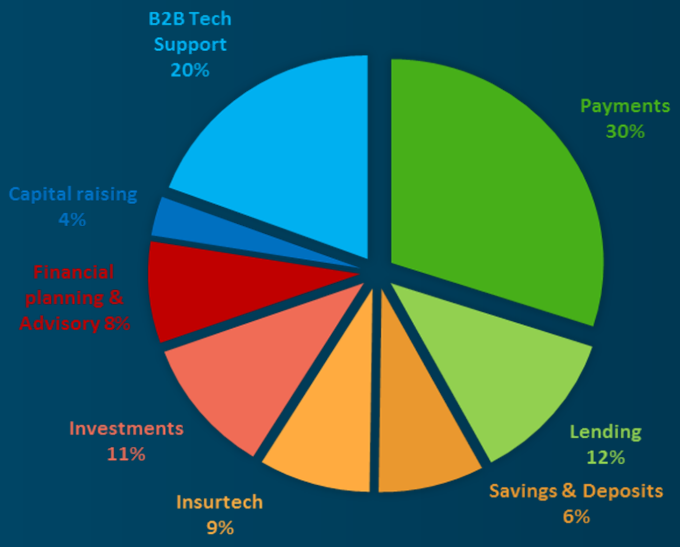
7.4. Current trends in shared data use in South Africa

The South African fintech market has grown significantly over recent years. The results from the South African fintech scoping exercise conducted by the World Bank in partnership with Genesis Analytics and IFWG in 2019, revealed that more than 200 fintechs[50] operate in South Africa[51]. This number is expected to grow through support from innovation hubs and the increasing adoption of technology in financial services.

49 Giya, Kagee and Thibane, 2021, "Regulating Data Markets through Open Banking: Lessons for South Africa," Paper presented at the 15th Annual Competition Law, Economics & Policy Conference.
50 Companies, established from 2008, using technology to offer financial products to South African's.
51 Fintech Scoping in South Africa 2020. available at: www.treasury.gov.za/comm_media/press/2020/WB081_Fintech%20Scoping%20in%20SA_20191127_final%20(002).pdf

BOX 4: Key insights from the South African fintech scoping exercise

Distribution of fintechs, by sub-industry segment in South Africa



SOURCE: Genesis Analytics, World Bank SA Fintech Report 2019

The largest and most mature segment is payments, making up 30% of overall fintech activity in South Africa. This is mostly due to large remittances volume, the need for migrant workers in the country to send money to their countries of origin in Southern and other parts of Sub-Saharan Africa. There are also several non-bank entities that have been operational for many years and that are registered to facilitate digital payments. Some of these businesses are offering innovative payment services and can be classified as fintechs.

The second largest segment is business to business technology support (Artificial Intelligence (AI), Blockchain and Robotic Process Automation (RPA)) making 20% of the sector, followed by lending segment at 12%. Lending fintechs in South Africa have shown significant potential with many new players entering the market, but the segment has only captured a small share of market to date.

Similarly, segments such as, savings and deposit, insurtech and financial planning and advisory and investments have shown great potential. The insurtech segment is characterised by numerous fintech entrants, however incumbents are responding to these entrants by digitising their processes in line with technological advancements in the sector.

The savings and deposit segment are small in comparison to traditional banks, but there has been reported activity in terms of new players entering the market.

Financial planning and advisory fintechs empower individuals and businesses by enabling direct access to financial advice using robotics and artificial intelligence.

Equity trading and investing is a largely exclusive sector in South Africa, traditionally serving middle- and upper-income consumers. However, fintechs are increasingly making these financial services accessible to the mass market.

Incumbents have felt the threat of fintechs and have realised the importance of re-evaluating their products offerings, customer journeys and internal processes. These companies are using technology, either developed inhouse or through partnerships or equity stakes in start-up businesses, to increase speed, improve efficiency, and make financial services more accessible.

The FSCA's 2020 Survey revealed an openness by most survey participants to the reality (or inevitability) of data-led innovation, enabled by an Open Finance framework[52]. Many of the market participants recognised the benefits that increased data-sharing can deliver, such as financial inclusion, increased competition and innovation.

The FSCA has observed fintechs in South Africa offering account aggregation, financial management, lending and payment solutions, while an increase in screen scraping activities, mainly being used by fintechs for payment initiation, has prompted the SARB NPSD's proposed policy interventions. Given that the sector is currently unregulated, the full extent of data sharing and Open Finance is not known; improved reporting on these activities will be important for financial sector regulators to monitor emerging risks[53].

