Customer-centric design is the process of building your product or service based on the wants, needs, and challenges of your customers.

OPTIONS FOR ESTABLISHING A CONSUMER DATA RIGHT IN NEW ZEALAND

FDATA ANZ

Jamie Leach

Contents

1 Foreword

Open Finance, a precursor to the Consumer Data Right began as a grassroots movement, campaigning for the legal rights of consumers and businesses to have control of their financial data and to be able to digitally share this data with businesses of their choice. It is part of a broader suite of Open Data initiatives, aimed at empowering consumers and small businesses to access, change and benefit from the data held about them by governments and institutions.

The initiative has gathered notable momentum; various markets around the world are assessing, adopting or implementing laws and regulations to support it. In the EU, Canada, USA, Mexico, Brazil, India, Japan, Australia, Russia, New Zealand, South Korea, Singapore and many other significant markets are already at varying stages of review, policy development or implementation.

Despite these positive market developments, there is still much to understand about the versatility of Open Data and Data Portability to unlock economic potential and to improve the financial wellbeing of customers. In addition to exploring these opportunities, there are also risks and ethical considerations which will be key factors for governments and regulators in developing policies moving forward.

Research is needed to understand, measure and forecast the considerable impact of Data Portability on society and to shape public policy to ensure a Consumer Data Right creates positive disruption and the appropriate flows of capital allocation in markets, as well as to assess the techniques of regulation.

FDATA wishes to commend the efforts of the New Zealand government in thoroughly researching the form that a Consumer Data Right may take, and how this regime will positively affect the nation. These works have been supported by various groups with the intention of designing and developing a fit-for-purpose solutions.

Two groups that have been diligently participating, and thus leading this research are the Data Collective and the API Centre. FDATA commends both entity's efforts and agrees in principle that Industry can play a major role in designing and developing a solution. Their selfless and comprehensive efforts have progressed the CDR conversation and continue to assist in the exploratory process with both Industry, Consumer Groups and the Government alike. Their decision to undertake extensive research and to consider various case-studies of

international jurisdictions are important steps in this process. FDATA supports their involvement in the process, as they both play an integral role going forward. The importance of a planned and fore-thinking approach that involves various stakeholder groups will only serve to benefit the ecosystem and benefit the nation.

In order to arrive at the most suitable solution for New Zealand, working with such groups of expertise and enthusiasm, along with a comprehensive suite of participants is essential. In Australia FDATA has provided comprehensive research and advisory to Federal Regulators and the Government alike. The following sections are designed to highlight a number of essential subjects and fields for your consideration. FDATA would be pleased to provide similar services to the New Zealand Government.

New Zealand is a forethinking, world leader in legislative change and FDATA commends their attempts to learn from other jurisdictions and consider all options before deciding on their own path. We wish you all the best with the adventure ahead.

2 About FDATA

The Financial Data and Technology Association is the not-for-profit trade association leading the campaign for Open Finance across many markets and is also a focal point of that industry knowledge in the FinTech community. FDATA was initiated in the UK during the negotiations to add account data access to the Second Payments Services Directive in 2013 and was formalised in 2014.

In addition to working with EU policy makers, FDATA was heavily involved in the UK Open Banking Working Group in 2015. In 2016 the working group's output was published by HM Treasury as the Open Banking Standard.

Having helped UK regulators to shape the agenda that led to the formation of UK Open Banking Implementation Entity (OBIE), FDATA has been represented on the Steering Group and played a significant role in helping OBIE in the drive for high quality standards and in ensuring that regulators and policy makers have been kept fully involved in the challenging areas.

The effort of coordination to common standards was recognised when FDATA was invited to develop a programme of engagement amongst policy makers in many different markets. Having already launched new chapters in North America in 2017 and Australasia in 2018, the request was made by the FinTech community to continue the development across other markets. FDATA Global now has active chapters in Asia and South America from 2019, and the mandate to further expand in Asia and establish an African chapter in 2021.

Adding to the wide scope of its international representation, FDATA has also been heavily involved in the UK in developing input to assist the Pensions Dashboard programme, as well as being represented in the Steering Group of the Open Savings and Investment programme run by TISA, in the FCA Open Finance Advisory Group and in several initiatives in the domain of digital identity.

This work is intended to be an organic, iterative document and will be updated as the story unfolds in subsequent versions. It is specifically designed as a high level and convenient reference guide in this edition and will continue to expand to provide more depth in technical and regulatory matters in subsequent editions.

The Australasian chapter of FDATA continues to work closely with Federal Ministries such as the Treasury Department and Department of Finance, Federal Regulators including the ACCC and OAIC, and all echelon of Industry in the pursuit of the most effective Consumer Data Right environment and the highest level of Open Finance, and subsequent sectors, available to consumers across the region.

