Consumer protection for open finance ecosystems

Fair Finance Consulting

Consumer protection and competition research and advisory services

Rafe Mazer, Director, Fair Finance Consulting

April, 2023[1]

[1] This work was produced with the support of the Bill & Melinda Gates Foundation. All opinions are solely those of the author.

Table of Contents

Consumer protection for open finance ecosystems

Rafe Mazer, Fair Finance Consulting | April, 2023

Consumer protection and market conduct supervision is an essential ingredient to any financial ecosystem. Where consumers are protected, they are more likely to trust and use financial services. Where providers are held to high standards of conduct, abusive practices such as excessive fees, fraud, or improper financial advice can be more effectively reduced and mitigated. This in turn encourages providers to compete equally on the quality of their services and customer experience.

An emerging approach to improve competition in financial services is to provide consumers more control over their financial information so that they can share this information with financial service providers, increasing competition and consumer choice—often referred to as "open finance."

As documented in the companion piece to this report, *Moving Markets Towards Open Finance: Policy considerations for emerging markets and developing economies (EMDEs)*, new models for consumer-led data sharing are expanding across the globe. These models can bring important benefits for consumers and financial sector innovation. **However, like all financial innovations, open finance brings risks which need to be identified and address. In particular, the wide range of financial and non-financial institutions serving consumers and handling their data in open finance ecosystems requires robust market conduct and consumer protection supervision.** This report identifies several emerging risks related to open finance, and proposes ways in which these risks can be measured, monitored, and mitigated against by leveraging the data available in open finance ecosystems. The report begins by discussing the primary consumer protection concerns in open finance, and then proposes several methods and data sources for monitoring consumer protection and market conduct in open finance, before concluding with a call to action for policy markets to implement consumer protection policies for open finance early on.

I. Consumer protection and market conduct supervision remains underdeveloped in open finance

Conversations with implementers of open finance and similar data-sharing models across the globe indicate consumer protection frameworks for open finance are relatively underdeveloped. While the newness of these models means there is not much documentation of good practices in consumer protection for open finance, we can learn initial market-level experiences to develop appropriate consumer protection policies. Through a review of open finance models, several key consumer protection and conduct risks have been identified, and are discussed in this report:

1. Lack of transparency and accountability in use of consumer data
2. Complex menus and intentional friction in the user experience
3. Consumer-affecting fraud
4. Inadequate complaints handling and dispute resolution for multi-party transactions
5. Lack of clear liability frameworks

6. Exclusion due to biased data
7. Unfair treatment and lack of product suitability

This section reviews and presents examples related to each of these risks, as well as indicative policy approaches being implemented in data-sharing ecosystems to address these risks. The following section then considers possible metrics and data sources for monitoring and mitigating these risks.

1. Lack of transparency and accountability in use of consumer data

One of the motivations for open finance regimes is to improve data usage transparency within financial services. Without a formal regime with standards for data usage, sharing, and destruction, firms may share consumers' data in ways that the consumer did not intend or believe they were authorizing. Through open finance, providers are held to enhanced standards to inform consumers on the usage of their data, seek period reauthorization for account and data access, and rules regarding whom the data may be shared with and for what purpose.

Ensuring that these data trails can be easily monitored by the data subject, that providers document consent and follow data protection standards fully, and that there are clear limitations on use of data, is an essential supervisory aspect of open finance to reduce the risks of data misuse. Medine and Plaitakis argue that "basic data protection provisions must be in place to create a safe and sound open finance regime" and caution against pursuing open finance policies in EMDEs where data protection policy is underdeveloped. [2] Without provisions such as data minimization, clear consent policies, or the right to revoke data usage permissions, consumers in open finance will be left vulnerable to significant risks of harm and misuse of data.

Data protection is not a focus of this report, as there is already a robust literature and range of experiences on data protection, including in open finance which can be referred to. However, data protection is the first key consumer protection risk listed here because of its singular importance to a safe and trustworthy open finance ecosystem. Just as data protection policies are a pre-requisite to open finance policy, monitoring of consumer control of their data, the ability of consumers to understand usage of their data, and providers' adherence to responsible data practices and data sharing limitations is an essential part of any consumer protection supervision approach for open finance.

2. Complex menus and intentional friction in the user experience

Mandating some minimum level of market participation and data types in open finance can be a useful strategy in many emerging markets, where the banking or payments sectors are highly concentrated. Putting in place a mandate does not however ensure that data-sharing will function well for the consumer. **Conversations with several authorities involved in open finance ecosystems raised concerns that some financial institutions may add in intentional friction or downgrade functionality either due to conservatism that leads to "overcompliance" with rules, or to forestall usage of open banking by their customers and the third-party providers the customers seek to provide access to.** Some of the common tactics employed to increase friction and discourage usage include:

[2] See, for example, Medine, David and Plaitakis, Ariadne. 2023. [Combining Open Finance and Data Protection for Low-Income Consumers](). CGAP

1. **Security scare tactics**. Financial institutions have used additional prompt messages to emphasize or exaggerate security risks for consumers sharing their data with another participant in the open finance regime. One regulator described prompts after consent that ask things like "are you sure you want to share your account's data with this provider?" While informed consent and clear articulation of security risks are important, there is a sense that sometimes incumbent firms will add extra security prompts or questions to play up potential risks and reduce the propensity of consumers to port their data to another open finance participant.
2. **Excess screens or steps**. Open finance supervisory authorities noted cases where financial institutions develop overly complex procedures for their customers to complete data sharing or payment initiation functions with third parties. One former regulator recalled a bank which had 15 click through screens and then routed customers to their call center to answer security questions in order to use open finance services.
3. **Failed and flawed transactions**. Making APIs either unavailable or poor performing can reduce consumers' likelihood to use data sharing or payment initiation APIs. In Europe, response times from banks on open banking APIs have been reported to take as long as 18 seconds,[3] while poor availability of bank APIs was common in the early stages of the UK's Open Banking,[4] although recent data indicates this has improved.[5]
4. **Inaccurate or incomplete information.** In January, 2023, the UK's Competition and Markets Authority sanctioned HSBC Bank for publishing inaccurate information, or not publishing required information through its Open Data APIs on more than 50 occasions. This included, "incorrect information related to fees, charges and rates, as well as to eligibility criteria and features and benefits of accounts and loans. The failures varied in length, with the longest lasting from 2017 to 2022."[6] Financial service providers in EMDEs have been found to omit information to steer consumers away from certain products[7], and open finance models appear to carry similar risks that providers may use omission or inaccuracy of information to limit the use of new products or services that run counter to their firm's interests.