Engaging the South African fintech ecosystem in 2021 revealed that fintechs will be inclined to enter the market if there is an enabling Open Finance framework (subject to meeting any applicable regulatory requirements). Consequently, Open Finance will likely be seen as a positive change for fintechs, as potential benefits are becoming understood. However, some fintechs may need capacity building on cybersecurity, data management and analytics, and API usage, to manage the envisaged risks.

7.5. Consumer and SME appetite for Open Finance in South Africa

Financial customers are more likely to participate in Open Finance markets if they see a suitable value proposition. They will also need access to the right technology, typically in the form of a smart device and data, and be confident to use it. The climate in South Africa appears positive for Open Finance but may face some challenges. While the number of mobile phone subscriptions exceeds the South African population by 1.7 times, data costs remain high[54] and only half of respondents in a 2022 PWC survey "Unlocking open banking in Africa" are either "currently using" or "will consider using" their smartphone at POS (40% said they are not interested in doing so)[55]. The majority of South Africans reflect a willingness to open transactional accounts with non-banks, with retailers being most preferred (27%) and Mobile Network Operators (MNOs) least preferred (13%), while 28% are altogether unwilling. The study also found that South Africa values mobile data privacy more than the other African markets surveyed (Kenya and Nigeria), with 40% of respondents preferring to not share their data at all; of those that trusted data sharing, most favoured banks (25%), with retailers a lagging second (10%).

52 "Regulating Open Finance, FSCA Research and Consultation paper 2020", Available at: www.fsca.co.za/Documents/Regulating%20Open%20Finance%20Consultation%20and%20Research%20Paper.pdf

53 In its 2020 Consultation Paper, the NPSD has already observed that: "Screen scraping presents safety and integrity challenges in the NPS."

54 See for example a report "Worldwide Mobile Data Pricing in 2022," which ranks South Africa at number 135 out of 233 countries, with 1GB of mobile data in the country costing an average of $2.20 (R37) - www.cable.co.uk.

55 See www.pwc.co.za/en/assets/pdf/payments-and-open-banking-survey-2022-unlocking-open-banking-in-africa.pdf

8. Regulatory Proposals

The FSCA's December 2020 Research Paper identified six recommendations for a successful Open Finance framework:

- Consent and authorisation
- Customer protection
- Dispute mechanism
- Data sharing standards
- Commercial models
- Data protection

Each of these topics is core and dependent on the others for an effective and protected Open Finance regime. These initial proposals are augmented with inputs received through consultations to give the final proposed approach.

Within an Open Finance environment, effective regulatory requirements and oversight are needed in respect of the various participants where the information of the financial customer is shared. Although there are many potential benefits from Open Finance, such a regime heightens, amongst others, data privacy and cyber security risks, and the need for clear disclosure alongside financial education and other consumer protection measures. The FSCA considers that the existing conduct frameworks are, to a large extent, sufficiently developed to begin to regulate activities within Open Finance, for instance in respect of advice and intermediary services, complaints and cyber security. These may be augmented over time with bespoke requirements, where the existing framework does not provide sufficiently tailored requirements or where the activity is novel to a large extent[56].

The FSCA is of the view that the implementation of a suitable Open Finance regime, and making customer data available to regulated participants, can create value for customers through digital personalised financial services products and services. The proposals below set out more detail regarding the FSCA's proposed approach.

8.1. Proposal 1 — Regulated Open Finance regime

Persons participating in Open Finance should be regulated for the safe and ethical sharing of user consent-based financial data to TPPs – further explained in Proposals 2 to 5. Considering the relatively low digital literacy in South-Africa compared to more developed regions, regulation is considered essential to driving positive customer outcomes and market trust.

56 It is envisaged that where there are unique requirements needed, as one may expect, for example, for risk management related to data sharing, these can be drafted and consulted on as a Conduct Standard or Joint Standard with the PA, as may be appropriate (and subject to how the prudential framework for Open Finance evolves).

Moreover, a mandatory regime may be more appropriate in jurisdictions where policies are geared toward promoting financial inclusion or increasing competition in the financial sector[57]. The FSCA is therefore also exploring the potential for relevant financial institutions to ultimately — and in a phased-in way — be mandated (required) to participate in the Open Finance regime, by developing the necessary infrastructure to share data with TPPs when the financial customer so requests and consents.

