

The Equifax logo is a red circle with the word "EQUIFAX" in white, bold, sans-serif capital letters.

EQUIFAX

The Open Data Institute logo consists of the words "open data institute" in a small, white, sans-serif font, positioned to the left of a large, black, stylized "ODI" acronym.

open
data
institute

The background features a pattern of white dots of varying sizes, some of which are arranged in concentric circles, creating a subtle geometric design.

Open Banking

Consumer consent frameworks
around the globe

Contents

Introduction	1
About Equifax and The ODI	1
What is Consent?	1
Executive Summary	2
Research Methodology	4
Research Results	6
Specific Open Banking regulations	6
How consumers give consent	8
Revoking consent	11
Rules and restrictions regarding consumer consent	12
Rules and restrictions regarding data use	13
Duration of consent	15
The consequences of breaking the rules	16
Conclusion	18
Appendix	19
Contributors	19
Interview questions	20
Other documents	20



Research carried out by the Open Data Institute for Equifax

Introduction

About Equifax and The ODI

This report was written by the Open Data Institute (ODI) for Equifax Ltd.

Founded in 2012, the ODI is an international, independent and not-for-profit organisation based in London, UK. The ODI works with companies and governments to build an open, trustworthy data ecosystem, where people can make better decisions using data and manage any harmful impacts.¹

Equifax is a global information solutions company that uses unique data, innovative analytics, technology and industry expertise to power organisations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions. Headquartered in Atlanta, Ga., Equifax operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. It is a member of Standard & Poor's (S&P) 500® Index, and its common stock is traded on the New York Stock Exchange (NYSE) under the symbol EFX.²

What is Consent?

The Information Commissioner's Office (ICO) defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Across the banking and financial sectors, this generally refers to a customer allowing a third party service provider access to data about them that is held by their bank or other financial institution.

Consent is one of the core aspects underpinning the trusted data sharing system known as Open Banking.

Open Banking allows retail banking customers to share account and transaction data with trusted partners. This shared data is combined with openly published non-personal data, such as lists of bank products and branch locations, to build useful services for customers, FinTechs, and banks themselves.

¹ Open Data Institute (2012), 'The Open Data Institute', theodi.org
² Equifax (2019), 'Company Profile', <https://www.equifax.com/about-equifax/company-profile>



Executive summary

Consent is an invaluable aspect of a trustworthy and effective data ecosystem. Consent mechanisms can vary substantially from country to country. This happens for a variety of reasons, such as the type of organisation governing consent, the social and legal context, the risks to individuals or different groups of people, or the technical landscape. Language can also impact how consent is treated, both in terms of different languages being interpreted differently across borders, but even within the same language. In English alone, terms such as “consent”, “authorisation”, and sometimes even “authentication” can be used interchangeably, further frustrating comparison.

Despite this, there are overarching similarities that can be discussed and compared across the boundaries set by governments and regulators, how consent is granted by consumers, how it is revoked, how long consent lasts, and the punishment for breaking the rules. Universally important aspects are that consent must be clear to customers, using language like ‘informed’, ‘explicit’, ‘affirmative’. Most regimes also emphasise that consent must be ‘free’ or ‘voluntary’, and as easy to revoke as it is to give.

The specific rules of how consent operates, such as duration, restrictions, and punishments are far less universal. Across our research we observed the time period for consent to range from 90 days in Europe, to one year in Australia and New Zealand, with most countries not defining this crucial aspect at all. Restrictions tend to be informed by the privacy laws of the different countries, which like consent can be very idiosyncratic across cultures and legal landscapes. The UK and Australia have built whitelists for their Open Banking regimes to control which organisations can participate, while Mexico and New Zealand have been less restrictive in this. Punishments can range both within and across countries depending on the severity of the infraction.

Open Banking regimes often offer a dispute resolution mechanism to allow organisations to work out solutions together.

Where the laws around consent have been broken, countries such as Japan and Mexico have been very explicit about repercussions in the form of hundreds of thousands of dollars in fines and years of prison time.

The UK and Europe have been leaders in this space in recent years with the implementation of legislation across the continent such as PSD2 and GDPR, and many countries look to them to understand what works well and what doesn't. Australia and New Zealand especially have been making progress, particularly leveraging the UK Open Banking Standard to inform consent due to cultural and economic similarities. Countries with dissimilar banking industries such as Mexico and Nigeria have also been pushing ahead with their own consent regimes via Open Banking initiatives, but taking a more regionally appropriate approach.