3. Consumer-affecting fraud

The digitization of financial services has unfortunately also led to new consumer-facing fraud risks in financial services. These risks include phishing scams, unauthorized account access, fraudulent product offers, and push-payment fraud (a growing fraud type which accounted for 44% of all financial fraud losses in the UK in 2021).[8] These fraud risks are present in open finance, which facilitates sharing of sensitive information, payment initiation, account opening, and provides access to accounts to execute transactions. As Mike Haley argues in his discussion of open banking security risks, "there are no new fraud types created by Open Banking but there will be new opportunities for fraudsters."[9]

---

[3] Nicole Green. "Yapily's recommendations for minimum open banking requirements in the EU." Yapily.

[4] Alex Rolfe. "UK Open Banking initiative stalling due to bank led outages." May 23, 2019. Payments Industry Intelligence

[5] Open Banking API Performance Data

[6] CMA takes action against HSBC for breaching Part 2 of the Retail Banking Order. January 19, 2023. Competition and Markets Authority

[7] See for example Gine and Mazer, 2016 and Mowl and Boudot, 2014.

[8] Annual Fraud Report. 2022. UK Finance.

[9] Mike Haley. Security & Fraud: Is open banking creating new challenges? Jun 27, 2022. Open banking Excellence.

Managing fraud risks was also one of the key gaps identified in "The Future Development of Open Banking in the UK," the final report prepared by the Joint Regulatory Oversight Committee for Open Banking in the United Kingdom.[10]

There are opportunities for data-sharing models to reduce fraud vulnerabilities in certain cases[11], including where secure connections between credentialed open finance participants reduce the need for providers to use screen scraping. Under open finance regimes, consumers provide consent for a specified, limited purpose usage directly to the account holder, who then securely transfers only the necessary information to the third party. This may be why the OECD Open Finance Survey found only one country reporting occurrences of data misuse due to data sharing frameworks, and in fact noted that "The reported case of data misuse is associated with a firm that collected and stored data based on screen scraping and which was found to be in violation with data protection requirements."[12]

Open finance systems can also mitigate and reduce fraud through sharing of data such as KYC records and increased tracking and sharing of data on fraud risks and fraud attempts. In the United States, FDX has created a fraud reporting endpoint which it's members can use to share fraud incidences as they occur.[13] If a third-party app sees evidence of suspicious activity on a bank account that may indicate a planned fraud attempt, the app can use FDX to send a message directly to a fraud endpoint of the bank, detailing which app, customer, and account, and the fraud indicators identified. This streamlines fraud monitoring and increases the probability the fraud is reported to the right contacts within the bank, who are likely the ones responsible for monitoring that fraud endpoint. FDX plans to enhance this feature in the future by adding the ability to then communicate to all apps connected to this bank account so they can take appropriate security measures.

In the United Kingdom, Pay.UK and the industry have worked to improve fraud data sharing, established Confirmation of Payee name-checking to prevent push payment scams, and launched a Mules Insights Tactical Solution (MITS), a new technology that helps to track suspicious payments and identify money mule accounts which are used to receive payments for push payments fraudsters.[14] Also in the UK, the Financial Conduct Authority (FCA) "is considering promoting the sharing of fraud data between account providers to facilitate early detection and prevention of fraud cases"[15], which aligns with the recommendations for fraud incidence data sharing made in the "The Future Development of Open Banking in the UK" report referenced above.[16] **Solutions like FDX's fraud endpoint and information-sharing requirements like what the United Kingdom is developing can help to improve fraud monitoring and reporting in open finance regimes, which can in turn help to develop better fraud prevention and harm reduction solutions**, which are discussed in the section of this report on consumer protection supervision models for open finance.

---

[10] The Future Development of Open Banking in the UK: Final report for the Joint Regulatory Oversight Committee. February 2023. Open Banking Strategic Working Group Secretariat.
[11] Report 2022: The Enablers of Open Banking, Open Finance, and Open Data. November, 2022. The Paypers.
[12] OECD. Shifting from Open Banking to Open Finance: Results from the 2022 OECD survey on data sharing frameworks. 2023. OECD Business and Finance Policy Papers, OECD Publishing.
[13] The Paypers. 2022.
[14] UK Finance. 2022.
[15] OECD. 2023.
[16] Open Banking Strategic Working Group Secretariat. 2023

4. Inadequate complaints handling and dispute resolution for multi-party transactions

Open finance models often increase the number of actors involved in financial transactions and data transfers, and introduce new types of actors—e.g. account aggregators—into financial services. Where multiple actors and multiple systems interact, the potential for failures may increase. **When multiple parties are involved in a failed transaction or other consumer dispute, determining where to seek restitution can be more complicated than in a bilateral firm-customer relationship.**

Most policymakers appear to recognize the importance of redress frameworks for open finance regimes, and have set standards for access, quality, and supervision. In Chile, for example, the Fintech Law requires that all the various participating institutions in open finance be responsible for attending and resolving consumer complaints related to both data use and services provided.[17] In India, Sahamati's code of conduct allows for citizens and account aggregator participants to choose from a range of dispute resolution mechanisms, including the Reserve Bank of India ombudsman, an Online Dispute Resolution (ODR) agency empaneled by Sahamati (to be piloted starting in March, 2023), or "any other legal mechanism of its choice."[18] According to Sahamati leadership, the ODR is an important addition to typical redress channels, because the ecosystem counts with participants who are under different regulatory oversight, which could create challenges for resolving disputes through traditional regulatory channels. Other countries have similarly set up new complaints handling bodies for open banking. As the World Bank notes: "In Japan, the Association for Electronic Payment Services, a private body, is responsible for handling customer complaints related to open banking. In Singapore, the Personal Data Protection Commission facilitates the complaint between the customer and the provider."[19]

In some cases, there may be existing redress provisions which could be applied explicitly to the data sharing ecosystems. The Central Bank of Nigeria's (CBN) Operational Guidelines for Open Banking stipulate that "Participants shall abide by the dispute resolution mechanism laid down under 'Liability Management, Customer Complaint and Redress Management' of the Customer Experience Standards (Appendix IV) as well as the CBN Consumer Protection Framework."[20] The CBN already monitors the quality of dispute resolution in the banking sector through the Customer Complaints Management System, and by applying this framework to the open banking regime, the CCMS system could be leveraged for complaints monitoring in open banking as well. At the same time, the CBN recognizes the need for enhancements of the complaints handling framework to address the multi-party nature of open banking models. The Regulatory Framework for Open Banking in Nigeria (2021) requires that all API users "Maintain customer service/complaint desk on 24 hours/7 days a week basis for financial institutions to resolve complaints of end-users."[21] This stipulation reduces the risk that a financial institution would be unable to swiftly raise and resolve an issue with a third-party provider (such as an aggregator) on behalf of their customer.