As reflected in Section 4, this approach is most common in jurisdictions currently implementing an Open Banking/Open Finance model, including the UK and European Union and Mexico. Some of the benefits of this approach versus a market-led approach are that it opens the market for competition and encourages financial institutions to develop API communication solutions. In this respect, a market-led approach has certain drawbacks, like longer negotiations to access the data, and the scope of that data may differ in each negotiation. In contrast, uniformity through legislative provisions facilitates competition as ease of entrance improves. A mandated regime does, however, come with complexity and costs, which should be carefully understood and considered in designing the Open Finance system, to mitigate the risk of undue market disruption. This will need careful consideration by South Africa's financial sector regulators, as the cross-cutting nature of the mandated approach potentially impacts market conduct, the safety and soundness of financial institutions and financial stability. Factors that will need to be considered in the design of a mandated Open Finance system include[58]:

- Which entities are required to share data, i.e. is data portability considered a right for all customers or are only large entities compelled to share?
- Who can access the data and for what purpose?
- What types of data are shared?
- Which sectors are covered e.g. banking only or also other financial institutions like insurance and asset managers?
- Who bears the cost of the regime, including for the data exchange and the set-up of the relevant infrastructure?

8.2. Proposal 2 — Tailored and proportionate regulatory oversight over participants in Open Finance

Regulatory requirements imposed should be proportionate to risks identified and foster positive competition and customer outcomes. Four types of participants are identified for regulatory oversight, being financial institutions, TPPs, fintechs and other service providers.

57 Montoya and Celedon (2021), "Guidelines for the Development of an Open Finance Framework in Chile, with a Focus on Competition and Financial Inclusion."

58 Plaitakis and Staschen, 2020, "Open Banking: How to design for financial inclusion," CGAP Working Paper 10, and "Report on Open Finance", 2022, by the Export Group on European financial data space set up by the European Commission.

Firstly, the regulated financial institution - like a licensed bank that receives a request from a TPP to share the customers' financial data based on consent - should be subject to data standards. Tailored conduct requirements for Open Finance can drive appropriate disclosures and education programmes to promote a basic level of digital literacy and understanding of the rights and responsibilities needed to provide informed consent.

Secondly, there are TPPs that provide financial services after obtaining the financial data of the customer, for example advisory or intermediary services. If this TPP provides financial services but is not subject to the same statutory requirements as licensed financial institutions, it may expose customers and other financial systems to risky behavior. To mitigate the risk, it is proposed that any entity that uses APIs to access customer accounts in order to provide financial services, must be licensed for such an activity and meet the regulatory requirements relevant to the specific use-case e.g. providing advice and intermediary services would require authorisation under Section 7(1) of the current FAIS Act (and the commensurate license activity under the future CoFI Bill framework)[59].

Thirdly, where the TPP — which may be a fintech company — wishes to provide the financial product itself to the financial customer and not only financial services, these TPPs will be subject to the same requirements as other traditional licensed financial institutions that are product providers. This includes taking deposits like a bank or performing underwriting and insurance activities like an insurer.

Lastly, there will be activities that the TPP performs that do not fall within the licence activity categories for either financial products or financial services, as outlined in the FSRA. For these activities, we are considering when and how to apply regulatory requirements. An example of this is where the TPP does not provide financial products or services itself but extracts financial data from different financial institutions and aggregates it for further processing by other TPPs to provide financial services to customers. A critical trigger will be the sharing of customer information by a financial institution to a TPP.

59 This is an area for further discussion between relevant regulatory agencies as it raises a number of questions, including:
- i The overall approach to licensing / authorisation / approval of 3rd parties and the role of the regulators vs data holders.
- ii Whether we need to think about a specific license / approval for this type of activity and a bespoke framework for 3rd parties (over above the financial sector laws if they provide a product or service).
- iii The alignment with the proposed screen scraping framework proposed by NPSD and the authorisation process for 3rd parties as contemplated in the NPSD proposals.
- iv Capacity of the regulatory agencies to perform any oversight role of 3rd parties.

Where the activities are being performed or offered on behalf of a licensed financial institution, it may be regulated in the same fashion as outsourcing activities.

Should bespoke laws be considered for Open Finance, these would be a collaborative effort amongst relevant regulators, and subject to further public consultation and engagement at that time.

8.3. Proposal 3 — Informed consent must be obtained from customers for the use of their (the customer's) data

An adequate data protection and consent framework is integral to a fair and trusted Open Finance regime. Comprehensive consent requirements provide a greater level of control for the financial customer; the FSCA believes that this increased control will assist in preventing unfair outcomes that may arise when using innovative technologies through the sharing of financial customer data.