Creating an easy, open way to compare consent could be useful to the international banking community in many ways:

- Different initiatives around the world could learn from each other, share resources on best practises, and coordinate on implementation.
- Comparison and coordination could help with interoperability in financial services between countries, potentially boosting trade and giving customers more and better options.
- More public awareness and understanding of consent could increase public confidence in these new processes, and reduce potential misconceptions around concepts like “Open Banking”.
- More public confidence could support user adoption, increasing the number of people with access to the benefits of Open Banking.
- Getting consent right in the banking sector and creating a trustworthy data ecosystem could create a demand for the same rigour in other sectors, and open up dialogue about consent and personal data across society in meaningful and informed ways.



Research methodology

Research carried out by the Open Data Institute on behalf of Equifax in Autumn 2019. The research methodology for this paper employed both desk research and user research. Desk research was completed by analysing Open Banking and banking data portability initiatives, as well as data protection legislation from the following countries:

User research was conducted by interviewing regional experts in Open Banking and banking data portability across Australia, Canada, Japan, Mexico, New Zealand, Nigeria, Spain and the UK. The full list of contributors and research questions are available in the appendix.

Canada
Open Banking Initiative: N/A - Review into the Merits of Open Banking
Key laws governing consent: Personal Information Protection and Electronic Documents Act (PIPEDA)
Relevant organisations: Payments Canada and Bank of Canada

USA
Open Banking Initiative: N/A
Key laws governing consent: Dodd-Frank Wall Street Reform and Consumer Protection Act
Relevant organisations: National Automated Clearinghouse Association (NACHA) and Consumer Financial Protection Bureau (CFPB)

Mexico
Open Banking Initiative: Law Regulating the Financial Technology Institutions ("The FinTech Law")
Key laws governing consent: Federal Law on Protection of Personal Data Held by Private Parties
Relevant organisations: Comisión Nacional Bancaria y de Valores (CNBV) and Open Banking Mexico

Brazil
Open Banking Initiative: N/A
Key laws governing consent: General Data Protection Law (GDPL)
Relevant organisations: National Data Protection Authority

UK
Open Banking Initiative: Open Banking
Key laws governing consent: GDPR and Data Protection Act 2018
Relevant organisations: Open Banking Limited, Competition and Markets Authority (CMA), and Financial Conduct Authority (FCA)

European Union (EU)
Open Banking Initiative: Second Payment Services Directive (PSD2)
Key laws governing consent: General Data Protection Regulation (GDPR)
Relevant organisations: Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) and European Commission (EC)

Spain
Open Banking Initiative: PSD2
Key laws governing consent: GDPR
Relevant organisations: DG FISMA and EC

Nigeria
Open Banking Initiative: Open Banking Nigeria (in progress)
Key laws governing consent: Open Vector report for OBN
Relevant organisations: Open Technology Foundation (OTF) and Open Banking Nigeria (OBN)

Hong Kong
Open Banking Initiative: Open Application Programming Interfaces (APIs) for Banking
Key laws governing consent: Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry / The Personal Data Ordinance
Relevant organisations: Hong Kong Monetary Authority (HKMA) and Privacy Commissioner

Japan
Open Banking Initiative: Banking Act amendments for 'Electronic Payment Intermediate Service Providers'
Key laws governing consent: Act on the Protection of Personal Information
Relevant organisations: Financial Services Agency (FSA) and Japanese Bankers Association (JBA)

Malaysia
Open Banking Initiative: Policy Document on Publishing Open Data using Open API
Key laws governing consent: Personal Data Protection Act 2010
Relevant organisations: Bank Negara Malaysia

India
Open Banking Initiative: Unified Payment Interface (UPI) / Aadhar
Key laws governing consent: Personal Data Protection Bill [DRAFT]
Relevant organisations: Reserve Bank of India (RBI)

Australia
Open Banking Initiative: Consumer Right Data (CDR)
Key laws governing consent: CDR
Relevant organisations: Australian Competition and Consumer Commission (ACCC)

New Zealand
Open Banking Initiative: Payments NZ API Standards
Key laws governing consent: Payments NZ API Standards - Consent Management API
Relevant organisations: Payments NZ

Specific Open Banking regulations

Whether or not countries have “Open Banking” regulations may be a matter of vocabulary and definition. Open Banking is the term used for the functionality including and beyond PSD2 in the UK, and it is likely that it may take on different forms in different markets. This could also include the use of open Application Program Interfaces (APIs) - APIs that give public availability to web services, the publishing of open data - data that anyone can access, use and share, and more. The UK initially designed this initiative to increase competition in the retail banking sector by encouraging innovative solutions powered through data sharing.