3 Glossary of terms

ADH	Accredited Data Holder
ADI	Authorised Deposit Institution
ADR	Accredited Data Recipient
AISP	Term under PSD2, Account Information Service Provider (FinTech that gathers customer data for its business model)
ASPSP	Term under PSD2, Account Servicing Payment Services Provider (which can be a bank or credit card issuer that offers digital access to customers).
ADH	Data Donor Institute - A firm or organisation that holds data about the data subject, that the customer may compel to share with an ADR
ADI	Accredited Deposit-Taking Institution
ADR	Data Recipient Institute - The firm or organisation who acts with the customers explicit consent to gather data from an ADH
GDPR	General Data Protection Regulation (EU wide, in force in May 2018)
IESG	UK Open Banking's Implementation Entity Steering Group
OBIE	UK's Open Banking Implementation Entity (9 largest banks current accounts delivering standardised API Access)
OPC	Office of the Privacy Commissioner (New Zealand)
OTP	One-time pin
PISP	Payment Initiation Service Provider (FinTech that enables payments between ASPSP accounts)
PSD2	Payment Services Directive 2 (EU wide, in force in January 2018)
PSU	Payment Services User (also known as the end customer)
RTS	Regulatory and Technical Standards (that have to be applied to PSD2). These have been settled by the European Parliament and were intended to come into full force in September 2019, but have been substantially delayed by technical issues in many EU markets.

SCA	Strong Customer Authentication (the method through which the ASPSP (ADH) checks that it is their customer who instructs them to perform a task).
TPP	Third Party Provider (AISP, PISP or other type of ADR acting on the behalf of the customer with explicit consent) where the PSU and ASPSP are the first and second parties.
TSP	Technical Services Provider - typically a firm that acts on behalf of a regulated ADR / TPP to get the data from the ADH on their behalf.

4 A Global Approach

Open Finance began as a grassroots movement, campaigning for the legal rights of consumers and businesses to have control of their financial data and to be able to digitally share this data with businesses of their choice. It is part of a broader suite of Open Data initiatives, aimed at empowering consumers and small businesses to access, change and benefit from the data held about them by governments and institutions.

The primary account supplier, such as a retail bank, insurer or fund manager, who is the original host of the financial data, may not be the firm that offers the best deal or the most helpful solution to the customer's problem. We can refer to these firms as being the Data Donor Institution (ADH). Having access to the customer data enables a Data Recipient Institution (ADR), often also referred to as a Third-Party provider (TPP) or Fintech, to more deeply understand the customer's needs and develop innovative and frictionless solutions that may provide a competing and potentially better outcome. This does not impact just financial services but could for example enable easier switching of utilities or organising of brand preferences in retail.

The initiative has gathered notable momentum; various markets around the world are assessing, adopting or implementing laws and regulations to support it. In the EU, Canada, USA, Mexico, Brazil, India, Japan, Australia, Russia, New Zealand, South Korea, Singapore and many other significant markets Open Finance is already at varying stages of review, policy development or implementation.

The EU has brought forward legal and regulatory frameworks to push towards an early stage version of Open Banking that focuses on the availability of payment accounts through the Second Payment Services Directive (PSD2). Open Banking is simply a subset of the financial services product verticals that could be made to move to an open architecture model. Under PSD2, money can also be moved, as well as viewed, by a suitably regulated ADR.

Despite these positive market developments, there is still much to understand about the versatility of Open Finance to unlock economic potential and to improve the financial wellbeing of customers. In addition to exploring these opportunities, there are also risks and ethical considerations which will be key factors for governments and regulators in developing Open Finance policies moving forward.

Research is needed to understand, measure and forecast the considerable impact of Open Finance on society and to shape public policy to ensure Open Finance creates positive disruption and the appropriate flows of capital allocation in markets, as well as to assess the techniques of regulation.

This may be thought of as the second phase of the Open Banking and broader Open Finance revolution, after the first unregulated version. As our understanding evolves there is a growing sentiment to extend this approach beyond Financial Services and into 'Open Life,' whereby the consumer can utilise a wider array of data points such as energy and health. The September 2020 report from BEIS, *"Next Steps for Smart Data"*, is one clear touch point on the journey to empowering customers through making it easy for them to choose to share their information with accredited parties.

As is already clear in markets such as India and Australia, Open Banking will certainly evolve to become Open Finance encompassing other areas such as pensions, investments and insurance which in turn will lead to even more transformative societal and consumer innovation. In summary, the Open Finance journey is just beginning and needs to be actively supported by a clear policy mandate for the best chance of success.

In all markets, the implementation of Data Portability has in front of it a number of different paths. Some of these paths are incredibly wasteful, largely owing to the probability of risky, costly, fragmented and overly complicated delivery, completely reducing the economic potential as a force for good. Firms that wish to utilise Data Portability want to innovate rapidly and compete in their customer-facing delivery.

Poor delivery will see these firms wastefully diverting resources to deal with the complexity, cost and risk of maintaining non-standardised points of connection or in trying to build a business model on a poor technology infrastructure. There are considerable customer-facing risks introduced by non-standardised delivery, which regulators will find it difficult to mitigate.

Many of the requirements of Data Portability should not be in the competitive space. Technical standards, security profiles and methods of dispute resolution, for example, are not improved by competition. In these areas, and in others, a single method (even if it was not as good as it should be) would outperform multiple, high-quality competing methods.