[17] Article 24. Ley 21.521 (Ley Fintec). January 4, 2023. Ministerio del Interior y Seguridad Pública. Gobierno de la República de Chile.
[18] Community Guidelines in the Sahamati AA Ecosystem. August 31, 2022. Sahamati Foundation.
[19] Technical Note on Open Banking: Comparative Study on Regulatory Approaches. 2022. World Bank Group.
[20] Operational Guidelines for Open Banking in Nigeria. March, 2023. Central Bank of Nigeria.
[21] Regulatory Framework for Open Banking in Nigeria. February, 2021. Central Bank of Nigeria.

5. Lack of clear and consumer-friendly liability frameworks

A common concern for open finance experts interviewed was the challenge of assigning liability for the risks open finance brings, including: Failed or fraudulent transactions, improper charges or fees, and misuse of consumer data. **Carr, et al (2018) cite two primary liability challenges for open banking regimes: Non-regulated financial institutions may not have to hold operational risk capital—which can be used to make consumers whole—and "the involvement of different parties in the flow of data or in the initiation of transactions raises the issue of how to assign liabilities between the banks and the third parties, and how to resolve potential disputes between them."**[22] To address these liability challenges they propose placing responsibility on the party where the transaction took origin, and developing streamlined dispute resolution procedures between open finance entities, including between financial institutions and third-party service providers.

Policymakers should establish clear liability frameworks which limit the burden of resolution imposed on the consumer, and create clear processes for resolution between participating firms. Surprisingly, clear liability rules are not as common as would be expected: The OECD survey on Open Finance found that only 17 of 31 responding jurisdictions reported having liability rules for sharing of incorrect, outdated, or otherwise inappropriate data.[23] But there are good practices emerging. In Mexico, for example, both financial institutions and authorized third parties are held liable when they breach data sharing requirements. Further, the Fintech Law in Mexico gives financial sector authorities the ability to penalize these actors through measures such as suspending information sharing or imposing corrective actions. Policymakers should aim to provide clear liability rules around at least two aspects of open finance frameworks:

1. Resolution of failed transactions and other consumer disputes. Some open finance regimes require the consumer to be made whole swiftly and separate from the resolution of liability between the commercial actors involved in the transaction. In the United Kingdom when a payment initiation services provider (PISP) conducts an unauthorized or otherwise incorrect transaction, the account servicing payment service providers (ASPSPs) must provide a refund to the consumer, and can separately seek compensation from the PISP. Australia's Consumer Data Right makes the principal jointly responsible for dispute resolution in relation to any of its affiliates, to support adequate complaints handling even where third parties are involved in a transaction.[24]

2. Conduct of third-party actors in open finance ecosystems. The levels of access to data, accounts, and roles of open finance participant types varies considerably across countries. In all cases though, a clear definition is needed of how much principals (e.g. banks) are responsible for the conduct of third parties they enter into commercial agreements with. In Australia, the Consumer Data Right (CDR) framework was amended in 2021 to establish a "CDR representative model," which "allows eligible participants to access the CDR and use data without the need for accreditation in circumstances where they offer CDR-related services to consumers as a representative of an accredited data recipient."[25] This means that

[22] Brad Carr, Pablo Urbiola, and Adrien Delle-Case. Liability and Consumer Protection in Open Banking. September, 2018. The Institute of International Finance, Inc.
[23] OECD. 2023.
[24] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021. 1.16.A., Explanatory Note. 2021. Australia Minister for Superannuation, Financial Services and the Digital Economy.
[25] Australia Minister for Superannuation, Financial Services and the Digital Economy. 2021.

accredited persons—those holding CDR-relevant data such as customer data—can now sponsor the participation of third parties—referred to as "affiliates"—that engage with the data the sponsor holds on consumers.

To ensure consumer protection in the sponsored affiliates model, Australia requires sponsors have in place a third-party management framework before they can sponsor any third-party participants, provide any necessary training or assistance to the affiliate before and during a sponsorship agreement, and "take reasonable steps" to ensure that their affiliates comply with their obligations in the CDR. To ensure that both affiliates and sponsors are liable for proper data use, the framework stipulates that "any data collected by a sponsor at the request of an affiliate is deemed to have also been collected by the affiliate" which "ensures the limitation to permitted uses and disclosures applies to affiliates when they have used their sponsor to collect data from data holders."[26]

The sponsors are also expected to update the Data Recipient Accreditor of new, suspended or terminated affiliates within five business days of such a change. Both the sponsor and affiliate must report to the authorities every six months on several key metrics:[27]

Sponsor reporting requirements	Affiliate reporting requirements
▪ Number of consumer data requests made on their behalf and on behalf of affiliates ▪ Number of consumer data requests received from both affiliates and accredited persons ▪ Number of sponsorship arrangements to which it was a party during the period	▪ Number of consumer data requests made to its sponsor and other accredited persons ▪ Number of consumer data requests received from accredited persons ▪ Number of sponsorship arrangements to which it was a party during the period