Outside of the UK in Europe, PSD2 looms large as the regional regulatory regime. Though this is not always considered an Open Banking initiative, it embodies much of the same characteristics. PSD2 regulates payment services and payment service providers, and works alongside the Single Euro Payments Area (SEPA) to ensure the harmonisation of payment products, infrastructures and technical standards across Europe. The scheduled introduction of Strong Customer Authentication (SCA) and Common and Secure Communication (CSC) in September bring new advances to this regulation.



Australia

Australia has adapted the structure of Open Banking in the UK as part of the implementation of the Consumer Data Right (CDR). This will require a similar rules around secure APIs featured in the UK's Open Banking, but for all CDR data. The difference in this is that the Consumer Data Right only begins with banking data. The end game is to roll out a similar API-based data portability regime for personal data in other sectors as well, such as energy and telecommunications.



Mexico

Mexico plans to enforce many of the same aspects as the UK, such as APIs and the sharing of open, aggregated and transactional data by financial services providers. However Mexico is taking an industry-led route that is focussing on innovative products for consumers over increased competition as its goal. It will also be allowing for premium APIs, APIs providing functionality which can be charged for by the financial institutes providing them, and will impose Open Banking on all financial institutions, not just the major ones.



Hong Kong

Hong Kong published their Open API Framework for the Hong Kong banking sector in 2018, setting out its intended approach to Open Banking. The Hong Kong Monetary Authority (HKMA) has also allowed industry to set its own standards without making it a regulatory requirement and the first API for product information was rolled out in early 2019.



India

India's Open Banking is built in part on the authentication process in Aadhar, the country's national identity platform. India's Unified Payment Interface (UPI) enables all bank account holders in the country to send and receive money from their smartphones without the need to enter bank account information or online banking details. As of March 2019, UPI is used by 142 banks, accounting for just under 800 million transactions a month with a combined value of US\$19 billion.



New Zealand

New Zealand is developing its Open Banking framework by adapting much of the UK standard. This is being driven by the voluntary cooperation of the major players in the market under the stewardship of the local payments association, PaymentsNZ. Similar to the UK, New Zealand's pilot includes account information and payments, and will be executed under the guidance of its own Open Banking working group. Unlike the UK, which rolled out account information functionality before payments, PaymentsNZ plans to launch both up front, putting a higher onus on having the proper consent model in place.



Japan

In 2017, Japan passed the Amended Banking Act to introduce a registration system for Third Party Service Providers (TPPs) and set the framework for collaboration between banks and TPPs. The act encouraged banks to open their APIs by 2020, with 100 financial institutions using these APIs by the Olympics being an important national goal. There have also been voluntary partnerships between financial institutions to launch digital payment initiatives. However, adoption by third parties has been low, in part because of the difficulty banks and FinTechs have in negotiating contracts.



Canada

Canada created an Advisory Committee on Open Banking to review potential benefits of Open Banking. In June 2019, the Standing Senate Committee on Banking, Trade and Commerce released its report entitled “Open Banking: What It Means For You”, which included a number of recommendations intended to lay the groundwork for the rollout of Open Banking in Canada.



Nigeria

Open Banking Nigeria (OBN) was launched in 2018 in a bid to drive innovation and choice in the Nigerian banking sector. Its objective is to roll out open APIs and encourage banks and FinTechs to adopt open standards for API implementation. Nigeria is creating a framework and they hope to draft their own standard that will be more appropriate for Nigeria and other countries in West Africa. OBN believes Open Banking will revolutionise the Nigerian banking sector and be a huge boost to the economy as a whole.



How consumers give consent



"[In Nigeria], Consumers give informed consent when they are able to see the type of data they will allow access to, how often or long the TPP would have access, and are able to successfully authenticate against their bank's system."