In its simplest form, the TPP requests access to the financial data held by the financial institution. The financial institution redirects the request received to the customer to obtain consent before the financial data is shared with the TPP. The request for consent should clearly convey the information through the user interface in a customer-centric manner, allowing for informed consent. Prior to obtaining consent, the financial institution must ensure authorisation by confirming the identity of the person providing consent. Overly complex consent process are a challenge, due to the inherently complex nature of financial products and services, in many instances aggravated by financial institutions combining a comprehensive amount of information in the consent form to mitigate regulatory and legal risk.

The FSCA proposes the following principles to promote obtaining and maintaining consent:

(a) TPPs are responsible for obtaining, maintaining, and revoking consent when collecting and using customer financial data; until regulated directly, the activities performed by these entities may be the responsibility of the contracting financial institution.

(b) Consenting to a TPP to collect and use customer financial data should not be conditional on obtaining other bundled products and services not related to the initial purpose.

(c) Consent should be unbundled and not aggregated with other consent agreements or permissions.

(d) Customers should freely and voluntarily give and withdraw consent.

(e) Consent should be informed and specific to the purpose.

(f) Consent should not be indefinite and should be easy to withdraw by the customer.

(g) TPPs should not utilise consumers' financial data once consent is withdrawn. Consent could be withdrawn for access to new data only, enabling the TPP to utilise existing data.

(h) TPPs should test consumer comprehension of the consent.

(i) The consent message should clearly identify the risks to consumers.

(j) Consumers should be informed of how their specific financial data will be used and for how long.

Since personal information in the POPI Act includes information relating to the financial history of the person, consent in respect of account information is governed under this Act; therefore, many of the principles alluded to above would not require a bespoke regulatory framework but will be governed by existing protection provided under the POPI Act and only the gaps would be provided for in a regulatory instrument by the FSCA, where there is a need to strengthen the consent requirements to protect the financial customer.

The POPI Act provides for the following requirements in respect of consent:

- Section 11.1(a) — the data subject or a competent person where the data subject is a child consent to the processing;

- Section 11.1(b) — processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;

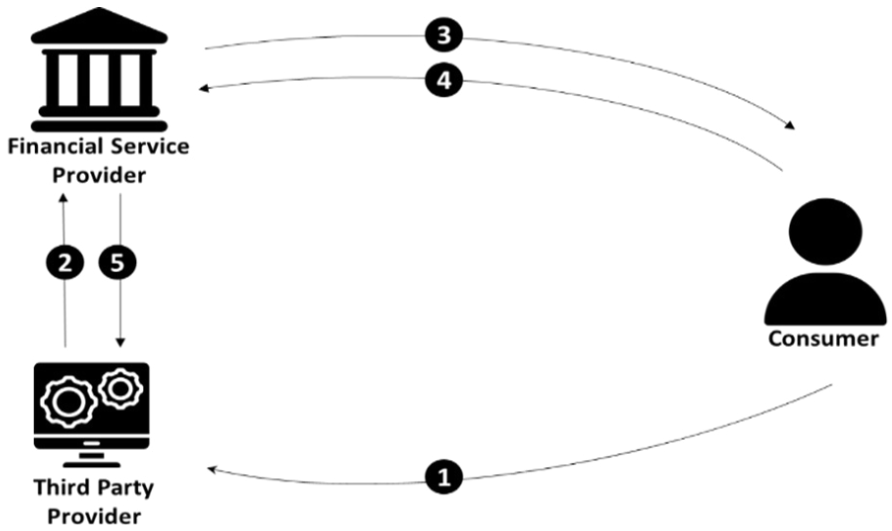
- Section 11.1(f) — processing is necessary for pursuing the legitimate interest of the responsible party or of a third party to whom the information is supplied; and

- Section 11.2(b) — the data subject or competent person may withdraw his, her or its consent, as referred to in subsection (1)(a), at any time, provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1) (b) to (f) will not be affected.

Therefore items (a), (b), (c), and (f) above can be considered in the bespoke future framework in respect of Open Finance.

TPPs should only seek access to the minimum data necessary for consumers' specific purposes they have consented to. For Open Finance to realise its potential benefits, all stakeholders, including the regulators, need to continuously inform consumers about Open Finance. Consumers need to understand what actions are taking place as well as the benefits and risks associated with Open Finance. There is a balance that is needed to inform consumers without making the message overcomplex and still ensure a positive user experience.

Diagram 1: Process flow



1. The consumer consents to the TPP obtaining their financial data.
2. The TPP seeks to access the consumer's financial data.
3. The financial institution authenticates the identity and scope of the consent of the consumer and requested authorisation to share their financial data.
4. The consumer authorises the financial institution to disclose their data to the TPP.
5. The consumer's financial data is shared between the financial institution and the third party.