Other jurisdictions, such as Switzerland, vary liability depending on the nature of the arrangement. As the OECD survey reports, "In Switzerland, the liability depends on the different co-operation models that can be used. For example, if based on outsourcing, it is usually the bank (or another financial institution granting access to data) that is held liable. If the services are based on a platform or a common offer, it usually depends on the contractual arrangements."[28] The South African Reserve Bank's "Consultation paper on open-banking activities in the national payment system" proposes a different approach for third-party liability, expecting "third-party providers" (e.g. fintech companies) to "bear the risks and costs that they introduce to consumers."[29] Finally, the European Union, in it's "Report on Open Finance" distinguishes between liability arrangements when the liability relates to a contractual agreement for data exchange, versus provisions regarding data exchange which are covered under legislation. The important distinction made here is between a data exchange that is voluntary as part of a commercial relationship, and a data exchange that is mandatory, as part of compliance with data sharing rules. In their view the liability should be reduced for the data provider where the data sharing is not voluntary.[30] This speaks to the risk that, if liability frameworks place too much burden on banks for

---

[26] Australia Minister for Superannuation, Financial Services and the Digital Economy. 2021.
[27] Australia Minister for Superannuation, Financial Services and the Digital Economy. 2021
[28] OECD. 2023.
[29] Consultation paper on open-banking activities in the national payment system. November, 2020. South African Reserve Bank.
[30] Report on Open Finance: Report of the Expert Group on European financial data space. October 2022. European Union.

the conduct of others, they could discourage their participation in open finance and reduce participation.

A clear liability framework with consideration of the various actors in open finance should be part of the initial set of rules and responsibilities set forth in open finance. Determining liability across these actors should not be a burden primarily placed on the consumer, they should be able to initiate a complaint or concern across the various involved parties and receive prompt response and redress. Policymakers will need to think carefully how they design the liability and redress rules for principle actors in open finance like banks and third-parties such as data aggregators so that all actors feel a responsibility to attend to the consumer's concerns, the process for addressing issues is clear across the actors, and reporting requirements for third-party compliance and supervision are clear.

6. Exclusion due to biased data

The use of data on individuals and firms to unlock new opportunities, reduce costs, and improve underwriting is one of the most important potential benefits of open finance, especially for many emerging market economies where reliable data on small enterprises is particularly limited. **At the same time, there are risks that: 1. New information sources may not be accurate and algorithms using this data could unintentionally exclude or discriminate against certain consumer segments; or 2. Certain segments of consumers may not have access to this type of data, which if it becomes considered an essential component of risk assessment, could exclude these consumers from the benefits of the products and services within open finance.** On this second risk, the European Union notes that "From a financial inclusion perspective, some members argue that a data perimeter could be composed with data that everyone is able to provide – if this is not the case, exclusion may arise from the inability of a consumer to provide data, rather than the assessment based on the data provided."[31]

In EMDEs, credit reference bureaus are often relatively underdeveloped and have only limited market coverage, leaving many consumers without a formal credit history. **New data sources integrated into open finance should take care to include data that can support expanded access for these currently "data-thin" populations. They must also try not to deepen exclusion by limiting access for consumers based on data types they may not have, but which are not yet well-proven to be useful for risk management.** As the State of India's Digital Economy report cautions, "given that they are often built on each other, if an individual gets left out of a foundational DPIP [Digital Public Infrastructure and Platform], the risk is that they would get excluded from an entire ecosystem. Universal connectivity and access to digital technologies are the starting point to leverage DPIPs. Those without access to these run the risk of exclusion. Such exclusions can in turn exacerbate preexisting gender, regional or income divides."[32]

One of the challenges emerging markets may face is a wide-ranging degree of digitization and technical readiness of different financial service providers to safely share their customers' data and provide products and services through an open finance solution. Entities like microfinance institutions, savings and credit cooperatives, and smaller banks serve important market segments, yet those consumers may not be able to benefit from open finance if these providers are technologically incapable of using open finance APIs. This could mean new providers such as FinTechs in an open finance system

[31] European Union. 2022.

[32] State of India's Digital Economy. February, 2023. Centre for Internet and Digital Economy. Page 24

cannot adequately serve these customers, because their accounts are not with larger commercial banks or others who are more immediately ready to integrate into open finance and share customer data with third parties.

For EMDEs with an explicit financial inclusion policy mandate, they may consider monitoring the profiles of consumers who utilize open finance products and services to measure the impact on inclusion over time. Where segments are underserved in open finance, policymakers can work with industry to consider ways to better reach these populations, including through partnerships between tech-enabled providers and those using more traditional service delivery methods. To address risks of data-driven exclusion or bias, policymakers can periodically review the data sources available in open finance, and support the inclusion of new types of data—such as agricultural sales or merchant payments data—which could help bring underserved segments such as farmers, women, or microenterprises into the open finance ecosystem.

7. Unfair treatment and lack of product suitability

Across different open finance markets in varying stages of readiness—from conceptual stage to several years into the journey—the most consistent use case mentioned was expanding access to credit for individuals and MSMEs. Expanding credit access for underserved small enterprises could be transformative for financial access in emerging markets, where credit markets remain underdeveloped and risk assessment challenging due to limited information on small firms and individuals. It is quite likely that open finance in emerging markets will lead to expansion in the number of digital lenders and potential access to credit**. As the recent experiences in Africa and Asia with small-value digital consumer credit and buy-now-pay-later products have shown, fast-expanding credit markets will raise important consumer protection risks that need to be protected against**, **including**:

1. **Risks of misleading or predatory contract terms**, such as hidden fees, high penalty fees, or aggressive debt collection practices;
2. **Lack of product suitability to the individual's needs or capacity to repay**, in particular if credit risk assessments are made with limited information on the consumer;
3. **Aggressive marketing of third-party credit providers** on open finance participant or aggregator channels, including where the channel provider is given commissions or other incentives to promote the lender's product;
4. **Multiple borrowing in a short period of time**, which could lead to high levels of debt and inability to repay; and
5. **Inaccurate or outdated information on loan obligations or repayment behavior,** without clear processes for borrowers to check and correct the information through a central entity like a credit bureau.