 Adédèjì Olówè, Trustee, Open Banking Nigeria

As noted earlier, consent mechanisms can vary substantially from country to country, though there are some commonalities across them. In numerous consent environments, we see three key elements: consent being explicit, voluntary, and not cumbersome. These three elements increase the likelihood of people being properly informed when consenting their data, as it adds enough friction in the process to allow awareness, without overburdening someone with terms and conditions.

One form of consent we see in countries that already have an Open Banking infrastructure, is the "redirect model". In the UK this means that customers give their consent to a Third Party Service Provider (TPP), but authenticate their consent with their bank, allowing the customer to keep the identity credentials that are used with their bank private. This model allows for a clear and simple way for customers to provide consent to TPPs. It also exists across the EU via PSD2, which has its data protection foundation within GDPR. Meanwhile Australia, New Zealand and Nigeria are rolling out consent in a similar fashion in their Open Banking initiatives as well.

"In New Zealand, both API Providers (ASPSPs) and Third Parties (TPPs) are subject to the Privacy Act, which sets out how they must collect, use and store personal information. Accordingly, consent obligations sit with both the APSPs and the TPPs."

 Steve Wiggins, Chief Executive, PaymentsNZ

Redirect models defined by Open Banking initiatives are not the only way to give consent.

Other Open Banking initiatives use the consent models that are defined in data protection laws that safeguard the rights of consumers around the collection, use, and sharing of their data. Hong Kong's Open APIs are governed by its data protection laws requiring 'express' and 'voluntary' written consent. India uses RBI's 'master directions' while its data protection is still in draft, which have similar requirements. Other countries with similar practices include Brazil and Canada.

Some consent regimes are less well-defined than others. For example Japan focuses more on ensuring there is a fair process than defining what that process might be. Key organisations in the US such as the Treasury and the CFPB recommend informed consent for data accessed via screen scraping, but have not defined enforceable rules.

Mexico is currently in the process of implementing Open Banking, and though it plans to have explicit consent built into the model, the mechanisms to do so have not yet been specified via the FinTech Law.

In Malaysia, like many other countries, there are distinctions between personal data and sensitive personal data. Financial data is classified as personal data which only requires consent, unlike sensitive personal data which requires explicit content.



UK Open Banking and Consent

by Emma Steeley, CEO, AccountScore

UK banking consumers for the first time have transparency, awareness and control over their data. The sharing of the data ensures that the customer is well informed of what data is being accessed, by whom and on what terms, including the frequency of access.

User experience has improved over a period of time and we have seen a significant increase in the completion rates of consumers sharing their data throughout the year, especially with the launch of Open Banking's Customer Experience Guidelines V3.1 with app-to-app redirection.

Open Banking stipulates that explicit consent is required in order to facilitate the sharing of bank transaction data.

The positives:

- Allows the customer to be in control of what data they share and when
- Provides the ability for a customer to revoke consent at any time
- Means organisations need to articulate clearly what data they are sharing and be clear about why
- Creates a method by which companies and government organisations can work within data protection regulation

The negatives:

- Organisations which have broken down silos now face restrictions on how they can use data
- Consent management by definition requires a user interface for customers which may not be consistent with an organisation's UI strategy or brand values
- Organisations may end up with multiple APIs to manage consent which could be confusing
- The entire consent model could make customers wary of sharing data where it is in their best interest

Consent Management

The complexity for consumers comes into play when they are able to manage their consents. With the increasing volumes of TPPs, that are now implementing a consent management platform in order to adhere to the Open Banking Customer Experience Guidelines, the consumer may have multiple data shares through multiple organisations, which may quickly become confusing.

AccountScore believes that consumers wish to organise similar activities into single places in their digital lives.

In its simplest form, consent management requires:

- A list of data assets a consumer possesses;
- A list of organisations they share them with; and
- A graphical representation of the interactions which exist between them

Global Consent

Being the first Open Banking implementation to go live across the globe has given the UK a distinct advantage. However, AccountScore believes that global consent is something that is not going away and that ultimately consumers will want a single app where they can see and amend these interactions across all organisations, thus creating an easy to manage consent data vault.

Revoking consent

Just as important as the process to provide consent, the ability to revoke consent is a key component of Open Banking. Open Banking in the UK and PSD2 have spearheaded the importance of allowing customers to withdraw consent at any time. The mechanism for this is through a permissions dashboard which can be accessed by the consumer through their bank, or increasingly at the TPP.

