Open Finance and Open Banking in sub-Saharan Africa

Foreword

Open Banking and Open Finance involve the sharing of data via standardised and secure interfaces at the request of clients. Such data sharing arrangements in finance are increasingly emerging in Sub-Saharan African (SSA) countries. This report examines common themes of such frameworks in terms of design characteristics, drawing on the experience of OECD countries; explains objectives and potential benefits of such frameworks in the context of the SSA region; analyses potential benefits and risks of such arrangements; and suggests pillars for the successful implementation of such frameworks in finance.

The report serves as background to inform the Digital Finance in Africa policy workshop of the 20-21st of June 2024. The policy workshop is a joint initiative of the OECD and the Mauritius Regional Centre of Excellence within the Financial Services Commission, and this report was produced with the financial support of the Financial Services Commission and the Bank of Mauritius. It was drafted by Aliza Amin with guidance from Iota Nassr, under the supervision of Fatos Koc, Head of Financial Markets Unit and Serdar Çelik, Head of the Capital Markets and Financial Institutions Division of the OECD's Directorate for Financial and Enterprise Affairs. It benefited from inputs from Matthew Soursourian, Seohyun Kim and Aleksandra Dymacz. Eva Abbott and Greta Gabbarini provided editorial and communication support.

Table of contents

FIGURES

Abbreviations and acronyms

APIs	Application Programming Interfaces
ASPSPs	account-servicing payment service providers
CBK	Central Bank of Kenya's
CBN	Central Bank of Nigeria
CDR	Consumer Data Right
CFPB	Consumer Financial Protection Bureau
DPAs	data protection authorities
FSCA	Financial Sector Conduct Authority
GDPR	General Data Protection Regulation
IFWG	Intergovernmental FinTech Working Group
MIT	Market Insight Transactions
MSMEs	Micro, Small and Medium Sized Enterprises
NCAs	National Competent Authorities
NPSD	National Payment Systems Department
OBR	Open Banking Registry
OFIS	Other Financial Institutions
OTP	One-Time Passcode
PAST	Profile, Analytics, and Scoring Transactions
PCI-DSS	Payment Card Industry Data Security Standard
PIFT	Personal Information and Financial Transactions
PIS	Payment Initiation Services
PIST	Product Information and Service Touchpoints
POPI Act	Protection of Personal Information Act
PSD2	Payment Services Directive
PSRs	Payment Services Regulations
SSA	Sub-Saharan African
TPPs	Third Party Providers

Executive Summary

The concept of Open Banking is generally well understood as the practice of sharing banking data via standardised and secure interfaces at the request of clients (OECD, 2023[1]). Open Finance could be described as the next stage in the evolution of Open Banking-type of data sharing arrangements. Building on existing frameworks, it expands data access and sharing to data sources beyond payment/transaction data, while it also includes other areas of financial activity (e.g. insurance) (OECD, 2023[1]).

Open Banking and Open Finance initiatives aim to enhance financial products and services, promote innovation, and foster healthy competition while empowering customers to make informed choices about their data. Using data to create innovative financial products has the potential to improve customer choice and lead to a more diverse range of tailored products that can be cost-effective and/or serve previously underserved parts of the population. Open Finance also presents opportunities to better inform consumers about their finances and their options, as well as enable client empowerment as customers gain control over their data. At the practical level, Open Finance solutions can also facilitate budget adherence, minimise unnecessary expenses, and streamline processes for seamless transitions between services. By promoting innovation through de-monopolising data, Open Finance can further encourage the expansion and diversification of the FinTech industry with potential beneficial impact on competition conditions and real economy growth.

Open Finance and Banking have the potential to benefit SSA countries by improving financial services, empowering customers, promoting competition, and encouraging innovation to address diverse and dynamic local needs. Any banking infrastructure limitations in certain SSA countries could be partially overcome by leveraging the region's high mobile money account ownership, and through innovative FinTech applications. Consent controls in data sharing agreements can effectively address data protection concerns in the region, enhancing customer trust and providing robust security measures against the emerging digital threats.

Open Finance is gaining traction in larger African economies, with South Africa being the most developed market hosting over 200 FinTechs offering various financial services, including account aggregation and lending. In particular, screen scraping (i.e. extracting data from a software application or web page's visual interface) is prevalent among FinTech startups due to its high cost-effectiveness. Concurrently, screen scraping practices involve significant privacy and data protection concerns, reinforced by jurisdictional issues with establishing the domicile of these entities. The need to foster capacity building for FinTechs and Third Party Providers (TPPs) in the region is reflected in the recognition of the value of Open Finance by the industry as a way of adapting their services to the customer needs.

Open Finance arrangements adopted by OECD member countries reflect varying policy objectives. For example, the EU revised Payment Services Directive (PSD2) aims to enhance the efficiency and competition of the internal market by providing a transparent legal framework for service providers while prioritizing data security and privacy to ensure effective consumer protection. SSA frameworks share similar objectives that relate to the promotion of competition, innovation, enhanced customer experience, and efficiency (e.g. Operational Guidelines from Nigeria).

Several OECD countries have implemented frameworks for Open Banking, with some expanding into the broader frameworks of Open Finance. Open Finance is defined in fewer jurisdictions and is typically implemented by extending the scope of the Open Banking definitions to encompass additional data sources and types. The nature of Open Banking and Finance mechanisms in Africa are either voluntary or mandatory. In select countries, legal frameworks have been incorporated, but the secondary implementing regulations are still pending.

As observed in OECD countries, there are two main design approaches to the data sharing frameworks: the market-led approach or voluntary framework (e.g. Japan, US, Switzerland), and the more prescriptive approach or mandatory approach (e.g. EU PSD2). In Africa, both approaches may be observed, for example Nigeria's voluntary approach can be compared against South Africa's incrementally mandatory approach. Each of the approaches fits the idiosyncrasies of the corresponding economies and is considered equally effective in delivering the objectives of such frameworks. The processing of customer data is limited within data sharing arrangements, as they are initiated through data access requests, indicating data subject's unequivocal consent to the ensuing operation. In most OECD countries, the customer is the only entity that has the authority to initiate such a data access request.

African Open Finance regulations are recognisably prudent regarding customer data protection (e.g. Operational Guidelines from Nigeria).Nigeria and South Africa's frameworks for Open Banking have delineated security and risk-specific protocols. All participants in Nigeria's Open Banking system are required to comply with minimum security principles which feature of layered security, clear separation of duties, least privilege, zero trust, dual control, need to know, and privacy as well as the risk-based Cybersecurity Framework. In South Africa, Open Finance activities may be regulated under the existing conduct frameworks that target specific areas such as cybersecurity or information security.

Certain security risks specific to screen scraping may be overcome through the use of Open Finance APIs, as they enable TPPs to access consumers' transaction data without requiring consumers to share their usernames and passwords. A few OECD countries require the use of APIs as a mandatory requirement for banks and other financial institutions to adhere to under the data sharing frameworks (e.g. Australia, Brazil, Türkiye). Many African countries have developed technical API standards, while others (e.g. Nigeria, Kenya) are currently in the preparatory process of defining such standards.

Accountability provisions are integrated into data sharing arrangements to promote legal clarity regarding the delineation of liability in cases of breaches of obligations concerning data access, quality, privacy, confidentiality, processing, sharing, storage, and cybersecurity standards (OECD, 2023[2]). Determining liability in such arrangements is a complex process as the cases are usually cross-border and involve multiple stakeholders. This creates difficulties with establishing the appropriate forum of jurisdiction and the lead national authorities in charge of the proceedings.

Apart from administrative and potential corporate liability, accountability frameworks encompass standards relevant to consumer experience, namely complaint-handling mechanisms and other redress and dispute resolution avenues. Nigeria and South Africa have both established well developed dispute resolution systems thar are enshrined directly in the Open Banking/ Finance regulatory frameworks. Such rules can also be found in other pieces of legislation, for example in Nigeria's Operational Guidelines which entail provisions regulating complaint mechanisms, liability management and dispute resolution avenues.

From the policy-making perspective, and irrespective of the approach taken by the authorities (i.e. mandatory frameworks/regulation or industry driven frameworks) it is necessary to consider shared objectives to ensure harmonisation of efforts across countries that have operating Open Finance/ Banking frameworks, as well as those which are currently developing such frameworks. Examples of common policy objectives of the SSA countries include prioritisation of consumer trust, interoperability standards and incentives that balance innovation with the necessary safeguards.

1 Open Banking and Open Finance in Sub-Saharan Africa: Market trends and associated benefits

1.1. Benefits of Open Finance

Open Finance arrangements tend to pursue common objectives such as spurring innovation in financial products and services, empowering consumers to make informed decisions about their data choices, and fostering healthy competition. These goals are reflected in the frameworks for such data-sharing initiatives across OECD countries (OECD, 2023[2]).

Leveraging data to create new innovative products and services has the potential to significantly improve the customer experience across the financial landscape. Data sharing initiatives aim to establish secure, regulated, and user-friendly environments that facilitate collaborations between banks, FinTechs, and other third-party service providers. This collaboration could foster the creation of cutting-edge financial services that not only elevate the customer experience but also align with international developments in financial services. This can lead to a more diversified portfolio of financial products that have the potential to be increasingly tailored to individual needs[1], less costly[2] if any efficiencies are passed on to the end customer, while they also have the potential to extend access to financial services to previously underserved populations, visible on the example of credit scoring for Micro, Small and Medium Sized Enterprises (MSMEs). In the latter case, Open Finance frameworks can play a crucial role in promoting financial inclusion for underserviced or financially excluded individuals (OECD, 2023[2]).

Open Finance presents new opportunities to educate consumers and help them make informed decisions around the use of their data for the provision of financial products and services. This may involve facilitating comparisons or aiding in the transition between different service providers. As customers incrementally get acquainted with exercising control over their data, they may in the future prioritise the choice of convenient data sharing arrangements potentially involving new service providers, which could significantly affect the shaping of future financial market dynamics.

[1] Open Banking and Open Finance can be a way to deliver hyper-personalisation, by utilising alternative and conventional data sources and behavioural science to deliver services, products and pricing tailored to the needs of individual customer. Although such practices can enhance customer experience, they also accentuate the privacy and data protection risks involved.

[2] Indeed, lower prices have been observed in several OECD countries for specific financial services (e.g. due to lower service fees) (OECD, 2023[2]).