None of these risks are unique to open finance-delivered credit, but the scale and diversity of actors in open finance requires robust rules regarding responsible lending, suitability, and related provisions. This will also require substantial supervisory capacity and resources, raising three questions for policymakers to consider as they develop open finance ecosystems:

1. **Are there existing consumer protection standards for fair treatment and product suitability?;**
2. **Do these standards apply for all the different parties that will utilize an open finance ecosystem to provide loans to consumers?; and**

3. **Is there sufficient supervisory capacity to enforce these principles in the currently regulated financial sector, and to expand this oversight function to an open finance ecosystem?**

Most open finance policy documents reviewed do not contain a wide range of consumer protection principles beyond transparency of information, data protection, and complaints handling. This may be because there are other laws already in place which cover the financial products and services found in open finance regimes. For example, both the United Kingdom and Mexico have dedicated financial consumer protection agencies with broad market coverage—the Financial Conduct Authority and CONDUSEF, respectively—which could take on some of the consumer protection aspects of open finance in the long-run. In these cases, including similar rules in open finance regulations could run the risk of conflicting with existing financial consumer protection policies, so may not be necessary or advisable. **However**, **some of the countries where open finance models are being considered do not have wide-ranging financial consumer protection provisions in place, and often these provisions do not cover all the possible provider types that could participate in an open finance ecosystem.**

Where existing consumer protection policies are limited, integrating a wider range of consumer protection provisions into the rules and policies that establish an open finance regime could be appropriate. In the Philippines, the Open Finance Framework (Circular No.1122 of 2021), requires participants to adopt customer awareness measures which include "products and services appropriate to the capacity and risk appetite of the consumer."[33] This provides a simple example of how concepts such as product suitability measures can be integrated into open finance regimes. The Bangko Sentral ng Pilipinas (BSP) has also seen its consumer protection powers expanded through the Financial Products and Services Consumer Protection Act (2022),[34] which obligates the BSP and other regulators to set policies in areas such as responsible pricing, suitability, and fair treatment.

Many EMDEs in regions such as sub-Saharan African have relatively small and under-resourced consumer protection departments within financial sector authorities, and limited mandates that may not match the consumer protection needs of open finance ecosystems, in particular by not covering many types of fintechs. **Open finance rules in many EMDEs may need to include more expansive consumer protection policies, standards, and obligations than many of the early examples of open finance policies globally, which have emerged from markets with broad consumer protection rules and resources already in place.** How to effectively execute this type of open finance consumer protection mandate is discussed in the next section on monitoring consumer protection in open finance.

[33] Circular No.1122, Series of 2021: Guidelines for the adoption of open finance framework. 2021. Bangko Sentral ng Pilipinas.
[34] Financial Products and Services Consumer Protection Act. 2021. Republic of the Philippines.

II. Monitoring consumer protection and conduct in open finance

Open finance is by design a fully digitized process. Digitization creates opportunities for even under-resourced consumer protection authorities to develop market monitoring approaches which take advantage of new methods for data-driven supervision of digital financial services. In recent years data-driven supervision methods have been developed and documented by entities such as Innovations for Poverty Action[35], Cambridge Center for Alternative Finance[36], CGAP[37], and the Alliance for Financial Inclusion.[38]

Investment in the collection and use of the data digital financial accounts and transactions provide could help low-resourced financial consumer protection authorities ensure open finance ecosystems are built with the necessary consumer protections and conduct oversight in place. It could also help to shift data collectiong from push-based (requesting periodic reports from providers) to pull-based reporting where supervisors have direct access to real-time data. There are three categories of data which could form the components of an initial open finance supervision model:

1. **Administrative data from financial institutions and third-parties participating in open finance;**
2. **Consumer-facing data and demand-side feedback channels;**
3. **Performance monitoring and reporting from participating entities and civil society organizations.**

This section presents initial concepts for specific data sources, methods of measurement and analysis, and supervisory priorities for each of these three categories. It then concludes by reviewing some of the primary challenges that authorities may face in implementing these types of supervisory methods.

1. Administrative data from financial service providers and third-party providers

Entities participating in open finance ecosystems must undertake a range of data monitoring and archiving requirements just to connect accounts and reconcile transactions across providers. For example, most regimes require collection and evidence of consumer consent for data access and sharing. Some participants must also report the number of accounts they have connected to, number of requests made, and the portion of successful and failed API calls.

Participants' ability to generates these reports means they should be able to perform more basic data collection and reporting activities which would bring value for consumer protection and market conduct supervision. There are several basic consumer protection data sets which should be included in the reporting requirements for open finance participants, which are discussed here.

[35] https://poverty-action.org/consumer-protection
[36] State of Suptech Report 2022. January, 2023. Cambridge Center for Alternative Finance.
[37] https://www.cgap.org/topics/collections/market-monitoring
[38] Regulatory and Supervisory Technologies for Financial Inclusion. February, 2022. Alliance for Financial Inclusion.

Consumer complaints data

Complaints data provide a window into the issues consumers are most likely to raise with their financial service providers, and how well these issues are received and resolved by the providers.[39] Additional layers of insight that come from complaints data include the types of channels used most frequently by consumers to engage with providers, demographic composition of complainants compared to overall customer demographics, and which products or transactions have the most frequent complaints raised.

Authorities overseeing open finance ecosystems should develop complaints data reporting rules and templates which capture not just traditional complaints data, but also new categories and data fields that reflect some of the particular issues or risks in open finance. Examples of complaints type categories and data fields that open finance may require adding to complaints reporting templates are shared in Table 1 below.

Table 1. Open finance relevant metrics for complaints reporting templates

Thematic area	Additional metrics for complaints data templates
Data protection	▪ Objections or questions regarding sharing of data with third parties ▪ Undesired marketing or communications from third-party providers ▪ Consent revocation or limitation requests ▪ Renewal or cancellation of third-party data access
Transaction or data call failures	▪ Failed transactions, specifying transaction type and third-party involved ▪ Inability to access or share data with another data recipient
Fraud and lost funds	▪ Fraud attempts from third-parties, by type, channel, product, and outcome ▪ Missing funds in open finance-linked accounts ▪ Unanticipated or suspicious third-party payment requests
Account switching	▪ Requests to switch accounts, by account types and consumer segments ▪ Issues attempting to switch or port accounts or account data ▪ Account closing or switching fees
Fees and charges	▪ Third-party fees and charges for open finance transactions and accounts ▪ Unexpected or disputed fees and charges ▪ Charges for subscription or service renewals and rollovers
Fair treatment and product suitability	▪ Issues with product terms or misleading sales practices ▪ Questions regarding role or conduct of third-parties (e.g. lenders, credit scoring services, data aggregators) ▪ Loan repayment issues or challenges ▪ Aggressive collections practices or account sweeping
Questions regarding open finance	▪ General inquiries regarding open finance by question type