Although there are still improvements ongoing regarding consents within Open Banking and PSD2, they are still widely looked to internationally, with other consent regimes following a similar model. New Zealand and Canada follow the PSD2 model of going through the customer's Account Servicing Payment Service Provider (ASPSP) or financial institution directly to revoke consent. Australia has taken a slightly different approach by having the TPP be the gatekeeper of revoking consent.

"In New Zealand a customer can revoke their consent in their authenticated environment at the API Provider (ASPSP). The ASPSP does not have to push a notification of the revoked consent to the Third Party (TPP). However, we have developed easy tools for TPPs to review all consents held."



Steve Wiggins, Chief Executive,
PaymentsNZ

Other data landscapes are less specific around which organisation consent revocation should go through, just that it should occur. Countries like Hong Kong, India, Japan, Brazil and Malaysia all have clearly written rules allowing for consent to be revoked, with Brazil and Hong Kong going as far as to stipulate it can be at any time.

"According to the new data privacy law [in Nigeria], customers can revoke consent but the ways and means to do that are not well defined."



Adédèjì Olówè, Trustee,
Open Banking Nigeria

Mexico and Nigeria are yet to complete designing Open Banking, but plan on having consent revocation at the forefront of their policies. The screen scraping regime of the United States is unclear but the CFPB's Principles recommend the terms of data access disclosed include "access frequency, data scope, and retention period."

"[In Mexico], mechanisms are not defined yet but the standard specifications and rules will be developed for consent revocation."



Mariana Velázquez Suárez, Expert,
Mexico Open Banking



Rules and restrictions regarding consumer consent

Some data sharing regimes also have specific rules around with whom data can be shared. In the UK, a TPP whitelist is used to restrict the API framework to organisations that are trusted. This whitelist, now known as the Open Banking Directory, was built so that the CMA9 and other banks could identify the TPP seeking to access its APIs and confirm that the TPP has the appropriate regulatory permissions. This vetting process ensures a higher level of security, and therefore trust in the overall infrastructure which could help promote greater innovation.

Similarly processes are happening in other countries as well. Australia is following the model of the UK in requiring that all third parties participating in CDR-powered services be accredited. Mexico will require service providers to be authorised by the relevant Supervisory Commission, under specific requirements laid out by the CNBV. The National Banking and Securities Commission (CNBV), is a decentralized body of the Ministry of Finance and Public Credit (SHCP), with powers regarding authorisation, regulation, supervision and sanction on the various sectors and entities that make up the financial system in Mexico. Nigeria too will require its Payment Solutions Services Providers (PSSPs) to connect with banks through a verification process.

Whitelisting is also one of the places where PSD2 and Open Banking differ. Although PSD2 plans to offer strong customer authentication (SCA), alongside other security features, they will not have a list of authorised parties. In addition to the EU, New Zealand and Canada do not have any specific rules around who consumers can consent to sharing banking data with, and Japan is only limited by its Personal Information Protection Law (PIPL).

One specific rule around acquiring consent that has appeared in a couple regulations has been “bundled consent”. Hong Kong’s personal data law labels this as “where a data user collects personal data from a customer through a service application form which is designed in such a way that renders it impracticable for the customer to refuse consent to the use of his personal data for purposes unrelated to the services to be provided to the customer.” Both Australia and Hong Kong specifically deny this type of consent.

“With the implementation of Open Banking in Mexico, in order for a third party to be able to connect to the regulatory APIs to access customer data, they require prior customer consent. The third party will have to be authorized by the relevant Supervisory Commission and will have to meet specific requirements in order to be authorized. At the CNBV the secondary regulation is under development.”

 Mariana Velázquez Suárez, Expert,
Mexico Open Banking

Rules and restrictions regarding data use

Across countries rules also exist around the purposes for which shared data can be used. This could vary from restrictions on what purposes that data can be shared for, to merely requiring a purpose be clearly stated, to none at all.

In data sharing programmes such as Open Banking, PSD2, and others, the only explicit restriction on types of activity for which banking data can be shared are related to other criminal laws, such as financing terrorism or for money laundering.