Mindful of the roles of multiple regulators, notably the PA, the SARB, the NCR and the Information Regulator, further engagement will be required on the FSCA's proposed regulatory approach to consent. This is to ensure regulatory and supervisory alignment.

8.4. Proposal 4 — Protecting customers by implementing appropriate risk management and disclosure frameworks

Open Finance, by its very nature, aims to leverage customer financial data to provide personalised financial products. In this ecosystem, the risk of data exposure to fraudsters increases. Fraud and scams are essentially unwanted and unexpected data breaches. The FSCA maintains that this leveraging of customer financial data must be done in an ethical and responsible manner to limit the exposure to fraudulent use of data. While the changing needs of financial customers for personalised and innovative products drive the need for an Open Finance regime, the FSCA supports risk frameworks that aid this innovation but retains sufficient risk management principles to mitigate the risks.

To protect financial customers, a clear risk management framework is needed to address data breaches, errors, and the consequences thereof to all stakeholders.

The FSCA proposes that the following principles be included in a risk management framework:

(a) Financial institutions and TPPs must possess security, data protection, and business continuity policies, procedures, and controls that are consistent with those already in place in the financial sector. Security must be ensured in all parts of the data transfer process.

(b) Role-players in the ecosystem must hold adequate resources, whether in the form of operational risk capital or liability insurance as a last resort to deal with customer damages resulting from data breaches, errors, and consequences. This includes when data is in flight, transported, and when it lands.

(c) Careful consideration will need to be given to breaches by the financial institution as data holder or the TPP, to ensure appropriate accountability, especially where there are customer losses suffered.

(d) Reputational risk should be included in a risk management framework even when the financial institution is not at fault.

(e) Consumer access to data held by financial institutions via TPP is a loss of service, which could be the fault of the financial institution's TPP.

To mitigate the risk emanating from a vulnerable customer not fully understanding the risks involved when sharing their personal data, the FSCA proposes a disclosure framework that takes consumer and SME digital literacy levels into account and is appropriate for the target market at hand. These disclosure requirements should promote customers being better informed about their rights and responsibilities, and should be supported by targeted financial education interventions.

Typical disclosure requirements that may be considered are those contained within the CoFI Bill (Chapter 6) including:

- Meeting the reasonable information needs and requirements of financial customers to whom they are targeted;

- ensuring that disclosures in respect of financial products and financial services take into account the reasonably assumed level of knowledge, understanding and experience of financial customers to whom they targeted;

- that the advertisement and disclosures targeted or provided to financial customers must-

    ◊ assist financial customers to make effective, timely and properly informed decisions and choices about financial products and services;

    ◊ promote understanding of the financial product or service concerned;

    ◊ not create unrealistic expectations regarding what a financial product or service can deliver;

    ◊ provide a balanced message regarding returns, features, benefits and risks of a financial product or service; and

    ◊ be in plain language.

A specific consumer risk in relation to disclosure that emanates from an Open Finance regime is that the customer may not know that they are triggering a data API call that involves costs and is part of the end-customer pricing. It is therefore proposed that this gap is addressed by a specific requirement that ensures transparency.

As with proposed requirements relating to consent, the FSCA will engage its fellow regulators on proposals relating to risk management and disclosure to ensure regulatory and supervisory alignment.

8.5. Proposal 5 — Data protection and data sharing standards

The data of the financial customer shared through consent with third parties are primary and secondary data before enrichment has been performed. The data in respect of an Open Finance regime covers three types of data: generic services data, customer data and transactional data. The FSCA views the setting of data sharing standards as important to prevent fragmented specifications and practices within the Open Finance regime.

Data that have been enriched are excluded from Open Finance, unless the customer has paid for the enrichment of the data set. In the event of the customer paying for the enrichment, the enriched data should be shared where appropriate consent has been given. These value-added data sets are discussed further under standards for cost sharing.

With the absence of widespread API, screen scraping can add additional pressure on existing financial institutions' web portals. This strain might increase in time, resulting in a compulsion to add APIs.

When APIs are widespread there will be little room for screen scraping, but screen scraping might still be used as a fallback position when APIs are not functioning. API is the recommended technology to share data for Open Finance and it is proposed that the APIs are open and standardised, and where appropriate global open API standards exist, these should be considered. As the functionality will be common within the Open Finance ecosystem, the standardisation of APIs will reduce duplication of functionality and technical costs by promoting reuse, leading to greater consumer usage.

Global open API standards can, in turn, ensure that the South African market retains domestic governance controls while benefiting from proven security and interoperability standards that lower costs for local participants.