In short, the Financial Data and Technology Association (FDATA) is advocating for robust international standards, open IP, properly coordinated implementation, the framework for extensions of scope and the sharing of best practise via an international forum, backed by strong and diverse governance. Through the United Kingdom-based Global Open Finance Centre of Excellence (GOFCoE), work is now underway, and will assist in developing this international framework.

In the UK, a small number of independent venture-backed personal financial managers were developed between 2005 and 2010, which led to a reasonably public exchange of views between these new TPPs and the banks about who owned the data, whether the customer had a right to share it, or control it, and whether the process involved was undermining security. Following discussions with the Office of Fair Trading - now merged with the Competition Commission and called the Competition and Markets Authority (CMA) - and then with HM Treasury, TPP participants - often described collectively as ‘Fintechs’ - pushed for the requirement of incumbent institutions to enable access to financial data in relation to lending, mortgages, savings, investments, pension, insurance and payments. This requirement could only be established via regulation of actors in this activity.

In 2013, HM Treasury agreed to seek to connect access to customer data to the Second Payments Services Directive (PSD2), which at the time was focused on providing TPP access to payment initiation. A clear liability model for payments data sharing was to be established within a legal and regulatory framework throughout the EU. Advocates of Open Finance in the EU continue to campaign for non-payment financial data to be brought into the scope of regulation.

Given the impetus and the possibility to improve financial inclusion and introduce some innovative use cases to the end customer’s betterment, many other markets around the world are examining whether to borrow some aspects of the EU’s PSD2 and whether to follow work developed in the UK to also push for robust technical standards of delivery.

Across the globe, in markets such as India, Brazil, Japan, Australia, Canada, USA, Mexico, Singapore, Hong Kong, Malaysia, Russia, South Korea, Nigeria and in many other parts of the world, the movement to push for Open Finance is gaining momentum, although at a different pace and starting point in each market place.

As easily highlighted by policy development over the last few years in Brazil, India, Australia and Canada, the scope of PSD2 is viewed across the globe as being too narrow, and in fact, when combined with the Regulatory and Technical Standards (RTS) for PSD2 developed by the European Banking Authority with input from the European Community, are viewed now as being significantly inhibiting to TPP business models.

5 A Customer Centric Consumer Data Right

Customer-centric design is the process of building your product or service based on the wants, needs, and challenges of your customers.

Recognising the Customer in a Customer Data Right is the foundational first step to Data Portability. The Consumer Data Right must be constructed with the Customer at the heart of all design, development and delivery. All other components in this submission are underpinned by this building block. The definitions in Section 13 can be used as a guideline to establish the limits of customer ownership over data, and intellectual property or value derived by the data holders.

Customers can take paper statements and financial information to their advisers and accountants. Why should they be restricted from sharing digital information? In the digital age, customers are becoming increasingly sophisticated. They expect excellent, intuitive customer service in all areas of their lives and will pursue the best solution that time allows for. They will also demand rights and protections.

Firms (and public policy) that stand in the way of this fundamental human right for customers to share and leverage their data for their economic benefit do so at their peril. Any firms engaging in this are only delaying, as it is not a fight that could ever be won. Simply ask any voter whether they should have a data right and a right to benefit from any value extracted from their data, and the answer will be unequivocally ‘YES.’

The European GDPR states that customer data rights command:

- Transparency about how data is being used
- Access to personal information if the owner asks for it
- The ability to request that data be deleted or corrected for accuracy
- The right to object to data processing and restrict processing
- The right to have their data provided in a standard format that can be transferred elsewhere.

6 Unlocking the Potential for Open Banking

The world continues to march towards increased digital enablement. Customers from a wide range of demographic backgrounds are digitally competent. Financial services, given the lack of tangible goods that need to be physically transported, is almost uniquely positioned to be the most affected by changing behaviours. An Open Finance policy, when implemented, will reduce the risk, tidy up the liability model via regulation and accelerate the opportunity for innovation in financial services. This roadmap can then be adapted to suit each subsequent sector included in the Consumer Data Right.

Opportunities for Consumers

Consumers have the most to gain from regulated and standardised Open Finance. The simultaneous innovating to solve their problems will be coupled to better value ways of accessing and paying for the services they need and improving the timeliness of switching. Services will be more insightful and intuitive. Risk-based services will be better priced. Financial inclusion for less sophisticated consumers will improve. Friction and frustration in application, onboarding and leaving service suppliers will be radically reduced. This will all be done in a way in which their risks are being properly managed by fully regulated market actors who are ready to make them ‘whole’ if mistakes are made. In short, consumers will be able to trust the new ecosystem and avoid bad actors.

Opportunities for Businesses

Whilst generally expected to be more sophisticated than consumers, businesses will benefit from significant speed and efficiency gains, making them more nimble and cheaper to operate. Obvious use cases would be in preparing lending data, automating complex bank and accounting reconciliations, speeding up the flow and readiness of financial information and making payments and receipts more efficient.