Customers may benefit from Open Finance-enabled use cases allowing for presentation of financial data using comprehensible, user-friendly design, which can facilitate consumer decision-making. This could encompass practical applications like financial management for businesses, estimating taxes, projecting future inflows and outflows, and offering a convenient platform to explore various loan or credit options from different providers (OECD, 2023[2]). Such use cases can be very beneficial from the customer experience perspective, as financial documentation is usually contained in lengthy and complex legal provisions. By using design features, technical notices may become more comprehensible to the target audience, therefore discouraging mere check-box compliance by service providers (i.e. in case of disclosure requirements)[3] and providing customers with a clear overview of the ensuing rights and duties. The use of Open Finance frameworks can streamline processes, reducing bureaucracy and friction, resulting in a more seamless transition when switching between services or providers. This efficiency contributes to a reduction in the time and effort typically associated with such transitions (OECD, 2023[2]). It could also decrease the number of consumer complaints, as consumers can make a well-informed choice of financial provider selection, while being aware of ensuing legal obligations.

By de-monopolising data, Open Finance has the potential to promote innovation which can foster competition within the financial services sector. Open Finance frameworks encourage the rise of TPPs such as FinTech startups) either by offering existing services in novel ways or by introducing new services based on new data access options. The impact of proliferation of these frameworks within the FinTech industry is already evident in terms of both the size of expansion and the rate of diversification of companies across various OECD countries (OECD, 2023[1]).The advent of new market participants, as observed in certain jurisdictions with Open Banking frameworks (such as account information service providers or aggregators), is also a likely outcome. Moreover, these frameworks may stimulate the number of collaborative initiatives between traditional banks and financial institutions on one side and FinTechs and other TPPs on the other (OECD, 2023[2]).

Other advantages of extending the access to financial data include overall improvement of customer experience through the delivery of services that are more streamlined, and cost-effective. This can cause a shift in market dynamics as service providers need to account for the changing needs of customers which may expect specific data sharing arrangements as part of the traditional financial services provision (OECD, 2023[2]). All in all, this can foster consumer empowerment, in line with the underlying idea of Open Finance, namely of giving back the control over data to the rightful owners.

1.2. Benefits of Open Finance in sub-Saharan Africa

The benefits of Open Finance and Open Banking, particularly the potential fostering of customer empowerment, and promotion of competition are particularly relevant to the SSA context. For instance, Open Finance frameworks can help companies customise their offerings to address the diverse and dynamic needs of SSA populations (e.g. using tailored microfinance and agricultural products to address the needs of rural communities). As the African population is forecasted to increase by one billion by year 2050 (Amadou, 2019[3]), financial services providers will need to diversify their offer to cater to the needs of such an increasingly heterogenous society.

Africa's financial landscape is characterised by a limited banking infrastructure. In such regions, Open Finance can continue to facilitate the leap frogging of older and less efficient banking systems by enabling FinTech innovation. As 33% of adults own a mobile money account, Sub-Saharan Africa is well positioned

[3] This can be compared with the increasing use of legal design in customer-facing legal documentation such as the provision of terms and conditions. Legal design aims to transform legal provisions into schematic, design-based blocks that utilise plain language to render the provided information more accessible. Analogically, user-friendly financial data design can serve a similar purpose of catering to previously undeserved audiences.

to harness its strong mobile payment user base to expand the services portfolio to areas such as insurance and investments (World Bank, 2023[4]).

In addition, consent controls made available through data sharing agreements can make customers feel more in charge of their data, which can be crucial in addressing data privacy concerns, as displayed by local populations region. Limitations to data privacy can put African users at risk of being exposed to digital threats such as hacking or identity theft. Fraud instances may contribute to generating a low level of trust displayed by customers towards the digital services and products.

Open Finance also creates opportunities for FinTechs in the region to compete with more traditional financial institutions (e.g. banks) and other established institutions (e.g. mobile network operators). This opens up the market to new entrants, which would not be possible without de-monopolising of data previously held by traditional financial institutions, that effectively enjoyed the position of gatekeepers. Such diversification of service providers may act as a stimulus for more innovation in the sector. As a result, consumers can enjoy a wider range of choices in financial products and services, with the offer being adjusted to different price ranges and varied individual needs.

One of the most important use cases for Open Finance in Africa involves the expansion of access to credit for individuals and MSMEs. This practice has the potential to impact access to financial services in emerging markets, where financial institutions may struggle with conduct risk assessments of individuals/ MSMEs due to a limited amount of information available. Therefore, proliferation of Open Finance frameworks in sub-Saharan Africa could help stimulate the growth of the FinTech lending industry, expanding the number of individuals and groups that can access credit (Mazer, 2023[5]).

Box 1.1. Financial literacy in Sub-Saharan Africa

In some SSA markets, barriers to identification, lack of internet access, poor financial literacy, and insufficient size of device ownership can make the benefits of open finance harder to access for vulnerable groups (FSCA, 2023[6]). Lack of formal identification remains a key challenge, as it proves to be an obstacle in adhering to customer due diligence standards, which largely restricts access to many services or products for the affected individuals. In the sub-Saharan region alone, 30% of unbanked users do not have the necessary documentation needed to open mobile money accounts (World Bank, 2023[7]).
Despite improvements to the rate of internet usage and a rising number of mobile money users, only 36% of the African population had access to broadband internet as of 2022 (World Bank, 2023[4])..The SSA financial landscape is also characterised by an uneven access to technology infrastructure, which is directly linked to varying levels of financial literacy across local populations. These characteristics have an impact on the level of trust displayed towards data sharing products and services, which have to be taken into consideration by the service providers.

Source: FSCA 2023, World Bank.

1.3. Current Market Trends in Sub-Saharan Africa

Open Finance frameworks have already been developed in larger African economies due to the significant level of market activity and consumer uptake in mobile payments. Presently, South Africa can be considered to be the most developed market for Open Finance in the region. Over 200 FinTechs are present in South Africa, with some of these companies operating from foreign domiciles (FSCA, 2023[6]). According to the Financial Sector Conduct Authority (FSCA), FinTechs in South Africa offer services such as account aggregation, financial management, alternative insurance, lending and payment solutions. While Open Banking practices are offered by some financial institutions and third-party providers, there

has been a particular increase in screen scraping activities amongst FinTechs. This practice has also been observed in select OECD countries, such as the US and Israel (OECD, 2023[1]).

Screen scraping[4] activity is common amongst emerging FinTech startups as a cost-effective method of collecting customer data. While this method is a useable mechanism for accessing data, it can potentially infringe upon data protection and customer protection frameworks as customers are unable to control the scope or duration for which third party providers are accessing their credentials. Other risks involve possibly limiting the effectiveness of fraud detection mechanisms, due to the involvement of an intricate web of intermediaries that have access to sensitive financial data. As the roles of stakeholders involved may not be clearly outlined, risks to the safety of payment systems may be accentuated. In particular, the South African Reserve Bank outlines risks that screen scraping may pose to cybersecurity of IT systems of the financial institutions involved (NPSD, 2020[8]).

A few operators that engage in screen scraping in South Africa are domiciled in other jurisdictions, which poses challenges to the enforcement of certain regulations (NPSD, 2020[8]). As many of these operators are not licensed as financial institutions, they can partially evade the obligations ensuing from being subject to domestic financial authorities. Setting aside the glaring challenges that this poses from the legal perspective, such operators may profit from regulatory arbitrage and utilise harmful data access strategies. Thus, the popularity of screen scraping may be attributed to lax regulatory regimes, as well as practical considerations of a lack of alternatives for cheaper and real-time electronic payments (NPSD, 2020[8]).

According to the FSCA 2020 survey, although most banks do not support third-party use of screen scraping, they effectively dispose of no mechanisms that are able to intercept such activities. Other detected risks to financial institutions include breaches to data privacy, cybersecurity and lack of uniform API standards, (FSCA, 2020[9]).

Concurrently, many surveyed companies understand that broader global trends will render the implementation of Open Finance frameworks inevitable. Enterprises appreciate the potential benefits to cultivating innovation, enhancing customer experience, and fostering competition. However, in order to reap these benefits, the risks will need to be addressed, which can be done *inter alia* through capacity building of FinTechs and TTPs.

In Kenya, there is currently a lack of standardised or industry-wide open APIs, which could have a negative impact on competition and business growth for smaller FinTech players. Current market practice of the opening of APIs has been mostly based on bilateral agreements established between banks and TPPs. Mobile service providers have yet to fully open up access to their APIs. Such market dynamics significantly limit the customer choice, as the ability of smaller companies to roll out new products and services is significantly reduced (CBK, 2020[10]).

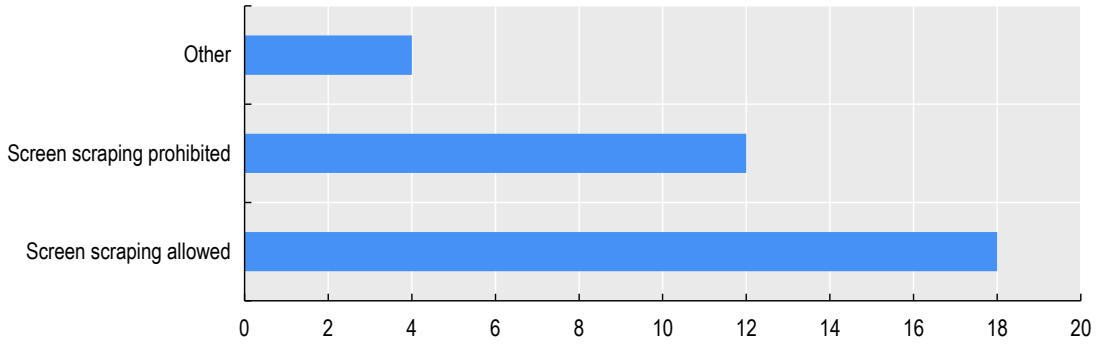
Ghana's regulatory sandbox, launched in 2023, has provided a means of churning market activity in Open Banking, as the conditions of the sandbox allow banks and third-party providers to test new products in a collaborative manner (Agpaytech, 2022[11]).