It is recommended that the industry, comprising of TPP and financial institutions, through a formal committee, develop or select the technical standards for open APIs, and those selections are approved by an oversight committee whereunder the technical committee sits, which oversight committee will be made up of the FSCA and other regulators. These technical standards, once finalised, may be embedded through the envisaged future Conduct Standard in respect of Open Finance.

It is proposed that there are nine guiding recommendations for the API design:

(a) Openness — ensure that licensed parties are able to access the API.

(b) Usability — ensure high-quality user experience for TPP and consumers.

(c) Interoperability — enable the exchange of data across stakeholders and that it can still be reused; leverage existing standards and taxonomies to avoid duplication of efforts.

(d) Independence — avoid dependency on any vendors or technologies to provide options in delivery models and implementation technologies.

(e) Stability — ensure consistency and transparency of changes.

(f) Transparency — provide clarity on environments and documentation.

Protecting the confidentiality and security of customer financial data for Open Finance is critical for promoting trust and confidence. In an Open Finance regime, there is an increase in the risk of a data leak, or undue use of the information, which can increase security risks and affect customers' privacy because of the increased use of customer data. A robust framework to mitigate these risks is required.

In respect of data protection, it is proposed that the requirements relating to cyber security in the draft Cyber Joint Standard apply to the development of the API and the use of the customer's financial data by TPPs.

These requirements in the draft Cyber Joint Standard include, amongst others:

- Clearly defined roles and responsibilities for exercising oversight in respect of cybersecurity risks;
- that cyber risk management is incorporated into the governance and risk management structures;
- establishment and maintenance of a cybersecurity strategy that is approved by the governing body;
- cyber security hygiene practices; and
- implementation of appropriate and effective cyber resilience capabilities and cybersecurity practices to prevent, limit, or contain the impact of a potential cyber event.

Customer consent alone is not sufficient to protect that person's data. The use and collection of personal financial data should be limited to the intended purposes and handled in line with customer expectations.

The following proposals are intended to manage data to protect customers:

(a) Customer financial data no longer necessary should not be retained in an identifiable form;

(b) the data should only be used for its intended purposes, within the scope of the consent given and in line with customers' expectations;

(c) uninformed consent should not override customers' expectations and intended purposes; and

(d) strong customer authentication should be in place to protect customer financial data.

TPP and financial institutions are to have information security and cyber security policies and guidelines in place. In addition to having policies and guidelines in place, TPP and financial institutions are proposed to establish and maintain effective security controls.

The FSCA will engage its fellow regulators on proposals relating to data protecting and data sharing to ensure regulatory and supervisory alignment.

8.6. Proposal 6 — Complaints and dispute resolution mechanisms for customers that participate in the Open Finance ecosystem

Providing a statutory complaints framework aims at mitigating risks of harm to consumers emanating from unfair treatment or misconduct by providers, as well as from fraudulent and/or erroneous transactions. Financial institutions have existing requirements in respect of complaints frameworks as provided by the relevant financial sector laws. The FSCA, therefore, believes that the existing legislation is to a large extent developed enough to provide for an Open Finance regime. Depending on the use-case, the existing framework would apply, for example a licensed Financial Services Provider applies the requirements in the General Code of Conduct for authorised Financial Services Providers and their representatives under the FAIS Act.

In future, the National Treasury's proposed CoFI Bill contains ongoing obligations in respect of financial customers, including:

- A financial institution that provides financial products or services to customers may not impose unreasonable barriers on those customers that prevent them from submitting a complaint;

- a financial institution must ensure its customers have access to and are provided with efficient and effective complaints management processes, including external dispute resolution mechanisms, that consider complaints in a fair and expeditious manner; and

- the financial institution has systems in place to monitor complaints, and processes that enable the financial institution to pro-actively identify and manage conduct risks, effect improved financial customer outcomes and prevent recurrences of poor outcomes and errors.

The FSCA is currently developing a harmonised complaints framework under the CoFI Bill that will apply to all financial institutions and in respect of all licensed activities. The harmonised framework will incorporate the matters highlighted in this recommendation.

If the complaint cannot be resolved by the financial institution, the relevant Ombud scheme will apply (as per the use case and therefore the relevant license activity). Where a dedicated voluntary Ombud scheme does not exist in respect of the specific use-case, the statutory Ombud (FAIS Ombud) will be the appropriate avenue for external complaints resolution, until the National Treasury reforms are fully implemented.