Opportunities for Regulators

Regulators will have significant gains in understanding markets and customer behaviour, enabling them to correctly sanction bad actors and provide greater flexibility in the measures

they can use to protect customers. Fintechs have introduced an array of new business models and techniques often making it challenging for regulators to keep up. Open Finance is one significant method for regulators to gain insight into such models, as Fintech models are typically highly connected to data and measurability.

Opportunities for Third-Party Participants & New Market Entrants

Currently, TPPs and other new market entrants are at a competitive disadvantage; their ability to attract new customers and compete with incumbent firms is limited by their ability to accurately assess the suitability of customers, as incumbents can use the data, they hold on customers largely for their exclusive benefit.

Enabling access to data removes those barriers and allows TPPs to develop better, more competitive solutions. Examples include improving the quality and completion rate of affordability tests in all lending situations and enabling credit provision and alternate credit models, such as payment provisions and third-party overdrafts.

Opportunities for Incumbent Banks, Fund Managers, Insurers and Credit Reference Agencies

Incumbents can also gain from Open Finance. Many of the UK banks and credit reference agencies have partnered with or acquired fintech businesses that specialise in harnessing financial data in their business models. Other banks have chosen to occupy the TPP role, giving a facility to their end customer to aggregate information into their platform from data held with other institutions.

Applying data science algorithms over the aggregated customer data can be used for curating valuable customer insights, empowering ‘digitally-enabled’ customers and strengthening marketing strategies.

From a regulatory and compliance perspective, open banking can improve efficiency while reducing costs for identity verification, anti-money laundering (AML) and Know Your Customer (KYC) requirements, fraud prevention and customer suitability checks. Beyond the technical advantages, simply knowing the customer better can improve customer experience, digital distribution, and enable incumbent firms to be better servants of their customer.

7 Digital Identity Framework

A coordinated and standardised approach to identity is critical to the future of the Consumer Data Right. As of October 2020, there is no coordination amongst the significant range of actors tackling the digital identity issue across comparative jurisdictions, such as Australia and the United Kingdom. New Zealand is in an enviable position of not only designing a workable Digital Identity Framework, but one that is uniquely fit-for-purpose for the needs of New Zealand.

When multiple actors work on competing services globally, it is left to the market to determine the identity framework. If New Zealand were to end up with multiple competing customer identity systems operating on different standards, this would inherently limit the customer's ability to direct their data to the service providers of their choice, irrespective of the sector or industry. Not every service provider will select the identity solution framework best suited to enable the end customer to access and share identity claims across the ecosystem. The need for interoperability between New Zealand is critical for trade, but within the country, the need for a mutually agreed digital identity framework is critical for cross-sectoral productivity and ultimately, the customer's benefit.

Failing to unite puts the onus on the customer to manage more than one type of identity solution. It is tantamount to requiring the customer to have multiple adaptors for every different identity plug and socket on the market. The customer would end up having to manage a variety of identity keys, rendering the Consumer Data Right virtually useless.

When designing the Consumer Data Right, it is important to consider: the customer must be part of the trust framework. Putting the customer back at the centre of the identity framework should be part of the mission of bringing Consumer Data Right to New Zealand.

Critical work is needed to develop identity standards and a more robust consent management model. Without establishing interoperable standards, the integrity of any identity management scheme is compromised. For an equanimous digital identity utility to exist, there are core principles that must be followed:

- Implement open standards instead of proprietary competitive systems
- Promote open data principles alongside privacy and security
- Support a range of customer journeys

- Allow competition in the provision of services built to common standards, rather than having competing standards

Federated Financial Services ID for the Whole Economy

There seems to be little ambition in the UK to support a state mandated biometric identity system like India's Aardhar. Such a system would have significant long-term advantages to improve security and convenience, whilst reducing financial exclusion but would be costly to implement. In the absence of such ambition, a Federated Financial Services ID for the UK economy seems like the obvious candidate to fill the void. New Zealand has the benefit of not only other jurisdictions government-designed options, but also a plethora of proprietary systems in the market right now.

In the Nordics, such a system exists and is widely adopted, enabling the identity testing requirements that have been created to combat money laundering to be reused in easing customer onboarding with new financial relationships and to sign into existing relationships. These services are based on having an interoperable federated identity system.

Collaboration is the key to delivering a pragmatic federated identity scheme. and an ecosystem approach is required to deliver secure identity authentication. There are numerous use cases for a federated financial services ID that go beyond financial services. Cross industry collaboration is worth exploring, since identity sits at the crossroads of government, industry, and the digital footprint. Bringing the health and telco industries to discussions will be an enabler. Mobile Network Operators and financial services could easily collaborate in this domain.