Under most consent rules, data is consented to be shared for specific purposes that are explicitly stated, using shared data for any purpose not stated is breaking the agreed rules. Japan’s data protection law restricts the use of data in this way, as does Canada’s privacy laws. Canada includes restricting banks from even sharing financial data with their subsidiary companies, such as an insurance company. Mexico’s FinTech Law similarly allows only for data to be used for the authorised purpose of the customer, as does Brazil.

Australia takes a different approach and imbues the need to state the purpose as part of the accreditation process to become a trusted TPP. This is then verified with unambiguous disclosure of how the data will be used again at the consent stage.

Across India, Hong Kong, Malaysia, Nigeria, New Zealand and the US, specific rules for Open Banking have not been created, instead, general legislative frameworks for individual countries apply.

“In the Fintech Law of Mexico, article 76, says that the transactional data will only be used for the specific purposes authorized by the customer and data will be treated as personal data which falls under the scope of the privacy law. The secondary regulation is still under development and it is being considered the scope of the use of data.”

 Mariana Velázquez Suárez, Expert,
Mexico Open Banking



Consent in Open Banking UK

by Miles Cheetham, Head of Propositions, Open Banking Implementation Entity

There is no question that consumer consent is an area that requires greater clarity and definition as data sharing ecosystems develop. It's crucial for building trust with consumers, but the lack of consistency in which consent is explained and obtained can cause consumer confusion. There are a number of dimensions to this.

The respective definitions of consent and explicit consent under GDPR and PSD2 are critical. How and when this needs to be presented to the consumer and how the differences between these two regulations can be made clear continues to challenge many.

Where possible, our emerging view is that the account information services provider (AISP) – a type of third party provider (TPP) - should consider what legislation or policies the consent requirement is coming from. Once this is determined, the AISP can capture this in their Terms and Conditions or elsewhere in launching their service. This should also cover aspects such as sharing data with other parties where it is required to create the end “product”.

This then allows other consent requirements to be presented as a separate request. As AISPs need to comply with consent arrangements provided for under PSD2 and a lawful basis under GDPR, the consumer needs to know exactly what they are agreeing to and under what terms. It is our emerging view this can be made very clear and might address:

- The purpose for sharing their personal data
- The value exchange – what the consumer will get in return for sharing
- The actual data, which the Open Banking Implementation Entity has defined as a set of data clusters
- The parameters under which it is being shared i.e. when it starts, for how long, the frequency of access being granted to the AISP and what rights are triggered - and when - in respect of that personal data

Building a clear, well-understood consent system with a good customer journey is essential to the success of the Open Banking ecosystem.

This will allow both banks and AISPs to be confident that they are meeting their regulatory requirements. Most importantly, we consider that this is an area which is essential to get right in order to establish trust with the consumer and therefore provide a key building block in a healthy data sharing economy.

From the consumer’s perspective we can summarise the key aspects that are important:

- Setting up a new service should not only be simple, but the key terms and the use of their personal data must be clear. This is where GDPR comes to the fore
- Granting consent to share personal data under Open Banking must make it very clear why it's needed, what's being shared, for how long etc. - and what the consumer will get for doing this. This is where PSD2 is the regulatory driver





The management and revocation of consent and its distinct implications from a PSD2 or GDPR perspective must be understood by all players, as well as the end consumer. Importantly, a bank or TPP should easily be able to recognise under what legislation the right arises as well as the implications of an end consumer exercising that right under each legislation. At this stage, both PSD2 and GDPR must be addressed

A great deal to consider. If we can collectively get these dimensions right then we'll be laying down the right foundation for the success of not just Open Banking but the wider data sharing economy that is developing.










Duration of consent

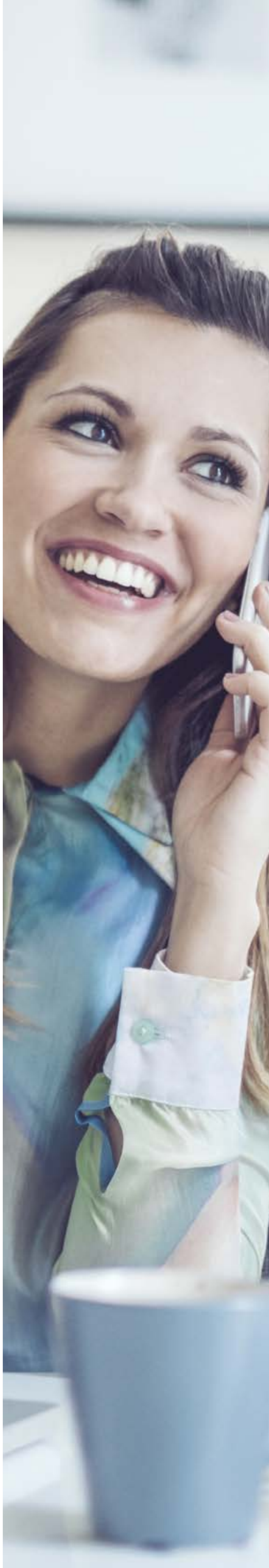
The duration of consent refers to the length of time a consumer consents to share data with a third party. It is the length of time for which that consent is valid and in which the third party can use the data.