Several of the additional metrics noted in Table 1 above relate to the conduct or products of third-parties. Where new products are promoted through existing brands, consumers may have trouble distinguishing between their pre-existing relationship with the original firm (e.g. a bank), and their relationship with new firms offering services on the back of the pre-existing relationship (e.g. a financial management service.) Such confusion has been observed in the rollout of mobile money provider/digital

[39] Matthew Bird, Kyla Longman, and Rafe Mazer. Leveraging customer complaints data to monitor consumer protection in mobile services in Uganda. September 2021. Innovations for Poverty Action.

lender partnerships in Africa.[40] This may lead consumers by default to complain directly to their pre-existing provider, even when the product in question is offered by a third-party partner of the pre-existing provider. The burden to parse this commercial relationship should not be left to the consumer, and a good practice would be to have these providers responsible for receiving and addressing complaints regarding their third-party provider partners. In fact, such expectations can be found in some of the liability arrangements of open finance models discussed previously—such as the Consumer Data Right in Australia—and should be considered when setting complaints handling and redress rules for open finance ecosystems.

A final consideration for complaints handling in open finance is the opportunity new actors bring to improve consumer complaints and provider accountability. As noted above, Sahamati in India is piloting an online dispute resolution system to handle issues that occur within its network of account aggregators, financial information providers, and financial information users. **Where there are concerns about the conduct of new third-party providers but limited supervisory capacity to oversee them, industry actors could help set up dispute resolution mechanisms that are standardized within the open finance interfaces of all providers, such as a common customer care icon or chat service on all apps and web browsers which offer open finance services so that consumers can use the same pathways to register complaints with all open finance participants**. The complaints data could then pool to a centralized database, which could be shared or summarized in reports to the relevant consumer protection supervisor(s). Such a system would also need to develop common customer identifiers, to match issues experienced by consumers across their various products and providers.

Fees, charges, and pricing transparency

Like all financial products, open finance-delivered products should adhere to the principles of fair and transparent pricing, so that consumers both know the costs they are paying and are not charged unreasonable or unexpected fees. **One of the ways to monitor compliance with these principles is to collect and review actual product and transaction data from financial service providers. This data could be collected at one or more of the following levels of granularity: Product-level data, account-level data, and transaction-level data**. The potential uses of each of these are detailed in Table 2 below.

Table 2. Product, account, and transaction-level data for open finance supervision

Level of granularity of data	Relevant indicators for open finance supervision
Product-level	▪ Number of opened and closed accounts ▪ Average account balances ▪ Income and margins of products ▪ Costs of similar products across the market, both within and outside open finance regimes
Account-level	▪ Switching of accounts across providers ▪ Scheduled and non-scheduled fees paid by type and amount ▪ Status of accounts (e.g. in arrears, dormant) ▪ Demographic segmentation by age, location, gender, etc.
Transaction-level	▪ Average number of transactions by customers

[40] Alex Fiorillo and Rafe Mazer. Digital Credit: Consumer Protection for M-Shwari and M-Pawa Users. April, 2015. CGAP.

	▪ Timing and amounts of charges and fees incurred on accounts ▪ Deposits, withdrawals, third-party payments by volume, type, and costs ▪ Demographic segmentation by age, location, gender, etc.

The primary anticipated benefits of such data would be to measure how competition is impacting consumer welfare in open finance. Some of the key metrics which could be measured are:

- **Costs.** Has there been a reduction in the cost of different financial services as open finance expands choice, or any concerning practices regarding fees for products or transactions?
- **Competition and switching**. Have consumers shifted products or providers, and from which providers or products are they switching, and to which new providers? Such analysis could be linked to a review of costs to see if consumers benefit from switching, including lower overall costs of products and services.
- **Suitability and consumer outcomes**. Are there any cost or usage patterns that may point to product suitability concerns, or reflect sub-optimal outcomes for consumers?

These examples are merely indicative, and when combined with demographic data can be used for a wide range of descriptive analysis. Analysis could include more sophisticated methods such as predictive modeling, cluster analysis, and other segmentation to help policymakers target supervisory resources on products or consumer segments where they see risks emerging from the administrative data analysis, allowing lower-resource authorities to engage in risk-based supervision in open finance, reducing their time and resource requirements.[41]

Administrative data collection and analysis is a high effort activity for both the firms submitting the data and the authorities reviewing the data. Not every situation will necessitate the collection of product, account, and transaction-level data across all providers. **Authorities should begin by defining their most important metrics for consumer protection in open finance, and then design a relevant and proportional set of supply-side data sources which can achieve this goal**, whether it is inclusive of the most granular of transaction data, or merely begins with provider-level reporting of aggregated statistics for their products offered through open finance.

Monitoring and preventing fraud

Fraud is a sensitive topic for financial service providers, as the perception of fraud risk can damage reputations and scare away potential customers. Providers may therefore be hesitant to share fraud data with others, even though the sharing of this data could benefit all providers by identifying common fraud types, consumers and transactions more commonly targeted by fraudsters, and even the identity of different fraudsters to flag other accounts they hold across the open finance ecosystem. Because of this, there is a growing call for the sharing of fraud data within open finance ecosystems. Given the sensitivity of this data, and the reluctance of some providers to share this data even with industry associations, regulators may need to require the reporting of fraud data to them directly for sharing to happen.

[41] For an overview of the use of digital finance administrative data for consumer protection supervision, see: Daniel Putman. Translating Digital Credit Transaction Data into Consumer Protection Supervision. 2022. Innovations for Poverty Action.

A comprehensive data set of fraud attempts, typologies, and targeted consumers could be an invaluable tool for the industry and authorities to improve fraud detection and prevention strategies. Such data would not require citing the specific providers. By sharing fraud data aggregated and segmented by product types, transaction types, consumer demographics, even details such as time of day, the industry could use tools like predictive modeling to improve consumer awareness efforts by focusing on the most vulnerable consumers or activities and to refine their criteria for flagging a transaction as suspicious. Analysis of fraud data in the United Kingdom's Open Banking has found that payment initiation fraud often targets an account be held by an older person, while the receiving account is often in the name of a younger adult. In this case transactions between an older payer and younger payee could be given heightened review where necessary.