Identity systems can have a few characteristics in common:

- they have users who get an identity in the system so they can carry out transactions
- they have Identity Providers, who store user attributes, ensure they are genuine, and complete transactions on the users' behalf
- they have Relaying Parties, who serve users after Identity Providers have vouch for them
- they have a governance body that oversees the system and makes the rules
- they are all based on a platform that completes the transactions by providing all parties with reliable evidence

Agreed Protocol for Authentication

Open ID Connect is a framework designed by the Open ID Foundation that is built on top of the OAuth protocol and is used to transport claims relating to a party in a particular field when data is transported through a restful API. In a federated ID model, the Open ID Connect framework would enable connecting applications to utilize the data stored across connected accounts to build a level of assurance against an individual claiming that they are who they say they are as they interact with 3rd party digital experiences, allowing users to control the security and privacy settings.

The identity framework is critical to valid authentication. Informed customer consent enables an authenticated user to transact; in fact, everything post-authentication is focused on what the authenticated user wants to allow. At the moment, there is no construct for overt awareness in the current consent systems. Using an OAuth model enables informed customer consent.

Secure authentication has three primary characteristics:

- **Pervasive**: ensures secure access across the network for all users, applications, and devices (both personal and corporate)
- **Connected**: information needed for protecting critical assets that can be shared across the security ecosystem
- **Continuous**: data collection, analysis, and action performed constantly

Continuous authentication (CA) constantly measures the probability of a particular user being who they claim to be, thus authenticating the user not once, but continuously for the duration of the session. The advantage to (CA) is a continual assessment of an authentication score which measures certainty of the account owner being the one using the device; companies can assign action constraints to each user based on tolerable risk or context. This can minimise the exposure of the most sensitive credentials and reduces the burden on the user to manage many complex passwords. Biometrics, including face-id and smart phone fingerprint readers are examples of technology that support CA.

There is also doubt to the effectiveness of SMS one-time-passwords (OTP) as a second factor for strong authentication A model of authentication that allows for storage of static passwords should be phased out and replaced by the OAuth API and paired with biometrics for convenience.

Biometrics do have vulnerabilities. Biometrics cannot replace passwords entirely because biometric information is immutable: we can't change our fingerprint or behaviour, and once it has been stolen, there is no way to reset. However, biometrics are still a valuable supplement to other authentication technologies.

Rules, Tools and Customer Experience Guidelines

Given the typically stringent requirements concerning the establishment of identity in financial services, to help, for example, ensure the appropriateness of the product for the customer, protect the financial services firm from losing money and reduce the opportunity for economic crime, fraud and money laundering, the financial services sector is in a good position to provide leadership in developing digital identity.

We also need to establish an identity to develop Open Banking. As described in the Security by Design section of this paper, the authentication methods (without intervention) will vary depending on the whether the customer has a digital relationship with the specific type of financial data.

Critical work is needed to develop identity standards and a robust consent management model. Without establishing interoperable standards, the integrity of any identity management scheme is compromised.

For New Zealand to successful develop a federated digital identity it will need to systemise the following attributes:

- The rules for an acceptable identity claim, that conform to an agreed risk tolerance per use case
- The technical standards for presenting the claims
- Customer experience guidelines for how a data subject grants consent (which may be fine grained) to enable the technical standards to perform

The rules for digital identity need to be centrally mandated. Firms and their customers need to know and trust that when they present certain data fields in a certain way, with the various methods of verification and proofs provided, that the other actors in the ecosystem will be able to rely on it. That is not to say that another actor will have to conduct business with a particular customer, just that the identity element is standardised and accepted.

It seems reasonable for New Zealand Government to pass the development of these Rules, to Digital Identity Steering Group, who may lead the industry guidance on permitted standards for identifying a customer for many years. Now is the right time to codify these guidelines and make their acceptance mandatory, to avoid different firms setting the 'bar' at different levels according to their risk appetite. In short, make some draft rules for a new federated identity system, publish them and consult on them.

FDATA believes that the organisation best equipped to develop 'open source' technical specifications to enable the rules to be expressed is the Open ID Foundation. Their open and collaborative approach would be seen as market sector neutral, and therefore would be a great way to bring the various parties in the New Zealand, working on bespoke systems or on sector specific systems into a technological discussion, and to ensure that the pathway to add the customer to the 'Trust Framework' is open.

The open standards approach would allow various vendors to establish expressions of the standard and compete to supply the technology. This is not the same as an identity vendor trying to get everyone to adopt a bespoke system. OIDFs eKYC working group is developing specificity on how the Open ID Connect framework would carry the 'claims' to underpin an identity. The variety of other identity programmes currently proliferating across New Zealand would all be included in this process and enabled to contribute their thinking and work to date.

OIDF have already provided the open standards-based method for enabling connections for UK Open Banking. This has been underpinned by a use case where the customer has already established a digital relationship with their bank. Leveraging this work will be important for situations where the customer has a digital relationship connected to their identity and might enable the Identity verification and KYC established by the on-boarding bank to be federated and reused by other market verticals.

If this was enabled by clearly established rules, then other markets where such a scenario is not possible, would be enabled to choose to rely on these identity claims or collect other attributes such as requiring the 'golden record' (birth certificate, passport, driving license) attributes to be provided to them.