9. Conclusion

Open Finance has the potential to positively benefit financial institutions, TPPs and consumers. The principles of Open Finance are in line with the FSCA's objective to promote the development of an innovative, inclusive and sustainable financial system. This draft Position Paper confirms the intended direction of the FSCA regarding the future regulation of Open Finance from a conduct and consumer protection perspective.

Considering the material role of data protection in an Open Finance regime, it will be fundamental to have the support of the Information Regulator, as this core element falls outside of the mandate of the FSCA. The FSCA also recognises the importance of a collaborative approach amongst the financial sector regulators — being the FSCA, PA and SARB — to ensure that the risks identified in relation to Open Finance are appropriately mitigated through a congruent regulatory and supervisory framework.

Many of the requirements needed to mitigate the risks in respect of Open Finance are provided for in the existing and planned future regulatory frameworks. Where gaps have been indicated, the future framework will need to be adapted to provide for such.

The FSCA intends to take actions to mitigate the risk brought into the financial system by those entities already involved in Open Finance and data sharing activities, but the final decision regarding the Open Finance mandatory approach in South Africa will be a collective decision by financial regulators led by the IFWG.

Future work by the FSCA may include research to better understand:

- Customer take-up of Open Banking offerings in South Africa; and
- The role of "data portability" in the financial sector to promote financial inclusion.

10. Invitation for Comments

All stakeholders are hereby invited to provide written comments on the policy proposals contained in Section 8 in this draft Position Paper by submitting their comments to fintech@fsca.co.za by 15 August 2023. Comments received will be considered and deliberated on and a final Position Paper published, in collaboration with the IFWG.

Annexure A: Main Themes from Public Consultation on 2020 Research Paper

General sentiments emerging from stakeholders through public consultation included:

- Fintechs will naturally enter the market if there is an Open Finance regime (subject to meeting any applicable regulatory requirements). Consequently, an Open Finance regime is expected to be seen as a positive change for fintechs, noting however that some fintechs may need capacity building on cybersecurity, data management, analytics and API usage, to manage the envisaged risks.
- An appetite amongst financial institutions holding data to participate in an Open Finance regime. For some data holders, participation will also depend on how well the use-cases and business opportunities are illustrated, however, some smaller organisations are currently unlikely to have the capacity to implement Open Finance and may struggle to maintain sufficient cyber security measures .

FSCA responses to specific comments by stakeholders follow below:

Theme	Comment	Response
General	Consideration must be given to other laws in addition to financial sector legislation.	Agreed, Open Finance is currently being considered within the broader ambit of legislation, which includes law related to the protection of personal information and cyber crime.
General	TPPs must be licensed.	It is proposed that TPPs meet a minimum set of criteria to be determined by the FSCA, subject to the nature of their participation in the Open Finance regime.
General	Other industry-led modernisation programmes will be more effective. Open Finance will not lead to financial inclusion.	Open Finance and other modernisation approaches are not mutually exclusive. Research findings suggest Open Finance may be one enabler of financial inclusion, provided it is implemented in a way that mitigates risks of consumer harm and digital exclusion.
General	Should we perhaps start with Open Banking, then Open Finance; staggered approach?	A gradual implementation approach is preferred, especially should South Africa mandate the sharing of data. Industry engagement will be critical in this regard. Consideration is being given to phasing in regulatory requirements intended to address risks of data sharing, already being observed, as proposed in this Section 8.

Theme	Comment	Response
General	What is the "Customer Financial Data" that is being referring to? What about processed financial data?	Customer Financial Data includes both primary and secondary data, as defined in Section 3.
Data sharing	Will there be industry participation in the oversight committee establishing standards?	Yes, it is proposed that industry participates in the establishment of the data sharing committee. See Proposal 5 — Data protection and data sharing standards
Data sharing	Will there be contractual requirements between financial institutions and TPPs within Open Finance?	FSCA is proposing regulations and oversight of Open Finance participants to protect financial customers. See Proposal 2 - Tailored and proportionate regulatory oversight over participants in Open Finance. Regulatory requirements will give guidance regarding contractual arrangements necessary to mitigate risks and protect consumers.
Data sharing	What is a value-added data set?	This refers to data sets in which data has been enriched, as defined in Section 3.
Consent	Is the consent use-case specific?	Consent should be informed and specific to the purpose for which it is being requested, meaning that the TPP should only seek access to the data necessary to provide the specific and agreed service being offered. Consenting to a TPP to collect and use customer financial data should not be conditional on obtaining other bundled products and services not related to the initial purpose.
Consent	Will the customer have to be informed how their data is used within a financial group?	Yes. The FSCA is proposing comprehensive consent requirements which gives customers' greater level of control over their data. See proposal 3 section 8.3
Dispute mechanisms	A dedicated Ombudsman specialising in Open Finance should be considered.	Agreed that financial customers should have access to an ombudsman; the model will be informed by the National Treasury-led ombud system reforms.
Dispute mechanisms	Current complaint mechanisms should be used.	Licensed entities will ultimately be subject to the cross-sector complaints management framework that is under development.