As of this publication, only the UK, EU, Australia and New Zealand have defined consent durations for their Open Banking initiatives. The UK and EU follow the 90 day guidelines set under PSD2, while Australia and New Zealand have decided to set a 12 month consent period.

	Country	Time Period
	EU	90 days
	UK	90 days
	Australia	12 months
	New Zealand	12 months



	Country	Time Period
	Brazil	Undefined
	Canada	Undefined
	Hong Kong	Undefined
	India	Undefined
	Japan	Undefined
	Malaysia	Undefined
	Mexico	Undefined
	Nigeria	Undefined
	USA	Undefined



The consequences of breaking the rules

With rules and regulations around accreditation and authorisation of third party service providers, there needs to be consequences for breaking the rules. Dispute mechanisms can also be created to help mediate conflicts, but penalties exist to encourage good behaviour. These penalties can range from organisations being suspended from the data sharing system, to having their banking licenses revoked, to fines and potential prison time.

Open Banking in the UK and PSD2 build on previous legislation in complaint resolution by increasing customer rights in the area of complaints handling. PSD2 requires payment providers to respond to and resolve complaints in a timely and appropriate manner. For example, payment providers must respond to complaints about customers being out of funds within 15 days.

In the UK the CMA required a customer redress mechanism to manage consumer complaints to ensure that complaints are appropriately dealt with between the bank and the TPP. While the regulations set out liability rules, which are particularly important in the case of a disputed payment, Open Banking is developing a Dispute Management System which enables multiple third parties to resolve disputes between themselves, speeding up resolution.

"In New Zealand, our framework requires organisations to register as an API Provider (ASPSPs) or Third Party (TPPs) and sign up to the API Centre's Terms and Conditions in order to use the API Standards. One of these terms relates to ensuring appropriate, clear customer consent is obtained and maintained. If this term is breached it may result in suspension of an ASPSPs/TPPS registration and ultimately result in termination from the API Centre. This means that the terminated ASPSP/TPP right to use the API Standards or a Standardised API with another ASPSP/TPP is revoked and they must immediately stop using the API Standards with other ASPSPs/TPPs. They must also remove any express or implied connection to the API Centre and the API Standards."



Steve Wiggins, Chief Executive,
PaymentsNZ

Most data protection regimes give the data subject the ability to raise complaints for breaking the rules around data sharing use. From this there are provisions for investigations into the claims, as well as the possibility for dispute resolution and arbitration. Depending on the outcome of the investigation and the severity of the breach there are different responses. Interestingly, in Canada it is explicitly stated that the findings of the investigation can be published.

In Mexico the FinTech Law grants Supervisory Commissions to suspend data exchange totally or partially, as well as temporarily or definitively. New Zealand similarly has the ability to terminate offenders from the API Centre and remove their APIs. Australia can revoke accreditation from the ACCC and the Central Bank of Nigeria can revoke a banking license.

"The Fintech Law of Mexico grants powers to the Supervisory Commissions to suspend partially/totally and temporary/definitively the exchange of data when the parties do not comply with the standards and the rules for the exchange"



Mariana Velázquez Suárez, Expert,
Mexico Open Banking

Nigeria, Japan, Canada, New Zealand and Mexico all have stated criminal punishments for severe breaches of the regulations. Mexico's FinTech Law specifically states that fines can be anywhere 5,000 and 150,000 Mexican pesos, and between three to nine years in prison.

"For a TPP/PSSP, licensed by the Central Bank of Nigeria, their licenses can be revoked or they can be fined. The actual fines are not codified, however, according to the National Information Technology Development Agency (NITDA) data privacy rule, companies can be fined up to N10m of annual revenue or 2%; whichever is greater."