In circumstances where this federated identity model does not work due to the customer having no existing digital services, or if the steering committee chose not to mandate it, New Zealand will be required to develop a methodology where the customer can establish and manage an identity, which they then pass through to the Data Holder (or another party in new

customer on-boarding scenario) in order for the customer to require the ADH to share the data with a ADR.

The challenge is that any given vertical, does not want to become reliant on another vertical, or be beholden to any system that they are not in control off in terms of standards or quality. Each firm is still on risk for getting their compliance done properly and want to be able to have cost control on this legal prerequisite to having a customer. For these reasons, the New Zealand government needs to require that the parties work together on standards.

A collaborative identity system such as this would enable the customer to share attributes that pertain to themselves as the data subject with the aim of reducing friction in their interaction, but also make it easier for firms to combat fraud and risk. There may also be an opportunity under GDPR's 'Legitimate Interest' regime, for the recipient party to share data back to the providing entity in a concerted effort collectively reduce financial crime. This adds to the mission of Interoperability cross borders.

We can also learn from the underlying principles of the UK and Australian experience guidelines when developing new capabilities.

As many of the applications operating as ADHs will be receiving data from multiple financial and non-financial verticals, it is critical that they are able to provide as cohesive a set of experiences as possible, so the customer doesn't feel that they are using multiple applications with no common journey.

Key Takeaways

- Digital Identity is a pre-requisite for a Consumer Data Right to function easily
- Not all Market Vertical Implementations will have large penetrations of digital identity in their sector
- The eKYC working group of the OIDF will provide technical standards for a collaborative New Zealand digital identity. This could be reused outside financial services and across financial services.
- If the customer has no digital connections, they still need to be able to create a digital identity when they provide their first digitally enabled data supplier with a golden record

- A digital identity steering committee would be a great place to coordinate this work, compelling cooperation across the market verticals and ensuring problems are solved and customer experiences are thoughtful.

8 Governance

Policy, Legal, Regulatory and Implementation

It would be helpful for the New Zealand market to have a simple and clearly articulated mission and policy vision for their Data Portability, to provide context to the law makers, regulators and implementers for each difficult decision.

Example Statement

“The Consumer Data Right in New Zealand will be designed around the end customer, putting their needs to the fore. The intention of the policy is to enable free flow of the customers data between regulated actors of the customers choosing, as exercised with their explicit consent.

The purpose is to stimulate innovation and competition to drive better customer outcomes. This can be measured in a number of ways, such as financial improvement, but also in feeling better informed or more in control. The Consumer Data Right should reduce barriers to switching or comparing products by making decisioning and actions easier to accomplish.”

Each recipient of this data, will be required to be regulated, adequately insured and party to the New Zealand’s Consumer Data Right system of customer redress.

- The ecosystem will be orchestrated and led by the designated Ministry of the New Zealand Government.
- The Sectors will be Open Banking, Open Energy, Open Telecommunications, etc.
- Each Sector will be supported by a diverse and representative group of stakeholders, constructed of a blend of Industry, Consumer Advocates, Domain Experts, International Representatives, etc.
- Each actor must abide by the technical, regulatory and ethical standards agreed under the regime and must transparently conform to these rules.
- All regulated firms will be required to fund their entry and operations. The New Zealand government will fund legislative reform and regulatory operations.
- Whilst competing in the market, participants are required to collaborate to ensure qualities are maintained and risks are mitigated.”

Regulatory Alignment with Market Situation

The use-case of Open Banking is not new. Third-Party Providers (TPPs) already act on behalf of customers to aggregate financial data from multiple sources in the unregulated space. To ensure continuity in the market, any new solution which interrupts the 'Live Market' of firms operating in this domain will need to be blocked from going live until they are accredited and comply with the Consumer Data Right.

The learnings from the UK experience, particularly around Strong Customer Authentication interrupting access via screen scraping before the new API technology was ready for service, is a critical learning point.

1. There must be alignment across delivery timetables and clear management of any inconsistencies that might create end customer and marketplace problems for existing services.
2. There must be an application and approval process for ADRs, similar to AIS providers under PSD2.
    a. This must include technical standards, security configuration, data privacy and audits against permissioned standards.
    b. This must include obligations placed on the data recipient, depending on their business model, to only take data types and longevity of access appropriate to their business model, and to show authorities that value continues to be exchanged between the ADR, and TPP and their customer. This should include some risk analysis and mitigation plan.
    c. There must also be a test of whether the application has adequate liability insurance cover to be accepted into the market.
3. There needs to be a process to remove or suspend an ADR from the market if it is not meeting the obligations of its permission or if it has suffered some security or data breach.
4. There must be a method of sanction against nefarious actors which seek to operate without regulated ADR status.
5. There is a need to support a digital certificate issuing capability and for the regulated status of actors to be easily determined.