1.3.1. Screen Scraping in OECD Member Countries

According to the 2022 OECD survey on data sharing frameworks, 18 out of 34 surveyed OECD countries continue to allow screen scraping practices as of 2022 (OECD, 2023[1]). There are significant security risks and liability burdens ensuing from screen scraping, while acknowledging the potential for APIs to provide a more secure method of accessing consumer financial data (OECD, 2023[1]).

[4] Screen scraping (or Web scraping) is a data collection method used to gathering information shown on a display to use for another purpose. Typically, it is used by a technique where a computer program extracts data from human-readable output coming from another program.

Figure 1.1. Screen scraping practices in the OECD area



Note: The report is based on 34 responses to the OECD Survey by 31 OECD countries: Australia, Austria, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, Poland, the Slovak Republic, Slovenia, Korea, Spain, Switzerland, Türkiye, UK, US, as well as by three non-OECD member countries Brazil, Hong Kong (China) and South Africa.Source:. (OECD, 2023[1]).

2 Policy objectives and regulatory trends in Open Banking and Open Finance

2.1. Policy objectives and Definitions

2.1.1. Definitions of Open Banking and Open Finance

Practices in OECD Countries

In the majority of OECD countries, there is no legal definition of Open Banking (Figure 2.1. Defining Open Banking and Open Finance

). The concept is generally understood as a practice of sharing banking data through standardised and secure interfaces upon data access request. In the UK, Open Banking is defined as a framework that facilitates secure sharing of customers financial information with third party service providers (Account Information Service Providers or "AISP"), granted consumer consent (OECD, 2023[1]).This definition also encompasses the capability of third-party service providers to initiate payments on behalf of a customer, provided explicit consent is obtained, a service referred to as Payment Initiation Services (PIS).

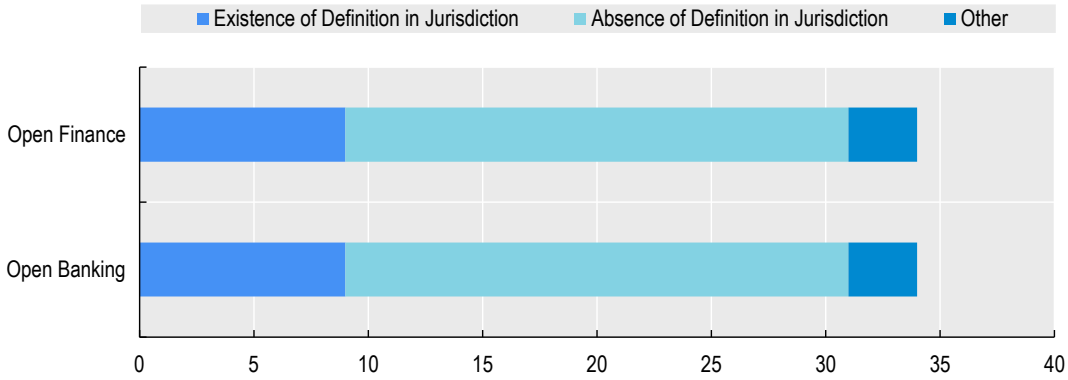
In the European Union framework, Open Banking refers to the granting of access to payment account-related data to third party service providers (EU PSD2). This is governed under Directive (EU) 2015/2366 on payment services (PSD2) and the Commission Delegated Regulation (EU) 2018/389 (OECD, 2023[1]).The goal of PSD2 is to enhance competition in the EU payments market by providing third party providers (“TPPs”) with access to payment accounts data held by account-servicing payment service providers (“ASPSPs”). ASPSPs are most commonly banks that previously held a monopoly on payment services and the associated data (OECD, 2023[1]).

Not all OECD member countries have established definitions for Open Finance within their jurisdictions (Figure 2.1. Defining Open Banking and Open Finance

). However, most of the countries that have such definitions had already laid down the foundations for Open Banking frameworks, which are then expanded to use cases beyond payments. These varied use cases can involve different types of financial services or products that can span across different sectors. For example, Australia has explicitly broadened its financial framework to sectors such as energy or telecommunications (OECD, 2023[1]). In Brazil, other areas covered under Open Finance framework include insurance, open pension funds, investment and foreign exchange (OECD, 2023[1]). In Israel, the scope of Open Finance regulations encompasses a broader set of data than for Open Banking, as it relates to data pertaining to current accounts, cards, deposits, saving, loans and securities (OECD, 2023[1]). In the

Netherlands, the term Open Finance is used to denote the opening up of financial institutions to collaborations with third parties, which is facilitated by data sharing and adoption of APIs (OECD, 2023[1]).

Figure 2.1. Defining Open Banking and Open Finance



Note: The report is based on 34 responses to the OECD Survey by 31 OECD countries: Australia, Austria, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, Poland, the Slovak Republic, Slovenia, Korea, Spain, Switzerland, Türkiye, UK, US, as well as by three non-OECD member countries Brazil, Hong Kong (China) and South Africa.Source: (OECD, 2023[1]).

Practices in SSA Countries

South Africa provides a framework of financial data sharing that extends beyond payments. Such expansion of the regulatory scope allowed for a gradual progression towards Open Finance. Five key use cases enshrined under this framework include account aggregation, financial management, payment initiation, alternative lending, and insurance. These use cases were chosen by the FSCA as the most aligned with the authority's mandate to protect and empower consumers and SMEs (FSCA, 2023[6]).

While Nigeria's existing regulations are categorised as Open Banking documents, the Circular on the Regulatory Framework on Open Banking in Nigeria states that the framework is for banking as well as "other related financial services" that include payments and remittance services, collection and disbursement services, deposit taking, credit, personal finance advisory and management, treasury management, credit ratings/scoring, mortgage, leasing/hire purchases, and "other services as may be determined by the Bank" (CBN, 2023[12]). While some of these services define the scope of Open Banking, others indicate that the document may operate more extensively as an Open Finance framework.

Kenya's strategy document focuses on open "infrastructure" as a guiding phrase, as opposed to Open Banking or Finance (CBK, 2020[10]). Similarly, the Bank of Ghana's Payment Systems Strategy 2019 – 2024 uses terms such as data sharing and open standards/architecture for transactions on electronic platforms (Bank of Ghana, 2019[13]). Rwanda also invokes the term data sharing rather than Open Banking (Government of Rwanda, 2021[14]).These trends may indicate that African countries may try to steer away from Open Banking and towards Open Finance frameworks in the future.

2.1.2. Policy objectives of Open Banking and Open Finance

Practices in OECD Countries

As aforementioned, Open Finance arrangements in OECD member countries are guided by multiple objectives. To show how such objectives are enshrined in law, the PSD2 Directive in the EU aims to ensure that within an efficient and competitive internal market, all types of service providers can have access to payment account data, without being obstructed by gatekeepers such as traditional banks.

Simultaneously, the legislation seeks to ensure a high standard of data security and privacy, thereby enhancing consumer protection. Similar objectives are pursued by data sharing frameworks in other OECD economies. For instance, the Korean framework aims to support the launch of innovative financial services through payment infrastructure and to increase consumer welfare through fair competition (OECD, 2023[1]).

Data sharing can be used to promote innovation through stimulating the development of new products and services across the financial landscape. In Japan, the amendments to the Banking Law of 2018 established an institutional framework designed to foster open innovation between financial institutions and FinTech companies, all the while prioritising user protection (OECD, 2023[1]).

Regarding customer experience, the Australian CDR is designed to empower consumers by enhancing the control exercised over data, facilitated through a straightforward and user-friendly service design. Likewise, in Brazil, one of the key goals of Open Finance is to restore the control over financial data to consumers. This stems from the acknowledgement that consumers are rightful owners of their data and possess the right to dispose of it, inter alia through consenting to data-sharing arrangements. Open Finance initiatives can also potentially improve financial access by supporting the development of FinTech applications built on the basis of such data sharing arrangements, thereby promoting financial inclusion (OECD, 2023[1]).

Another objective involves the incorporation of third parties into the existing data and consumer protection regulatory frameworks. In the United States, despite the absence of Open Banking-specific legislation, existing frameworks remain applicable, such as the Gramm-Leach-Bliley Act (GLBA) which incorporate principles of data protection and privacy. In Canada, the Advisory Committee on Open Banking has outlined six key consumer outcomes to guide the vision and serve as a foundation for an Open Banking system in Canada. These include the protection of consumer data; empowering consumers by giving control over their data; extending consumer access to a broader array of useful, competitive, and consumer-friendly financial services; ensuring that consumers have reliable and consistent access to services; offering recourse for consumers when issues arise; and ensuring consistent consumer protection and market conduct standards (OECD, 2023[1]).

In some countries, although the legal frameworks have been established, the implementing secondary regulations are still pending. For example, in Mexico, the legal provision mandating the disclosure of Open Banking information on payments and transactions exists, but the regulatory guidelines for its implementation have not been issued yet (OECD, 2023[1]).Conversely, Israel establishes an Open Banking framework for payments; however, due to the absence of accompanying implementing legislation, its effective incorporation has not been realized as of yet (OECD, 2023[1]). Korea's Financial Services Commission has instituted an Open Banking policy aimed at fostering competition in the financial markets and optimizing consumer welfare. In Japan, the Banking Law was amended in 2018 to promote Open Banking initiatives, obliging banks to open their APIs in a non-binding commitment, thereby allowing FinTech companies, such as electronic settlement agents, to access the banks' systems (OECD, 2023[1]).

Other countries are in the process of establishing their frameworks. Canada, for example, issued a mandate in March 2022 to develop a “made in Canada” regime based on the recommendations in the final report of the Advisory Committee on Open Banking (OECD, 2023[1]).

Practices in SSA countries

In line with the abovementioned objectives, Nigeria’s Operational Guidelines aim to improve efficiency and access to financial services while also improving competitive landscape (CBN, 2023[12]). The Circular on the issuance of a regulatory framework additionally indicates promoting innovation as a goal (CBN, 2023[12]). However, competition and access to financial services are prioritised across both documents.