Centralized fraud databases and related analysis could also address a point of contention between some banks and third-party providers regarding trade-offs between fraud prevention and timely execution of transactions in open finance. "The Future Development of Open Banking in the UK" report found that banks raised fraud risks as a reason to limit expansion of sharing of open banking services and data sources, while third party providers viewed these risks as overstated, and a possible excuse for limiting the growth of open finance by incumbents.[42] **Robust reporting of fraud data and sophisticated analysis could help resolve these differences of opinion by providing data on the actual size and nature of fraud risks and forcing industry actors to work together to reduce fraud, instead of focusing more on debates over the perceived level of fraud in the open finance ecosystem**.

2. Consumer-facing data and demand-side feedback channels

Measuring consumer experience in open finance should be part of any supervisory approach. By consulting with consumers and reviewing the interfaces they use for open finance, authorities will be able to understand why consumers behave in certain ways, and how well the products and services are designed to support their understanding and proper use of the innovations open finance makes possible. Several demand-side data sources offer promise for improved open finance supervision (see Table 3.)

Table 3. Demand-side and consumer-facing data sources for open finance consumer protection supervision

Data source	Proposed data collection
Product menu scripts and screenshots	Database of scripts and layouts for open finance products, including account opening, transactions, and other functions
Registration of contracts and terms of service	Archives of standard form contracts and data consent clauses for consumers enrolling in products or conducting transactions
Revenue-sharing and commission structures	Details of how open finance actors share revenue from consumers and any commissions related to products offered by third-party providers
Digital transaction audits	Execution of account opening, cross-provider transactions, product comparison, and advisory services by consumers under observation of the authorities to monitor quality and compliance
Social media and app store data	Consumer feedback on social media accounts or app store reviews, and meta-data related to open finance-affiliated apps on app stores

[42] Open Banking Strategic Working Group Secretariat. 2023.

Product menu scripts and screenshots

Intentional friction or confusing interfaces is a commonly cited conduct risk in open finance. Authorities may want to request providers share with them the full scripts and screen shots for their menus, so they can measure the number of steps, clarity of instructions, and placement of different options on menus and screens**.** This data could identify any cases of intentional friction, complexity, poorly designed or confusing interfaces that can hinder user experience. The review would also allow for identification of good practices in menu design or clarity of terms, which could be used to develop standard disclosure templates or transaction sequences.

Registration of contracts and terms of service

Consumer contracts in digital financial services may contain concerning or prohibited terms of service, but monitoring the many and often lengthy terms of service of products can be challenging. In an ecosystem as expansive as open finance, authorities may want to require all contract and terms of service templates be registered and filed with the authority to be considered valid. The authority could then use keyword analysis or natural language processing methods to identify any concerning or illegal terms or clauses without having to manually review each contract and terms of service.

Revenue-sharing arrangements and commission structures

Open finance can help consumers more efficiently review, compare, and choose from similar products on offer by different financial service providers. Some countries may have pre-existing rules regarding commissions and financial advisory services that protect consumers from conflicts of interest in these models. But not all countries where open finance is being considered benefit from such consumer protection measures. In these cases, at a minimum providers should have to disclose these arrangements to the authority, and the authority could then consider setting standards for disclosure of incentives, commissions, and other conflicts of interest to consumers, in the absence of more robust protections regarding advisory services.

Digital transaction audits

Audit studies—or mystery shopping—have been used by financial sector supervisors for decades.[43] While traditionally in-person, audit study methods are being adapted to digital products and transactions to assess factors such as interface usability, reliability of transactions, and transparency of information provided.[44] Digital audit studies can also be conducted at a lower cost than in-person audit studies. Open finance lends itself to remote audit studies, and authorities should consider running periodic audit studies on a random selection of products, or focusing on products which are new, receive high volumes of complaints, are complex, or more susceptible to consumer risks.

Social media and app store meta-data and unstructured text

Because open finance brings many new, smaller fintech and technology firms into contact with financial consumers, authorities may want to consider monitoring social media and app stores to gain insight into

---

[43] Rafe Mazer, Xavier Gine, and Cristina Martinez. [Mystery Shopping for Financial Services](). 2015. CGAP.

[44] William Blackmon and Brian Mwesigwa. [Measuring Fees and Transparency in Nigeria's Digital Financial Services](). February, 2022. Innovations for Poverty Action.

the conduct of these digital financial service providers. This could include monitoring consumer posts directed towards the firms of interest and reviewing the app stores to identify any concerns regarding the reviews of providers participating in open finance. The app store data could potentially provide information if there are any apps advertising open finance-related services that are not in fact registered within the open finance registry.

3. Performance monitoring and reporting from participating entities and civil society organizations

Participants in an open finance ecosystem can help supervisors to monitor and address risks that occur during inter-firm interactions in open finance, such as poor performing APIs, data security issues, and abuse of recurring payments features. For example, a bank participating in open finance could incorporate periodic monitoring of the data use of third-party partners into their existing data protection and data security measures—in fact such monitoring is required in some open finance jurisdictions. This could include random checks to confirm erasure of data by these third parties when requested by customers, auditing of the consent archives of third-parties to confirm alignment with the stated uses of the data, and periodic surveying of bank customers who have used the third party's services. Such checks will help to identify any uses of the data or activities the consumer did not authorize or intend—such as marketing and product solicitation or sharing with unauthorized parties.

Open finance participants could also help monitor the use of recurring payments in open finance. While recurring payments are convenient and facilitate new products and services consumers benefit from, these recurring payments could be abused by third-parties. The experience of online subscriptions in e-commerce and media point to similar potential risks in open finance. As recurring payments become more common, industry and supervisors can monitor the use and evolution of these features by third-parties. A starting point could be banks and other account holders sharing detailed information on the extent of the use of recurring third-party payments by their customers, the product and use types for recurring payments, and the charges associated. From this initial data the industry and authorities could develop indicators which can help to identify any recurring payments that may raise consumer protection risks, while letting recurring payments use cases continue to grow and innovate.