Adédèji Olówè, Trustee,
Open Banking Nigeria



Conclusion

Consent is a complicated, but necessary aspect of data sharing and governance, especially within the banking sector where data can provide significant insights into the activities of people and organisations and where misuse of that data can lead to significant harm. Consent is inextricably tied to the legal, political, economic and social idiosyncrasies of a country, region, or market. This means that certain aspects can be hard to compare, and that regional knowledge is very important for operating across markets.

However there are some key similarities regarding how consent is given and revoked, as countries place importance on it be explicit, well-informed, straightforward, and for a clear purpose. Countries also believe in limits and punishments, though these can be varied and have a strong link to the privacy laws of a country.

Some countries have similar consent environments to each other. Australia and New Zealand have built their Open Banking initiatives off of the UK model and the three countries have similar consent environments.

The “redirect model” of obtaining consent is seen worldwide as well, from Europe to Australia and New Zealand, to Nigeria’s Open Banking environment as well.







The ability and ease to revoke consent is seen as important as to give it. Most consent environments have implemented or are implementing the ability to revoke consent as easily as the ability to give it.

Most countries have not decided on the exact length of time that consent should be granted for. Those that do fall under the PSD2 mandated length of 90 days, or in the case of Australia and New Zealand have opted for 12 months.

As Open Banking is becoming an increasingly multinational movement, and inspiring similar initiatives in other sectors, then we recommend that banks and regulators perform and openly publish further research to make it easier for people and organisations to understand the rules for consent that apply to them.

This research could deepen our work, for example by exploring whether there are differences in the definitions of terms such as ‘explicit’ and ‘informed’, but it could also cover further research questions.

Some suggestions that we identified in our work were:

-  Who is allowed to consent on behalf of a business?
-  How does consent vary across sectors and different categories of data?
-  Can people delegate consent to a third party and, if so, under what conditions?
-  How do customers understand the rules of consent?
-  How do banks and third party providers understood the rules of consent?
-  Are the penalties for breaking the rules enforced?

Continuing to research Open Banking internationally and engaging with the global community to share best practises will help Open Banking initiatives create impact and lead to a more open and trustworthy data ecosystem.

Appendix

Contributors

Name	Role	Organisation
David Beardmore	Commercial Director	ODI
Josh D'Addario	Consultant	ODI
Miranda Marcus	R&D Programme Manager	ODI
Peter Wells	Director of Public Policy	ODI
Sonia Duarte	User Researcher	ODI
Andy White	CEO	Australia Payments Network and on the Advisory Committee of Data 61
Adédèjì Olówè	Trustee	Open Banking Nigeria
Gerry Gaetz	CEO	Payments Canada
Emma Steeley	CEO	AccountScore
Jumpei Miwa	Director, Fintech and Innovation Office	Financial Services Agency
Mariana Velázquez Suárez	Expert	Mexico Open Banking
Miles Cheetham	Head of Propositions	Open Banking Ltd.
Rubén Bajo	COO	Afterbanks - Morpheus Aiolos S.L.
Steve Wiggins	Chief Executive	Payments NZ

Interview questions

- Are any important actors missing? If yes, please tell us which ones
- How do consumers give consent?
- Are there any rules that restrict who consumers can consent to sharing banking data with?
- Are there any rules that limit what the data can be used for?
- How long a time period can people consent to sharing data for?
- Can people revoke consent? If so, how?
- What are the consequences of breaking these rules?
- Does your country have specific Open Banking regulations? If not can you describe, and link to, any information on the regulations (whether current or pending) that informed your previous answers?

Supporting documents

- [How far Open Banking has come: our five takeaways](#)
- [Open Banking: Preparing for Lift Off](#)
- [How Nationwide is using Open Banking to help the 'financially squeezed'](#)
- [Open Banking in the UK and France](#)
- [Open Banking: setting a standard and enabling innovation](#)



Support and questions

For further information or to discover how Open Banking can work for you, please email:

eumarketing@equifax.com

EQUIFAX® | Powering the World with Knowledge™

Equifax Limited is registered in England with Registered No. 2425920
Registered Office: 1 Angel Court, London, EC2R 7HJ
Equifax Limited is authorised and regulated by the Financial Conduct Authority