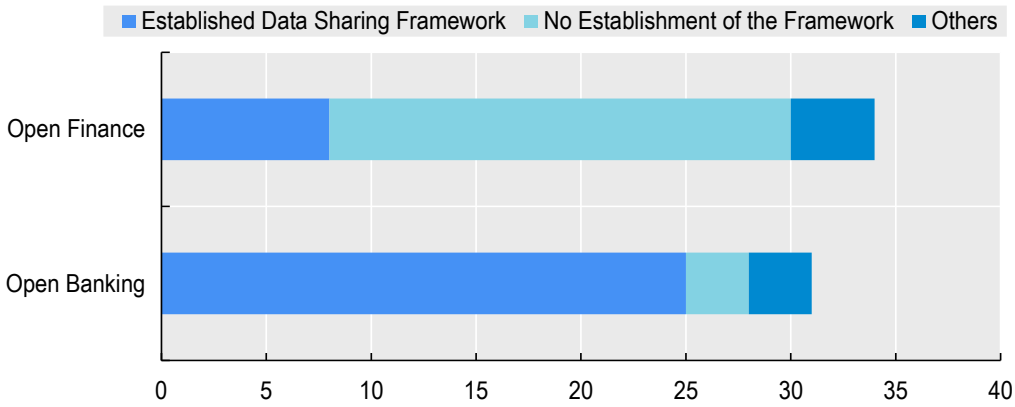
In South Africa, innovation, customer experience, and competition, particularly for FinTechs, are similarly emphasized as policy objectives (FSCA, 2023[6]). The framework aims to minimise data security risks that could ensue from the screen scraping activity in the South African market.

The Central Bank of Kenya has set out the primary objectives of its National Vision and Strategy as prioritizing customer centricity, establishing interoperability standards for digital finance, and ensuring high quality of financial products and services, which is in line with the objectives that guide many OECD countries (CBK, 2020[10]). Likewise, Mauritius has built its central automated payment switch, MauCAS, on open standards for the purpose of improving interoperability and efficiency (Bank of Mauritius, 2023[15]). The Bank of Ghana is also specific about the role of data sharing standards as a strategic initiative to promote financial innovation (Bank of Ghana, 2019[13]).

2.2. Management Structure

2.2.1. Types of Governance Frameworks

Figure 2.2. Established Frameworks for Open Banking and Open Finance



Note: The report is based on 34 responses to the OECD Survey by 31 OECD countries: Australia, Austria, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, Poland, the Slovak Republic, Slovenia, Korea, Spain, Switzerland, Türkiye, UK, US, as well as by three non-OECD member countries Brazil, Hong Kong (China) and South Africa.
Source: (OECD, 2023[1]).

In Sub-Saharan Africa, a few larger economies such as Nigeria and South Africa have published Open Banking/Finance frameworks, while others such as Kenya, Ghana, and Rwanda are in the process of developing frameworks as part of their long-term payments system and digital finance strategies (Figure 2.2).Open Banking in Nigeria is guided by two key regulatory documents: the Regulatory Framework for Open Banking, released by the CBN in February 2021, and the Operational Guidelines for Open Banking, released in March 2023 (CBN, 2021[16]; CBN, 2022[17]).The former document primarily defines data access levels for qualifying Open Banking participants as per a tiered risk management system also laid out in the framework. Together, these data and service risk ratings are to be factored into the technical design of the API model and its information security specificationsThe Regulatory Framework establishes a 4-tiered risk management system based on the maturity levels of participants. The four categories include Tier 0) participants without regulatory licenses, Tier 1) participants who are partaking in the CBN Regulatory Sandbox, Tier 2) licensed Payment Service Providers and OFIS (Other Financial Institutions), and Tier 3) deposit money banks. Tier 0 participants must be sponsored by Tier 2 or 3 actors to be eligible for onboarding, while the eligibility of Tier 1 participants is based on their successful admission

to the regulatory sandbox. Tier 2 and 3 participants are required to produce risk assessment reports for themselves and for any Tier 0 institutions that they are sponsoring.The Regulatory Framework further outlines four categories of data and services that include Product Information and Service Touchpoints (PIST) 2) Market Insight Transactions (MIT), 3) Personal Information and Financial Transactions (PIFT), and 4) Profile, Analytics, and Scoring Transactions (PAST). The risk rating increases for each data and service category, starting with the lowest risk category for PIST and ending with the highest in PASR category. All categories of participants have access to PIST and MIT data. For other categories, tiers 1, 2, and 3 can access PIFT data, but only tiers 2 and 3 can access PAST data.The current policy and regulatory landscape for Open Banking/Finance in South Africa is characterised by three key documents, which include 1) a consultation paper published by the National Payment Systems Department (NPSD) on Open Banking activities, 2), the FSCA research paper on Open Finance, and 3) a draft Position Paper by FSCA on Open Finance, which is also the most recent of all three documents (FSCA, 2020[9]; FSCA, 2023[6]; NPSD, 2020[8]). Although the roles of these authorities vary as the NPSD's mandate focuses on the regulation of payment systems, while FSCA is responsible for regulating conduct of financial institutions, all views regarding Open Banking and Finance are coordinated by the Intergovernmental FinTech Working Group (IFWG).

Although the exact design of the mandatory regulatory regime is currently still being determined, the Draft Position Paper identifies four types of participants for regulatory oversight: financial institutions, third party providers, FinTechs and other relevant service providers (FSCA, 2023[6]).FSCA recommends that financial institutions are subject to data protection standards and that any entity that is using APIs to access data for providing financial services will require a license along with adhering to the necessary regulatory requirements. If such entities provide financial products in addition to services, they will be subject to similar requirements as those applied to traditional financial institutions. For activities that are neither financial products nor services, such as customer data aggregation, which are not being performed for a licensed financial institution, the nature of regulatory requirements is yet to be determined. The recommendations outlined by FSCA are in line with the NPSD consultation paper, which recommends the licensing and regulation of third-party providers, thereby demonstrating the policy coordination between both entities.

Kenya is currently in the development stage of its Open Banking framework. The Central Bank of Kenya's (CBK) National Payment System Vision and Strategy 2021 – 2025 outlines the country's intentions for future regulation of Open Banking. As per the document, the National Treasury and Planning is in the process of finalising a digital finance policy that focuses on the integration of financial service delivery and digital technology, and which includes open infrastructure as a main strategic objective. The vision is informed by priorities such as customer centricity, interoperability for digital finance, and quality of financial products and services, which are in line with the benefits offered by data sharing (CBK National Vision and Strategy). It also looks towards Open Finance as a means to improve innovation in payments technology and business growth. The CBK will also define clear risk management frameworks and standards that clarify liability and consumer protection, as per the National Payments System Vision and Strategy (CBK, 2020[10]).

Ghana's Payment Systems Strategy 2019 – 2024, released by the Bank of Ghana, is a central document for understanding the progress of regulating Open Banking in Ghana (Bank of Ghana, 2019[13]). The Strategy entails the creation of data sharing standards as a as a strategic initiative to promote financial innovation.

Between the years 2019 and 2024, the Bank of Ghana intends to define open standards and architecture for electronic platforms used for government transactions. This is a separate scheme from the greater 2021 – 2024 initiative to promote Open Banking for the purpose of stimulating innovation, competition, and customer choice. This entails creating and setting standards for data sharing and engaging stakeholders in developing a roadmap for data sharing.

According to the strategy, it appears that the push for Open Banking guidelines/standards is driven more greatly by the need for enhanced provision of financial services rather than the need to regulate the ongoing Open Banking market activity itself, as has been the case in South Africa. According to the strategy, the Bank of Ghana intends to develop Open Banking guidelines specifically by the end of 2023 (Bank of Ghana, 2019[13]).

While there are currently no Open Banking/Finance regulations or schemes that have been implemented in Rwanda, the Bank of Rwanda, the Ministry of Finance and Economic Planning, and the Ministry of ICT & Innovation are currently exploring the possible benefits of developing such an initiative as per the Rwandan FinTech Strategy (Government of Rwanda, 2022[18]). Rwanda has introduced a regulatory sandbox initiative and a class of payment initiation providers, both of which have been modelled after Europe's PSD2.

The Rwanda FinTech Policy 2022 – 2027 launches a steering committee as a core governance structure under which there are four working groups that will focus on implementing the policies. These working groups are based on four priority sectors. For example, Paytech and Credit working group is responsible for enabling, guiding and monitoring policy developments related to data sharing and API standards (Government of Rwanda, 2021[19]).

Select countries such as Mauritius have incorporated open APIs directly into their payment switches as opposed to publishing a framework first. According to the Bank of Mauritius, the Mauritius Central Automated Switch (MauCAS) is API-enabled and built on open standards (Bank of Mauritius, 2023[15]).The MauCAS allows non-bank third-party providers to access select customer data stored by banks via the Bank of Mauritius while ensuring strict security. It is intended to allow payment operators to eventually develop Open Banking solutions. The MauCAS, launched in 2019, is Mauritius's central payment switch and intends to reduce the operational and financial costs of current retail payments.

Beyond the MauCAS's API-enabled technology and governance, there are no documents regarding the governance of Open Banking that have been released by the Bank of Mauritius thus far, suggesting that Open Banking growth is intended to be market-driven rather than regulator-driven. However, the Bank has stated that the switch abides by the EU PSD2 framework (Bank of Mauritius, 2023[15]).

2.2.2. Mandatory vs. Voluntary Mechanisms

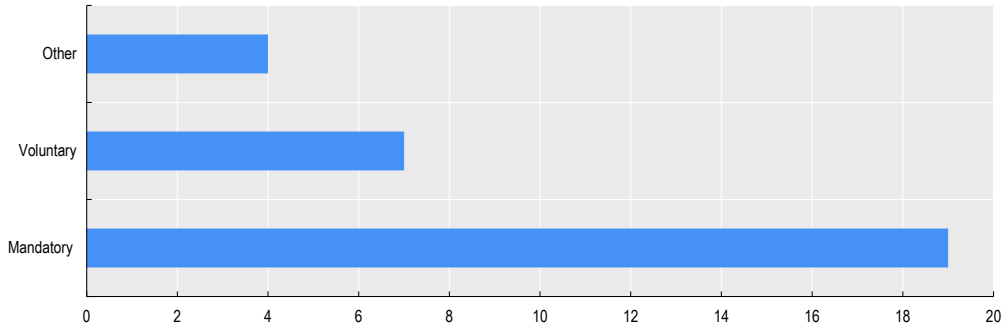
Practices in OECD Countries

The majority of data sharing arrangements in OECD countries are compulsory. In the EU, PSD2 and all relevant Regulatory Technical Standards and Guidelines are obligatory for payments accounts providers (Figure 2.3). Specifically, the sharing of user payment account data is mandated for intermediaries providing online/mobile banking services to their customers, upon user request and with their consent. Access to the account is restricted to licensed TPPs acting on behalf of the user and with their consent. In Australia, any entity designated as Consumer Data Right (CDR) data holder is obligated to participate and make available specific data under the Consumer Data Right. In Türkiye, top 10 banks were required to open their Payment Initiation and Account Information API Services by December 2022, while the remaining banks were given an extension until December 2023 to comply (OECD, 2023[1]).