How Brazil monitors performance indicators across the open finance ecosystem

In Brazil, the open finance governing body has developed a ticketing system for issues raised by open finance participants with each other. The Central Bank of Brazil (BCB) has access to the system so they can review the disputes. While the BCB can intervene if needed, for these types of disputes the preference is that these are resolved either by the providers themselves, or through the industry open finance governing body. Only if these channels fail would the issues be escalated to the relevant regulatory authority. There are three primary ticket types currently used:

1. **Administrative tickets**
    a. User registrations
    b. Registration updates
    c. Password resets
2. **Tickets addressed for the Working Groups of the Open Finance Structure**
    a. Questions and suggestions for improving technical documentation

   b. Incidents, questions, and suggestions for improving tools, such as the service desk and directory
3. **Bilateral tickets from one open finance participant to another**
   a. Interoperability issues
   b. Data quality
   c. Responses to specific cases
   d. Other non-compliances with open finance documentation.

The ecosystem has also developed a dashboard which provides visibility on key indicators of the performance and growth of the open finance ecosystem. In the medium term there are plans for another platform which will automate the processing, reconciliation, and analysis of the reports from all participants. Currently the BCB has its own process to gather and analyze the volume of calls through the ecosystem, which APIs are called, the endpoints called, and the results of these endpoints. It then uses this information for supervisory actions.

4. Challenges to enacting consumer protection supervision in open finance

Enacting any of the above supervisory approaches for consumer protection and market conduct in open finance requires substantial long-term investment and effort. Already authorities with lower resources or staff capacity have shown challenges in supervising new financial technologies and product innovations.[45] Several policy and technical challenges could impede progress in implementing consumer protection supervision in open finance, and should be anticipated and addressed:

1. Coordination across relevant consumer protection, competition, and data protection authorities.
2. Staff and technological capacity for data-driven supervision.
3. Gaps in detection of risks and consumer harm

Coordination across relevant consumer protection, competition, and data protection authorities

Open finance typically involves multiple supervisory authorities, with complementary and at times overlapping consumer protection obligations. As open banking approaches shift to open finance and open data, new financial sectors (e.g. insurance) or industries (e.g. telecommunications) will be included in these models. This will increase the number of agencies and authorities involved in supervision and enforcement. There is a risk that authorities may not properly coordinate the development of their data collection and analysis processes, resulting in different levels of supervision and protection for different open finance actors and consumers, as well as redundant or inefficient reporting requirements for firms.

Staff and technological capacity for data-driven supervision

Experience implementing data-driven supervision approaches with financial sector regulators has shown that some authorities may not initially have the right types of staff or technology in place. In the early stages of planning for consumer protection supervision of open finance, authorities should review their current data sources and collection channels to determine what investments might be needed for each of the data sources described above, and whether such investment is worth the potential benefits that data could provide for supervision. Not only should staffing be reviewed, outsourced suptech solutions

[45] See, for example: Alliance for Financial Inclusion, 2022; Cambridge Center for Alternative Finance, 2023;

should be considered as well to determine whether it is preferable to hire new staff or to contract with a firm that can provide the required data analysis through off-the-shelf solutions.

Gaps in detection of risks and consumer harm

Complex or difficult to define consumer protection issues such as fair treatment or suitability may not be easily measured through one single source of data. Increasingly supervisors are using a range of indicators to assess outcomes,[46] relying on triangulation of data sources and the metrics they produce. Open finance authorities will need to identify data sources that can measure these risks. New issues such as third-party charges, data usage, and commercial terms of provider tie-ins expand the supervisory needs in bilateral consumer-provider financial services. At the beginning of the design of an open finance consumer protection strategy, authorities should develop a list of metrics each anticipated data source could provide for their various consumer protection priorities, and what aspects of these priorities they will not be able measure. By doing so authorities can develop composite indicators for each consumer protection priority that do not rely on one data source, and triangulate across data sources to improve accuracy and depth of analysis for each consumer protection priority.

III. Consumer protection cannot wait in open finance

Tens of millions of accounts, millions and millions of account records, hundreds or even thousands of firms, and billions in US dollar-equivalent funds transacted. The scale some open finance models are reaching shows how beneficial these models are for financial sector development and innovation. Yet consumer protection in open finance remains relatively underdeveloped in most markets.

Part of this is that consumer protection always lags behind market development—if there is no market filled with consumers, who are you protecting, and what exactly are you protecting them from? **But the scale of open finance in some markets makes it essential to develop robust consumer protection supervision frameworks. For markets at an earlier stage of open finance development, there is now a set of key risks and lessons learned on consumer protection in open finance from pioneer markets like Brazil, Europe, and the United Kingdom they can use to build consumer protection rules and supervision models into their ecosystem from the beginning.**

This report considered seven consumer protection risks in open finance:

1. Lack of transparency and accountability in use of consumer data
2. Complex menus and intentional friction in the user experience
3. Consumer-affecting fraud
4. Inadequate complaints handling and dispute resolution for multi-party transactions
5. Lack of clear liability frameworks
6. Exclusion due to biased data
7. Unfair treatment and lack of product suitability

[46] See, for example: Antonique Koning, Juan Carlos Izaguirre, and Aveesha Singh. Customer Outcomes-Based Approach to Consumer Protection: A Guide to Measuring Outcomes. June, 2022. CGAP.

This list is of course not exhaustive. Open finance is a derivative of open banking, and a predecessor of open data in some markets, meaning that the frontier of issues is as broad as the range of data types individuals may someday leverage for their benefit in the digital economy. The list of related risks will expand and evolve, the data sources to track these risks become more complex, and the range of firms that need to be supervised include more industries and product types**. Supervision of open finance and open data will be a shifting and expanding target that necessitates expanding the capabilities of digital data collection and analysis in financial sector and competition authorities.** To supervise the ecosystem and intervene when consumer protection principles are violated, open finance and open data will also require coordination across authorities, and between authorities and key actors in the ecosystem such as firms, industry organizations, and civil society.

At the heart of all of this is digital data and consumer feedback. This report suggests three data classes that could be initial building blocks for an open finance consumer protection data center and supervisory model:

1. Administrative data from financial services providers and third-parties
2. Consumer-facing data and demand-side feedback channels
3. Performance monitoring and reporting from participating entities and civil society organizations.

As a first step, authorities should take stock of the available data within each of these classes, and consider how each of these data sources can contribute to the measurement and monitoring of consumer protection risks in open finance. The potential for open finance to improve competition, enhance consumer value, and support financial inclusion in EMDEs is on par with breakthrough innovations such as mobile money. But achieving this potential will require a trustworthy, fair, and secure ecosystem, and data-driven consumer protection supervision should be central in the implementation of all open finance and similar data-sharing models.