Acronyms and Abbreviation

AI: Artificial Intelligence
API: Application Programming Interface
CGAP: Consultative Group to Assist the Poor
CoFI Bill: Conduct of Financial Institutions Bill
GDPR: General Data Protection Regulation
EFT: Electronic Funds Transfer
EU: European Union
FAIS Act: Financial Advisory and Intermediary Services Act
FCA: Financial Conduct Authority
FDX: Financial Data Exchange
FIC: Financial Intelligence Centre
FSCA: Financial Sector Conduct Authority
FS-ISAC: Financial Services Information Sharing and Analysis Centre
FSR Act: Financial Sector Regulation Act
IFWG: Intergovernmental Fintech Working Group
KYC: Know-Your-Customer
MAS: Monetary Authority of Singapore
MNO: Mobile Network Operator
NACHA: National Automated Clearing House Association
NCR: National Credit Regulator
NPSD: National Payment System Department
OBIE: Open Banking Implementation Entity
OPI-WG: Open Finance Integration Working Group
PA: Prudential Authority
POPI Act: Protection of Personal Information Act
PSD: Payment Services Directive
PWC: PricewaterhouseCoopers
RPA: Robotic Process Automation
RTS-SCA: Regulatory Technical Standards on Strong Customer Authentication
SME: Small and Medium Enterprises
TCF: Treating Customers Fairly
TPP: Third Party Providers
UK-RTS: United Kingdom Regulatory Technical Standards
US: United States

Glossary

Account Information Service Providers: provides account information services as an online service to provide consolidated information on one or more payment accounts held by a payment service user with one or more payment service provider(s).

APIX Sandbox: an online global marketplace and sandbox for collaboration between financial Institutions and fintechs. APIX facilitates a collaborative environment for financial institutions and fintechs to exchange ideas in a community-led environment, co-design new financial products and services within a cloud-based and secure sandbox.

Application Programming Interfaces: a set of rules and specifications followed by software programmes to communicate with each other, and an interface between different software programmes that facilitates their interaction; APIs enable direct database to-database data transmission enabling granular, real-time reporting and automated validation.

Artificial Intelligence: the theory and development of computer systems able to perform tasks that traditionally have required human intelligence.

Blockchain: is a shared, unchangeable ledger that facilitates the process of recording transactions and tracking assets in a business network.

Conduct of Financial Institutions (CoFI) Bill: aims to significantly streamline the legal landscape for conduct regulation in the financial sector, and to give legislative effect to the market conduct policy approach. It will strengthen customer protection by putting in place a single comprehensive market conduct law in the financial sector, resulting in the consistent application of consumer protection principles across the sector.

Cyber Security: the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

General Data Protection Regulation: It is a European Union law that came into effect on 25 May 2018. General Data Protection Regulation governs the way in which people can use, process, and store personal data (information about an identifiable, living person).

Insurtech: technological innovations that are created and implemented to improve the efficiency of the insurance industry. Insurtech powers the creation, distribution, and administration of the insurance business.

Open Banking: sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services, such as those that provide real-time payments, greater financial transparency options for account holders, and marketing and cross-selling opportunities.

Glossary

Open Data: information or content made freely available to use and redistribute, subject only to the requirement to attribute it to the source. The term may also be used more casually to describe any data that is shared outside the organisation and beyond its original intended use..." It includes data sharing by non-financial institutions.

Payment Services Directive 2: European regulation for electronic payment services. It seeks to make payments more secure in Europe, boost innovation and help banking services adapt to new technologies. PSD2 is evidence of the increasing importance Application Program Interfaces are acquiring in different financial sectors.

Platform-type business model: technology-enabled business model that creates value by facilitating exchanges between producers and consumers.

Robotic Process Automation: partial or full automation of manual, rule-based and repetitive human activities by robotics software or bots.

Screen Scraping: practice which makes it possible for third parties to access bank account data and automate actions on behalf of a consumer using that consumer's online banking access credentials.

Financial Sector Conduct Authority

Riverwalk Office Park, Block B, 41 Matroosberg Road, Ashlea Gardens, Pretoria, 0002

012 428 8000

www.fsca.co.za