In the UK, Open Banking is mandatory for Account Servicing Payment Service Providers under the PSRs (Payment Services Regulations), and detailed technical and operational requirements apply additionally to the CMA 9 under the CMA Order. ASPSPs are required to grant access to customers' payments account data without contract, free of charge and without restriction or discrimination. As of now, Open Finance is

not obligatory. Smart Data[5] will impose mandatory data sharing across specific sectors once a scheme is established. Establishing such a scheme would require government to bring forward secondary legislation outlining the specific parameters of the smart data scheme within the context of a particular sector. Open Finance could potentially be established as one of the sector specific schemes under Smart Data, in which case it would become mandatory, but there has been no decision or policy commitment by Government to do so as of yet (OECD, 2023[1]).

Figure 2.3. Mandatory or voluntary character of data sharing arrangements



Note: The report is based on 34 responses to the OECD Survey by 31 OECD countries: Australia, Austria, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, Poland, the Slovak Republic, Slovenia, Korea, Spain, Switzerland, Türkiye, UK, US, as well as by three non-OECD member countries Brazil, Hong Kong (China) and South Africa. 'Other' category includes mandatory character for some intermediaries only; time-limited mandatory requirements that have now expired or work-in-progress frameworks that are yet to be implemented.
Source: (OECD, 2023[1]).

Practices in SSA Countries

The nature of Open Banking and finance mechanisms in Africa are either voluntary or incrementally mandatory. CBN does not mandate actors in the financial ecosystem to participate in data sharing, although it is possible that the data sharing will be made mandatory for all actors in the future (Mazer, 2023[20]). While banks are not required to participate in the practice itself, they are still obliged to comply with the data sharing and API standards set by the CBN (Gray et al., 2022[21]). For instance, all participants are required to enter a data access agreement and service level agreement between providers and consumers. A voluntary approach means that the implementation of Open Banking will depend not on mandated participation by qualifying institutions but by the successful collaboration between the CBN, banks, NBFIs, and API developers.

The FSCA in South Africa recommends an incremental approach to implementing Open Finance, i.e., a phased mandatory regulatory regime that initially focuses on use cases for Open Banking such as payment initiation before broadening its scope to use cases such as alternative lending or insurance which can involve more risks (FSCA, 2023[6]). According to FSCA, a mandatory regime may help promote financial inclusion and financial sector competition. As per the OECD Survey, this approach is in line with practices in other jurisdictions trying to promote competition, such as Mexico and the UK (OECD, 2023[1]).

[5] 'Smart Data' refers to the secure sharing of consumer and product data with third-party providers upon consumer consent. Providers may then use this data to provide innovative services for consumers and SMEs. This can be considered as an extension of the "right to consumer data" under the General Data Protection Regulation (GDPR). (Siobhan Dennehy, 2022[2]).

2.2.3. Open Banking Registry

Thus far, Nigeria is the sole country to have dictated the development of an Open Banking registry as part of the Open Banking framework (CBN, 2021[16]). All participants in Tiers 1, 2, and 3 are to be listed in the Open Banking Registry (OBR), which will be provided and maintained by the CBN to ensure regulatory oversight and transparency around registered actors in data sharing agreements. The registry will be available to the public as a repository of APIs. Detailed registrants will be identified by business registration numbers issued by the Corporate Affairs Commission.

2.3. Information Sharing

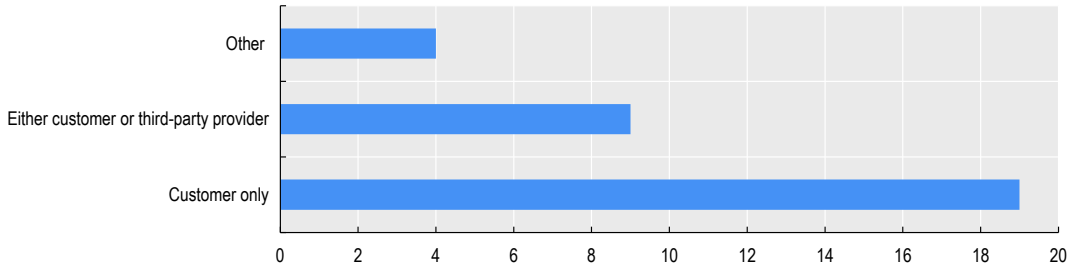
2.3.1. Consent Management

Practices in OECD Countries

Initiation of data requests and corresponding customer consent is another crucial aspect of data sharing arrangements and plays a significant role in safeguarding customer data and their privacy, while also having operational implications for data providers. In most OECD countries, only the customer has the authority to initiate a data access request. For instance, in the UK and Japan, data access request can only be initiated with customer's explicit consent. In other countries, such as Switzerland and Mexico, there are no specific rules, and the general legal framework is applicable. In the Czech Republic, anyone can initiate a data access request to the Open Data portal (OECD, 2023[1]).

In some countries, such as Brazil, Colombia, Germany and South Africa, data access request may be initiated by the customer or the third-party provider, with the essential condition of having acquired customer's consent. Similarly, in the United States, while not exclusive to customers, most firms generally require customer-permissioned access. In Australia, accredited data recipients initiate the data access request on behalf of a consumer, provided the consumer has expressly consented to the data recipient collecting their data (OECD, 2023[1]).

Figure 2.4. Initiation of Data Access Request



Note: The report is based on 34 responses to the OECD Survey by 31 OECD countries: Australia, Austria, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, Poland, the Slovak Republic, Slovenia, Korea, Spain, Switzerland, Türkiye, UK, US, as well as by three non-OECD member countries Brazil, Hong Kong (China) and South Africa.
Source: (OECD, 2023[1]).

Customers have the ability to revoke their consent to data sharing across jurisdictions. The procedure for such withdrawal is contingent on the specific country's domestic framework or the overarching data sharing legal framework (e.g. GDPR and PSD2 in the EU Member States). In the EU, consent may be withdrawn by the payer at any time, but it must occur no later than at the moment of irrevocability in accordance with

Article 80 of PSD2. Consumers can revoke consent via the third-party provider (e.g. France), electronically (e.g. Hungary) or through the credit institution direct interfaces and/or directly through the third-party provider (e.g. Latvia) (OECD, 2023[1]).

Practices in SSA Countries

In Nigeria, "customers shall always have control over their data and be able to access, manage or withdraw their consent at any point in time," and providers can only share customer data to consumers after proof of consent has been authenticated (CBN, 2023[12]). If an entity wants to share data with non-Nigerian participants, a specific approval needs to be obtained from the CBN, which is assessed on the basis of application detailing how the data is intended to be used. The Operational Guidelines split consent management into a consent stage, an authentication stage, and an authorisation stage, with stage corresponding to varying legal obligations. The guidelines provide a considerable amount of detail on consent management from the beginning to the end of the process, particularly for the authorisation stage. In the consent stage, users must be made aware of any requests to access data or funds from their account, the nature of the data in question, the parties involved in the data sharing request, and the duration for which these parties would maintain information access.

To verify user identity, participating actors are then required to provide authentication measures. These measures must be implemented within authorised channels, such as email addresses, mobile phone devices, or through the use of biometric verification. Furthermore, the user endpoint in these channels should also be verified using mechanisms such as OTP (One-Time Passcode) verification.

Finally, within the authorisation stage, customers can manage their consent options for providing data to participating actors, including options for enabling or revoking access permissions. Customers should also be able to manage their consent through a minimum of two channels and be informed of their right to revoke consent. To prevent fraud, providers must also ensure that the API supports out-of-band authentication as necessary and stores the associated data. Customers must always be notified when an entity accesses their data via email, SMS, or in-app notifications. Furthermore, a transcript detailing the use of the customer's data must be provided to the customer on a monthly basis or upon request.

In South Africa, requests for data access can be initiated by the customer or by the third-party provider, based on customer consent (OECD, 2023[1]). This is in line with practices in other OECD countries, such as Brazil Colombia, Germany, and South Africa (OECD, 2023[1]). FSCA requires that the customer consent is well-informed and is made available to financial institutions/ TPPs upon request. Customer consent should be unequivocal, i.e. never be aggregated with other consent agreements and freely given, i.e. never be made conditional upon obtaining unrelated financial products or services. The duration of access has to be limited in time and remain easily revokable upon customer request Furthermore, third-party providers must ensure that customers understand the implications of giving data access consent, as well as comprehend the ways in which their data will be used.

Many of these data protection principles are enshrined in the Protection of Personal Information Act, 2013 (POPI Act), which includes specific standards that have to be respected when obtaining data subject consent.

2.4. Data protection and Identity

3.4.1 Data Protection

African legislation and regulation around Open Finance are recognisably prudent regarding customer data protection. For example, in Nigeria, the Operational Guidelines for Open Banking require that participants are explicitly required to comply with the Nigerian Data Protection Regulation and any CBN-issued data

protection regulations with regards to FIs (CBN, 2022[17]).This includes enabling the customers to exercise their right to data portability and implementation of measures preventing data breaches. The guidelines also mandate the development of a data governance policy and data ethics framework that ensure that data processing activities are managed in full respect of data protection principles.

As per the guidelines and the Nigerian Data Protection Regulation, providers are forbidden from using, accessing, or storing customer data for purposes other than the services requested by the end user. Providers must also ensure that any data obtained for the purpose of Open Banking is retained for a minimum period of seven years. Furthermore, any third-party storing customer data must possess the technical and organisational measures to manage data acquired through Open Banking APIs.

To ensure responsible data flows, providers must digitally store all financial data shared by the customers and maintain a comprehensive record of all information involving sharing requests and other associated actions.