6. One aspect of Banking regulation which would need consideration before Open Banking regulation is brought forward is the risk weighting between actors on the TPP side. Comparative frameworks have the customer facing TPP as the regulated actor and required to supervise any supporting actors in their chain of data custodianship. In reality, many Technical Service Providers, who play a role in getting data for TPPs when the customer provides consent, are very significant actors with huge volumes of customer data but no requirement to be regulated under the UK example. Relying on new start up TPPs in the regulated customer facing role to adequately test and supervise very large technology companies is creating a range of risks. The Australian CDR is seeking accreditation and governance oversight of participants at all level of scheme.

7. Whilst there is a certain logic in the customer facing role being regulated so that the customer is sure who to complain to when they require redress, it creates some challenges in creating a complete liability model as those actors with the highest volumes of data may remain unregulated. If any actor stores customer data, they are logically capable of being hacked. Therefore, in any new CDR format, policy should contemplate making every actor in a value chain responsible for the data that they hold on a customer. This may, in turn, enable more flexible business models where the hurdles for becoming a regulated actor are more risk balanced rather than singular.

8. Whilst regulated actors will have an obligation of reporting a security breach to the appointed regulator, there needs to be further consideration of the tools and skills available to the regulator to undertake traceability assessments when there is a suspicion that an actor may have lost data so that;

    a. a company can be compelled to take responsibility

    b. the Financial Ombudsman / Privacy Commissioner could be reasonably informed

    c. customer redress systems are in place and fully tested.

9. Where an actor is deemed to be no longer competent due to an emerging or perhaps a sustained issue, the technology, architecture for CDR should enable the regulator to quickly disconnect the participant from the directory, disabling the ability of an ADR to continue to access data. Whilst that does not reduce the ongoing risk in the data that the ADR already has stored in their database, it does at least enable some ability for the regulator to show that the problems are not being permitted to get worse.

10. The timing of market entry is important to consider in the context of fair competition. For example, we need to ensure that certain actors categorised as large incumbent providers are compliant with their requirement to be ready to share as an ADH on or before the date when they occupy the ADR role. The potential for systemic volume failures of data transmissions have plagued a number of jurisdictions internationally.
11. The regulation and policy should provide sufficient force to compel actors to participate within a timeframe.
12. The Privacy Commission should deliver a single customer redress and arbitration process to deal with issues arising for end customers, whether they be consumers or businesses. Competing dispute resolution capabilities are simply non-functional in the same way as competing air traffic control systems would be hazardous.

9 Principles Based Approach

Getting the balance right of appropriate responsibility at each level of market interaction is important.

It could be argued that in most circumstances that a few key principles could helpfully be enshrined in law. The customer's ability to enforce control of their financial data and how it might be used may need the fundamental protection of the law. Open Banking creates data mobility for financial data. GDPR creates some rights of universal portability, with a number of jurisdictions adopting these principles without implementing the overarching legislation.

One helpful definition to clarify the difference is that 'portability' enables the data subject to get data back to themselves in a machine-readable format, whereas mobility enables the data subject to compel through explicit consent one regulated actor to share specified data with another regulated actor. In addition, creating clarity in the liability model and who would pay in certain situations, might make it easier for the regulatory interpretations to develop more easily.

The law is not a great place to assert technical requirements or the development of lower level policy surrounding implementation. There needs to be sufficient head room for regulators and leaders from the commercial space to solve problems and make adjustments to fulfil the policy objectives intended. It helps to have a really clear statement of the principles and overarching objectives and for the regulatory leadership to engage in understanding the policy requirements and consult with the market participants.

10 Consent

Explicit consent is crucial. The ADR **must** get customer consent for both the service offered and the data points required to perform the service. Consent should be a defined term, written in plain language. It should never be buried in terms and conditions.

Should the customer elect to revoke consent, it is essential that the ADR has a means of discovering/being notified that this has taken place, as their business model may depend on continuing access to data. As such, revoking consent could necessitate the severance of a contractual relationship between the customer and the ADR. There may be, for example, an important alert, line of credit, renewal window or some services provision that is effectively tethered to the access - the customer should be aware of any break in contract and any resulting impacts. ADRs should make clear to customers that they have the right to revoke consent, but also that doing so will prevent the ADR from continuing to offer services. This supports the need for defined terms, written in plain language.

The ADH should be aware of the data provided by the customer to the ADR but should not know the details of the proposition offered by the other part of the consent model. Specifically, the ADH needs to be prohibited (in processes and in regulation) from using any knowledge of the ADR consent to generate automated counter-marketing. The ADR won the customer's business in fair competition and the ADH should not be able to use a unique advantage of the consent connection to compete in a way that is not open to other competitors. An example of this would be where the ADH sees that their customer has connected a new app and uses that knowledge to communicate with the customer offering a competing service, which would not be an activity that is open to other competitors.

It is important that the ADR offers to the customer a time bound consent if the service is time bound. If the service is not time bound, like a money management service, the customer should be able to set the length of consent. The ADR should be required to remind the customer that the consent is in force on a regular cadence to ensure the customer is still getting value. We recommend that the ADR is required to communicate through the agreed channel that they are collecting data at least once a quarter, and that the ADR should always make it easy, using a standardised consent dashboard, for the customer to choose which consents to revoke – whilst providing clear information on the consequences of any termination of access.