In South Africa, to prevent data privacy risks associated with screen scraping, FSCA recommends the development of technical standards for APIs along nine guiding principles: openness, usability, interoperability, independence, stability and transparency (FSCA, 2023[6]). The Payment Association of South Africa is also exploring policy options such as 1) developing an industry solution for e-commerce purchases, 2) following the European PSD2 approach, or 3) developing and ensuring enforcement standards like the Payment Card Industry Data Security Standard (PCI-DSS).

For further protection, South Africa's FSCA proposes that customer financial data should not be identifiable and should only be used for purposes expressly consented to by the customer. Uninformed consent should not override customer expectations, and strong customer authentication measures should be implemented to ensure data security.

South Africa's NPSD requires that third party providers do not store customer data beyond what is strictly necessary for the provision of services, while also bearing liability risks in case of non-compliance. Furthermore, the data has to be used in accordance with its intended purpose and be safeguarded by security measures (NPSD, 2020[8]). In addition, the NPSD recommends creating and regulating a new class of third-party providers, where those practicing screen scraping must identify themselves to the Reserve Bank.

The Central Bank of Kenya intends to support the development of a framework for financial data protection and governance that would complement the existing Data Protection Act of 2019. In its preparatory stage, the Bank is conducting research into the ways in which financial data is collected, stored, and shared, with the view of enacting a framework capable of addressing the associated risks in the future (Central Bank of Kenya, 2020[22]).

In Rwanda, the Data Protection and Privacy Law of 2021 forms the foundation of the framework governing any data sharing initiatives. It provides requirements for collection, storage, and processing of personal data, which have to be adhered to when authorising data sharing arrangements between consumers and TPPs (Government of Rwanda, 2022[18]).

3.4.2 Identity Management

Nigeria's regulations contain provisions with regards to identity management. Nigeria's Operational Guidelines require each endpoint that accesses an Open Banking service or product to be identified and for its specific attributes to be examined (CBN, 2022[17]). Identifiers such as the Biometric Verification Number, National Identity Number, and Tax Identification Number have to be stored in independent identity systems.

Providers are also responsible for implementing digital tokens, along with identity token management system that ensures that TPPs are in possession of legitimate tokens and have the right access in relation

to specific data permissions or functionalities. Upon consent verification, providers must create encrypted tokens that contain the specific rights granted by the customers.

2.5. Security and Risk

3.5.1 Cybersecurity

All participants in Nigeria's Open Banking system are required to comply with minimum security principles, which feature layered security, separation of duties, least privilege, zero trust, dual control, need to know, and privacy principles, as well as to respect the risk-based Cybersecurity Framework of the CBN (CBN, 2022[17]).

In South Africa, according to the FSCA, there are existing conduct frameworks that can help regulate Open Finance activities for certain areas, such as cybersecurity and information security, until a bespoke policy is implemented (FSCA, 2023[6]). For instance, existing policy rules that can support cybersecurity related risks to Open Finance include the draft Joint Standard for Cyber Security and Cyber Resilience Requirements, which intends to support and ensure robust cybersecurity-related risk management practices across financial institutions. These requirements include developing and incorporating a cyber risk management framework, the establishment of a cybersecurity strategy, and cyber security hygiene practices.

3.5.2 Risk Management

As per Nigeria's Operational Guidelines, risks associated with Open Banking can include risks pertaining to cybersecurity, third party involvement, money laundering, data integrity, data privacy, product management , and regulatory and compliance risk (CBN, 2022[17]). The guidelines also recommend an enactment of risk management committee and risk management frameworks for technology risk management, allowing for system security and functionality, and strong authentication measures for protection of data and systems.

In South Africa, the FSCA requires a clear risk management framework or all stakeholders (FSCA, 2023[6]). Such a framework should clearly demand from financial institutions and third-party providers to hold adequate resources for any customer damages ensuing from data breaches, as well as relevant processes and controls for security, data protection, and business continuity. Such measures should also factor in reputational risk.

To prevent risks associated with lower digital literacy, FSCA also proposes disclosure requirements that are in line with the proposed Conduct of Financial Institutions Bill, which accounts for customer information needs (FSCA, 2023[6]). Any disclosures or advertisements should also consider the characteristics of the target market and must assist and promote customer awareness of financial products and services. This is reaffirmed by the NPSD, which underscores the importance of customer literacy for mitigating risks.[6]

[6] It is worth acknowledging that disclosure requirements may not be sufficient to mitigate all digital illiteracy/ low literacy-related risks. Behavioural insights show that consumers may feel overwhelmed and burdened with the amount of information presented to them. Thus, disclosure notices should be clear and effective for allow for end-user comprehension.

2.6. Technical Specifications

2.6.1. API Standards

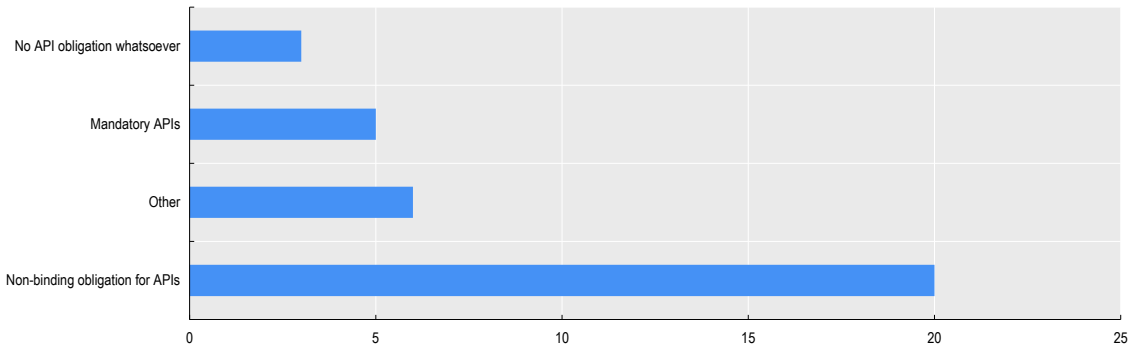
Open Finance APIs enable third party providers to access consumers' transaction data without requiring consumers to share their usernames and passwords. This eliminates the technical challenges associated with screen scraping. Direct connections replace credentials with tokens, resulting in better security, faster speeds, and higher connection success rates (OECD, 2023[1]).

Practices in OECD Countries

Select OECD countries incorporate APIs as a mandatory obligation for banks and other financial institutions to comply with under the data sharing frameworks (e.g., Australia, Brazil, Türkiye). In the UK, the CMA order has enforced a binding obligation on the nine largest banks to implement and uphold specified read and write access APIs. Other banks are subject to more general access requirements under the PSRs that do not mandate APIs. However, the FCA requires the use of dedicated interfaces (which are typically APIs) for certain payment accounts. In practice, many of UK banks adopt the Open Banking APIs as a de-facto industry standard. In Israel, Open Banking is based on NextGenPSD2 standards (OECD, 2023[1])..

Switzerland has issued a recommendation to adopt specific API standards. Likewise, in the US, the Consumer Financial Protection Bureau (CFPB) has issued a set of principles to ensure consumer protection, but there is no mandatory requirement regarding the use of specific technological means. The technology neutral principle in financial regulation, prevalent across most OECD countries, prohibits the imposition of concrete technical specifications, as was the case in the enactment of PSD2 Directive (OECD, 2023[1]).

Figure 2.5. Existence of APIs as a mandatory or non-binding obligation for banks and/or other financial institutions



Note: The report is based on 34 responses to the OECD Survey by 31 OECD countries: Australia, Austria, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, Poland, the Slovak Republic, Slovenia, Korea, Spain, Switzerland, Türkiye, UK, US, as well as by three non-OECD member countries Brazil, Hong Kong (China) and South Africa.
Source: (OECD, 2023[1]).

Practices in SSA Countries

Nigeria's Operational Guidelines advocate for technical API standards and provide two detailed resources for API standards and calls, including "API Identification and Categorisation" and "Voluntary/Involuntary API Standards (CBN, 2022[17]).Technical standards for data sharing interfaces also exist in most OECD countries, as to improve technical compatibility and user friendliness of the services provided (OECD, 2023[1]).

In South Africa, in order to minimise the risks presented by screen scraping, the NPSD consultation paper (NPSD, 2020[8]) recommends creating and regulating a new class of third-party providers, in line with which those practising screen scraping must identify themselves to the Reserve Bank. The objectives of the NPSD paper and FSCA position paper indicate that the existence of an Open Finance framework itself should act as a deterrent against screen scraping by encouraging the use of open APIs. However, they are not made as a mandatory obligation.

According to Kenya's National Payments System Vision and Strategy 2021 – 2025, CBK will work to define API standards and mandate robust and secure data portability for the Kenyan market (CBK, 2020[10]). This will be based on the framework laid down by the Data Protection Act of2019, to ensure appropriate consent management for all aspects of data governance. These standards will include API specifications for identification, verification, and authentication, as well as customer account information and data access, transaction initiation, and format and coding languages for APIs. Thus far, CBK has completed the framework and security review for APIs and is working towards creation of industry-wide standards (CBK, 2020[10]).

2.7. Liability Management and Dispute Resolution

Practices in OECD Countries

Liability provisions are integrated into data sharing arrangements to establish legal clarity regarding accountability in instances involving data access, quality, privacy, confidentiality, processing, sharing, storage, and cybersecurity breaches. Determining liability is a complex process typically handled on a case-by-case basis due to the involvement of various authorities. This complexity arises from the need for consistency with existing data protection regimes and potential contractual arrangements utilised for data sharing, depending on the specific case (OECD, 2023[1]).

The attribution of liability in OECD country data sharing arrangements varies. In Switzerland, the liability depends on the different cooperation models employed (OECD, 2023[1]). For example, if based on outsourcing, the bank or another financial institution granting access to data typically assumes liability. In cases where services are based on a platform or a common offer, liability usually depends on the contractual arrangements in place. In the United States, liability for consumer data privacy and protection is generally addressed through the requirements of the Gramm-Leach-Bliley Act. Regulation P, implementing the GLBA, notes that "the regulation establishes rules governing duties of a financial institution to provide particular notices and limitations on its disclosure of non-public personal information". In Brazil, all regulated and licensed institutions, with all participating institutions being licensed, are held accountable for any issues resulting from non-compliance with these regulations. In Korea, the financial or corporate entity facing an issue bears responsibility, and the consumer protection department of each financial company or corporation is tasked with handling and rectifying customer complaints (OECD, 2023[1]).

In the European Union, these provisions must align with the General Data Protection Regulation (GDPR) and should incorporate details regarding redress options, dispute resolution, and consent granting and revocation mechanisms, according to the general framework, extending beyond the options provided by a

particular data controller or data processor (OECD, 2023[1]). Alongside establishing liability provisions, the Open Finance frameworks should facilitate and empower contractual agreements. These contracts are essential for addressing any gaps in new use cases or specialised scenarios that may necessitate additional clarity on the legal, technical, and other conditions governing data sharing (OECD, 2023[1]).

Provisions related to liability should also encompass a framework for handling complaints, as well as mechanisms for redress and dispute resolution. Regarding complaints handling, in most instances, customers have the option to lodge complaints with either the data source entity (AISP) or the third-party service provider. In Mexico, financial institutions and authorised third parties that violate data sharing requirements stipulated by law or regulation are held liable for such breaches and may face penalties from the relevant financial authority. In such cases, financial authorities possess the legal authority to suspend information sharing, issue observations, and enforce corrective measures to ensure the integrity of the information and compliance with the legal and regulatory framework. Customers and affected third parties can report instances of violation by banks and other financial institutions to the relevant financial authority, enabling the authority to conduct supervisory activities, confirm the violation, and impose the respective penalties (OECD, 2023[1]). Individuals may also issue separate complaints to data protection authorities (DPAs in case of the EU Member States), in which they may detail data protection infringements caused by specific entities. DPAs may then impose fines on the entities found to be in breach of the data protection regulations. In case of severe violations of obligations enumerated under Art.83 (5) GDPR, DPAs may impose fines of up to 20 million euros or 4% of global turnover of an undertaking, whichever is higher.

Practices in SSA Countries

Dispute resolution is well documented in both Open Banking/Finance frameworks for Nigeria and South Africa. Rules for complaint mechanisms, liability management, and dispute resolution have also been established in Nigeria's Operational Guidelines (CBN, 2022[17]). All participants are required to establish procedures for handling dispute resolutions, in which complaints should be acknowledged within 24 hours and resolved within 48 hours.

For disputes between participants, dispute resolution processes and timelines must be outlined in Service Level Agreements (CBN, 2022[17]).If the resolution is not satisfactory or if the dispute agreement is breached the participant may refer the dispute to the CBN jurisdiction. Similarly, customers can escalate issues to the CBN if the complaint has not been satisfied within 14 days, as long as the complainant has already exhausted all the internal dispute resolution avenues, the issue has internally been marked as resolved, and if it is not under litigation or being adjudicated upon by a court of law.

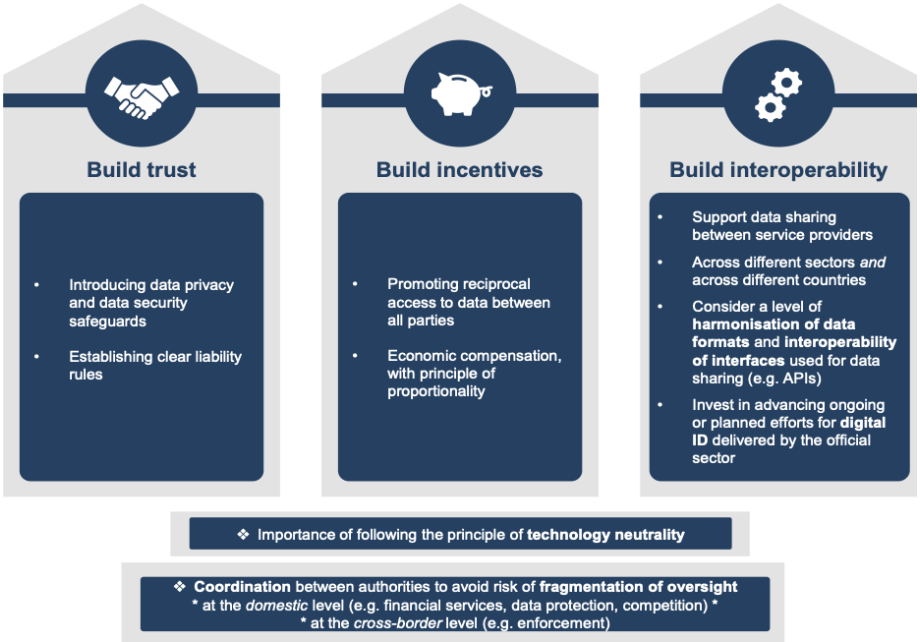
In South Africa, the South African Reserve Bank recommends the introduction of mechanisms for dispute resolution and liability management; however, according to FSCA, there are existing conduct frameworks available to financial institutions, such as the General Code of Conduct under the Financial Advisory and Intermediary Services Act, for managing statutory complaints that can be extended to matters related to Open Finance (NPSD, 2020[8]; FSCA, 2023[6]).The proposed Conduct of Financial Institutions Bill outlines obligations with respect to customers, such as ensuring there are no barriers to filing a complaint, having a complaints management process and external dispute resolution mechanisms in place. The FSCA is in the process of developing a harmonised framework under this bill that would apply to all financial institutions and is considerate of matters related to Open Finance. When a financial institution is unable to resolve a complaint, either the relevant Ombudsman scheme or the statutory Ombudsman take over the complaints resolution, until National Treasury reforms are complete.

3 Policy considerations

In OECD countries, there are two main design approaches to the data sharing frameworks: the market-led approach or voluntary framework (e.g. Japan, US, Switzerland), and the more prescriptive or mandatory approach where data sharing is imposed by regulation (e.g. EU PSD2). In Africa, this report identified examples of both, with Nigeria's voluntary approach and South Africa's incrementally mandatory approach. Each of the approaches fits the idiosyncrasies of the corresponding economies and is considered equally effective in delivering the objectives of such frameworks.

Nevertheless, it is necessary to consider shared pillars to ensure that countries that have operating frameworks, are currently developing frameworks, or are yet to introduce Open Finance or Banking frameworks into their regulatory strategies are fully equipped with the resources needed to expand the benefits and minimize the risks associated with Open Finance. A phased approach with an extensive consultation of stakeholders could be considered by jurisdictions planning an Open Finance framework, for a smoother, gradual expansion towards cross-sectoral data sharing. Cost-benefit analyses may be considered where policy makers opt for intervention through policy action to promote such transition (OECD, 2023[2]).

Figure 3.1. Pillars for successful implementation of Open Finance data sharing frameworks



Source: OECD (2023), "Open Finance policy Consideration".(or (OECD, 2023[2]))

3.1. Build trust

As highlighted in this report and previous OECD research, the implementation of comprehensive privacy and data protection safeguards is crucial to the success of Open Finance. Establishing measures for data protection and security is crucial to effectively safeguard personal data, instil a sense of control among users, and thereby cultivate consumer trust. This involves clearly delineating roles in accordance with data protection rules, such as designating "data controllers" and "data processors," as per the terminology adopted by some legislations, and assigning responsibilities aligned with principles like purpose limitation, data minimisation, data retention, privacy by design and by default, accountability, and data security, as outlined in international standards. The OECD Privacy Guidelines and the G20/OECD High-Level Principles on Financial Consumer Protection provide reliable guidance to policy makers in this respect. Privacy-enhancing technologies can complement organisational and legal measures, enabling data processing and analysis while preserving the confidentiality, and in certain cases, the integrity and availability of the data. Moreover, achieving consistency between data protection laws and Open Finance frameworks at the national level is essential to offer legal certainty, transparency, and trust in the development of Open Finance solutions (OECD, 2023[2]).

Consumer education plays a role in fostering trust among consumers, aligning with the promotion of privacy and data protection. By raising awareness, consumer education can influence the implementation and adoption of Open Finance data sharing frameworks. Some consumers might be hesitant to share their data or may not comprehend the products and services offered if they lack awareness of the safeguards in place to protect them. Lack of awareness may also affect the success of adoption of other digital tools, such as digital IDs) (OECD, 2023[2]).

Formal consent plays a central role in Open Finance as it allows users to control the flow of their financial data. For it to be considered unequivocal and freely given, users must be provided with an appropriate level of information, communicated in a clear and comprehensible language. However, consent has its limitations and practical challenges. Namely, consent management and data dashboards can ensure compliance with data protection requirements. Consent, although pivotal, is just one facet of a broader privacy and data protection architecture that should be encompassed by Open Finance. This architecture should also acknowledge the rights of data subjects over their data, such as the rights to receive information, the right to object to the processing of their data, and to revoke consent at any point in time (OECD, 2023[2]).

Trust is a particularly critical pillar for emerging market and developing economies such as those present in Africa. Given the opportunity of Open Finance to expand access to credit and increase the number of FinTech lending firms, recent experiences with small-value digital consumer credit and buy-now-pay later products suggest that mitigating consumer protection risks must become an important consideration for African governments. Such risks can include predatory contract terms, lack of product suitability, aggressive marketing, multiple borrowing and therefore high levels of debt, and inaccurate or outdated information, and often stem from reduced financial literacy In this light, strengthening consumer protection measures, liability rules and dispute resolution mechanisms will be critical as Open Finance also helps to scale lending activity (Mazer, 2023[5]).Open Finance can be a particularly useful opportunity for strengthening the enforcement of consumer protection claims departments in financial sector authorities that may be currently not prioritised. To enhance consumer protection, the level of coordination across relevant consumer protection related authorities and staff needs to be enhanced, along with improving technological capacity and mechanisms for detection of risks (Mazer, 2023[5]).

3.2. Build incentives

The right incentives need to be in place for participants in Open Finance frameworks, to counter the costs that incumbents may need to pay for the development and maintenance of APIs or other connecting interfaces for data sharing. Additionally, these incentives help cover the general system upgrades necessary to enable the sharing of data in digital formats suitable for such infrastructure. Examples of potential incentives may include reciprocal data sharing or economic compensation. Reciprocal access to customer data is present in a minority of OECD countries where data sharing arrangements are in effect. Without reciprocity, banks and other incumbent firms have less motivation to invest in delivering infrastructures such as APIs. Even when regulatory requirements mandate data sharing and the provision of such infrastructure, the absence of commercial incentives may lead to malfunctioning or underperforming of data sharing infrastructure or its lack of maintenance. FinTechs have reported both of these sub-optimal outcomes anecdotally as issues hindering their access to data under existing arrangements (OECD, 2023[2]).

In order to achieve these goals, promoting reciprocal access to data among all parties within Open Finance ecosystems may be necessary. Policymakers in jurisdictions where mandatory data sharing is free of charge could explore the possibility of allowing economic compensation under fair compensation schemes. This approach aims to equitably distribute costs among participants while preserving competition. It should incorporate the principle of proportionality to avoid hindering smaller firms from accessing data and to guard against anti-competitive behaviours. Furthermore, relevant policies and data sharing frameworks should be designed to deliver tangible benefits to individual users, intending to incentivise uptake and maximise the success of such frameworks. Offering financial or other benefits should significantly enhance the willingness to share payments data (OECD, 2023[2]).

In the SSA context, proportionality and incentives to participate in Open Finance frameworks are necessary for smaller FinTech companies and startups that may not be otherwise able to afford to financially compensate commercial banks for gaining access to customer data. Effectively expanding the benefits of Open Finance in this region will require understanding of the unique financial constraints faced by African startups that may not be as salient in many OECD countries. However, data reciprocity and proportionality should be considered best practices regardless of the economic context.

3.3. Build interoperability

Coordination is essential among authorities overseeing various aspects of Open Finance activities, especially considering the cross-sectoral nature of these frameworks. This is crucial to prevent the fragmentation of oversight, which may arise due to the involvement of multiple authorities such as financial supervisors, data protection authorities, and competition authorities. Establishing collaboration protocols for information exchange and cooperation among the authorities involved in Open Finance frameworks may be considered. Additionally, further analysis is required to address the emergence of new entrants offering both financial and non-financial services or operating outside the scope of financial supervision (OECD, 2023[2]).

Furthermore, international coordination becomes crucial for overseeing cross-border data sharing activities. Coordinating at the cross-border level presents challenges across legal aspects (liability, property rights over data), technical dimensions (different data standards, variations in data vocabularies due to language differences), and enforcement levels (potential differences in legal frameworks, issues with designating jurisdiction and competent authorities). The OECD has an existing Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy (OECD, 2007[23]), and its ongoing review will also address cross-sectoral aspects. This is essential to maximise the convergence and interoperability of these frameworks (OECD, 2023[2]).

The long-term success of Open Finance may depend on the level of interoperability achieved, capable of supporting data sharing between service providers across different sectors and countries. Achieving this interoperability requires some degree of harmonisation of data formats and the interoperability of interfaces used for data sharing, such as APIs. Currently, interoperability is facilitated through the utilisation of API aggregators, which integrate various APIs and offer a single implementation point for TPPs. However, this approach also poses risks related to market dominance in terms of safeguarding the competitive dynamics (OECD, 2023[2]).

The development of standardized APIs could be initiated by the industry, supplemented by a mechanism for National Competent Authorities (NCAs) to potentially offer guidance and steer its development. This approach aims to contribute to a more defined legal framework for industry compliance. In the absence of API standards, firms participating in such ecosystems must connect and integrate various APIs, a process that can be both technically complex and require an investment in time, cost, and technical capabilities that may not be readily available to smaller players, such as SMEs and FinTech start-ups. The inability to integrate different APIs may hinder their ability to access data, thereby preventing them from reaping the benefits of such frameworks (OECD, 2023[2]).

Policymakers might also consider endorsing initiatives to assess the impact of data sharing frameworks, recognizing the inherent difficulty in quantifying the ultimate impact on innovation, competition, and value-added services resulting from data sharing. Currently, measurement typically relies on direct or intermediate impact indicators, such as API calls, the number of TPP licenses issued, and the number of consumers who claim to have utilised Open Finance-related services. As an initial step, policymakers could encourage entities obligated to provide data to report activity based on API calls (including the type of API, duration of sharing, and data recipient). This step aims to create a comprehensive map of the data sharing landscape, providing a foundation for further impact analysis. Such analysis could also assist in determining which sub-sectors of Open Finance-type arrangements would derive the greatest benefits based on cost-benefit analyses (OECD, 2023[2]).

Fragmentation of oversight between both sectors and countries can be harder to avoid in the SSA context due to its diverse regulatory landscape and varying levels of technological readiness/infrastructure based on the size of the economy. This can also be a result of lack of standardized protocols and lack of resources for regulatory bodies. Avoiding such risks will require expansion of identification systems across the region as well as the development of protocols and standards that are harmonized across different contexts.

References

Agpaytech (2022), *Is Ghana Ready For Open Banking?*, https://www.agpaytech.com/pdf/ghana.pdf. [11]

Amadou, S. (2019), "Fintech in Sub-Saharan Africa: A Potential Game Changer", *IMF*, https://www.imf.org/en/Blogs/Articles/2019/02/14/fintech-in-sub-saharan-africa-a-potential-game-changer (accessed on 15 October 2023). [3]

Bank of Ghana (2019), *Payment Systems Strategy 2019 - 2024*, https://www.bog.gov.gh/news/payment-systems-strategy-2019-to-2024/. [13]

Bank of Mauritius (2023), *MauCAS | Bank of Mauritius*, https://www.bom.mu/maucas-0 (accessed on 12 October 2023). [15]

CBK (2020), *Kenya National Payments System Vision and Strategy 2021 - 2025*, Central Bank of Kenya, https://www.centralbank.go.ke/wp-content/uploads/2020/12/CBK-NPS-Vision-and-Strategy.pdf (accessed on 24 August 2023). [10]

CBN (2023), *Issuance of the Operational Guidelines for Open Banking in Nigeria*, Central Bank of Nigeria, https://www.cbn.gov.ng/Out/2023/CCD/Operational%20Guidelines%20for%20Open%20Banking%20in%20Nigeria.pdf (accessed on 22 August 2023). [12]

CBN (2022), *Operational Guidelines for Open Banking in Nigeria*, https://www.cbn.gov.ng/Out/2022/CCD/OPERATIONAL%20GUIDELINES%20FOR%20OPEN%20BANKING%20IN%20NIGERIA_APPROVED%20EXPOSURE%20DRAFT.pdf. [17]

CBN (2021), *Circular on the regulatory framework on open banking in Nigeria*, https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf (accessed on 14 December 2023). [16]

CBN (2021), *Circular on the regulatory framework on open banking in Nigeria*, Central Bank of Nigeria, https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf (accessed on 14 December 2023). [30]

Central Bank of Kenya (2020), *Kenya National Payments System Vision and Strategy 2021 - 2025*, https://www.centralbank.go.ke/wp-content/uploads/2020/12/CBK-NPS-Vision-and-Strategy.pdf. [22]

Central Bank of Nigeria (2023), *Issuance of the Operational Guidelines for Open Banking in Nigeria*. [27]

Central Bank of Nigeria (2022), *Operational Guidelines for Open Banking in Nigeria*, https://www.cbn.gov.ng/Out/2022/CCD/OPERATIONAL%20GUIDELINES%20FOR%20OPEN%20BANKING%20IN%20NIGERIA_APPROVED%20EXPOSURE%20DRAFT.pdf (accessed on 22 August 2023). [26]

FSCA (2023), "Draft Position Paper on Open Finance". [25]

FSCA (2023), "Draft Position Paper on Open Finance", https://www.fsca.co.za/Regulatory%20Frameworks/FinTechDocuments/Draft%20Position%20Paper%20on%20Open%20Finance.pdf (accessed on 15 August 2023). [6]

FSCA (2020), *Regulating Open Finance Consultation & Research Paper*. [9]

FSCA (2020), *Regulating Open Finance Consultation & Research Paper*, https://www.fsca.co.za/Documents/Regulating%20Open%20Finance%20Consultation%20and%20Research%20Paper.pdf (accessed on 24 August 2023). [29]

Government of Rwanda (2022), *Rwanda Fintech Strategy 2022 - 2027*, Ministry of ICT. [28]

Government of Rwanda (2022), *Rwanda Fintech Strategy 2022 - 2027*, Ministry of ICT, https://www.fsa.go.jp/en/news/2023/20230626.html (accessed on 6 October 2023). [18]

Government of Rwanda (2021), *Rwanda Fintech Policy 2022-2027*, Ministry of ICT. [19]

Government of Rwanda (2021), *Rwanda Fintech Policy 2022-2027*, Ministry of ICT, https://www.minict.gov.rw/index.php?eID=dumpFile&t=f&f=41305&token=4bcac6970c5d433ff070e4b9c25bb346763debed (accessed on 6 October 2023). [14]

Gray, J. et al. (2022), *Open finance: Prerequisites and considerations for fit-for-context implementation in Africa*, Cenfri, https://cenfri.org/publications/open-finance-prerequisites-and-considerations-in-africa/. [21]

Mazer, R. (2023), "Consumer protection for open finance ecosystems", https://www.raidiam.com/wp-content/uploads/2023/05/Consumer-Protection-for-Open-Finance.pdf. [5]

Mazer, R. (2023), "Moving markets towards open finance: Policy considerations for emerging markets and developing economies", https://www.raidiam.com/wp-content/uploads/2023/05/Moving-Markets-Toward-Open-Finance.pdf. [20]

NPSD (2020), *Consultation paper on open-banking activities in the national payment system*, National Payment System Department, South African Reserve Bank, https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight/Consultation%20Paper%20on%20open%20banking.pdf (accessed on 2 September 2023). [8]

OECD (2023), *Open finance policy considerations*, https://www.oecd.org/publications/open-finance-policy-considerations-19ef3608-en.htm. [2]

OECD (2023), *Shifting from open banking to open finance*, https://www.oecd.org/publications/shifting-from-open-banking-to-open-finance-9f881c0c-en.htm. [1]

OECD (2007), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352 (accessed on 14 December 2023). [23]

OECD (2007), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352 (accessed on 14 December 2023). [31]

South African Reserve Bank (2020), *Consultation paper on open-banking activities in the national payment system*, National Payment System Department, https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight/Consultation%20Paper%20on%20open%20banking.pdf. [32]

World Bank (2023), *From Connectivity to Services: Digital Transformation in Africa*, https://www.worldbank.org/en/results/2023/06/26/from-connectivity-to-services-digital-transformation-in-africa. [7]

World Bank (2023), *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*. [24]

World Bank (2023), *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*, https://www.worldbank.org/en/publication/globalfindex/Report (accessed on 15 October 2023). [4]