11 Privacy by Design

Confidentiality is breached when a person is re-identified through a data release, data sharing or when information can be attributed to them. The likelihood of this happening, or risk of disclosure, is not easily determined. The implementation of enforced data sharing and release as per a Consumer Data Right heightens the fear of a breach occurring, but does it need to raise the risk of such an event?

A key challenge for data custodians is to provide data with maximum utility for users but still maintain the confidentiality of the information. Technology is playing an ever-increasing role in protecting both the end-user, but also the supply chain at every step of the process. The introduction of Compliance Technology or Regulatory Technology is propelling tech-enabled adherence to policy, rules and legislation.

One commonly adopted framework for assessing risk associated with data portability is the Five Safes Framework. This framework provides a structure for assessing and managing disclosure risk that is appropriate to the intended data use. This framework has been adopted by the Australian Bureau of Statistics (ABS), several other Australian government agencies as well as national statistical organisations such as the Office of National Statistics (UK) and Statistics New Zealand.

THE FIVE SAFES FRAMEWORK

The Five Safes Framework takes a multi-dimensional approach to managing disclosure risk. Each ‘safe’ refers to an independent but related aspect of disclosure risk. The framework poses specific questions to help assess and describe each risk aspect (or safe) in a qualitative way. This allows data custodians to place appropriate controls, not just on the data itself, but on the manner in which data are accessed. The framework is designed to facilitate safe data release and prevent over-regulation

The five elements of the framework are:

- Safe People
- Safe Projects
- Safe Settings
- Safe Data
- Safe Outputs

12 Security by Design

Technical Design of Consumer Data Right

It seems sensible to deliver the Consumer Data Right using modern restful APIs. An API has essentially two components:

1. The Security Profile
2. The Data Payload

It is somewhat similar to standardised electrical outlets. The Security Profile is both the socket and the plug. If it is not exactly standardised, the connection is not possible or made. The Data Payload is analogous to the electrical appliance powered by the successful connection.

Security Profile choices

The key challenge in developing the common plugs and sockets is in whether the end customer has a digital identity, backed by a sufficient identity check or KYC, that would enable the identified customer to prove they were the data subject, or are acting for the data subject, when they go through the Consent Flow.

In the UK Open Banking, the API Consent Flow redirects the customer from the accredited data holder (ADH) to the accredited data recipient (ADR) to enable the ADH to identify that this it is their customer, using the typical method that the consumer uses to Authenticate themselves with their provider. This works elegantly in the banking sector and should translate to other sectors, because most customers have established a unique digital identity with their data holding service provider, i.e. bank, electricity retailer, to connect to online or mobile app via a login screen.

Other than redirection (from the ADR or app provider to the ADH) to complete the Authentication step, the other significant Authentication technique is referred to as being ‘decoupled,’ which is a methodology whereby the ADH could sends an ‘out of band’ pin code to the end customer through a different channel (OTP authentication), who then proves they are in possession of their mobile device, entering the pin in the ADH interface. This extra obligation on the customer creates an additional and unnecessary layer of complexity on the customer.

13 CDR Data

For clarity, it's simple to consider data in four categories:

1. **Customer-provided data** – provided directly by customers to their bank

Examples: contact information, financial history, payee lists for bill payments, demographic details, etc.

Customers clearly 'own' this data and should be able to dictate it be shared without restriction. The repetitive process of continually providing this information can be a barrier to switching providers; if a customer opening a new account could simply direct their current provider to share their personal details with a new provider, it may significantly reduce the friction of switching. The sharing of Customer-provided data, or Personal Information will lead to new innovative products designed to enhance the customer experience and add to the competitive environment of financial services and digital identity frameworks.

2. **Transaction data** – generated through transactions made by a customer's account

Examples: withdrawals, transfers and other transactions; account balances, interest earned and/or charged, etc.

Transaction data should be shared, at the direction of a current or former customer. Regulators need to consider the amount of historical data that may be required; an open-ended period would put an excessive burden on data holders and we can expect advancements in digital archives and records as time progresses. In many jurisdictions, regulators have determined that a pragmatic approach is that data holders may only be obliged to transfer data for the same period they are required to hold it for existing regulatory obligations.

3. **Value-added customer data** – data that results from an effort by a data holder to gain insights about a customer

Examples: credit scores; income/assets verification; customer identity verification; data on an individual customer that has been aggregated across the customer's accounts and standardised, cleansed or reformatted.

While the primary data was likely provided by the customer or generated by the customer through transactions, the true value is being derived through actions taken by the data-holder. Sharing this data would represent a transfer of value from the data-holder to the customer (or a TPP) and may breach intellectual property or commercial agreements. **Generally, this is outside the scope of open banking. For similar reasons, pre-aggregated data sets should also be considered outside the scope of Open Finance.**

4. **Product data** – Financial data for which there are no CDR consumers

Examples: eligibility criteria, terms and conditions, pricing, performance of a product or instrument, accessibility, process or procedure, etc.

Determining the products scope is also critical. The Australian government, in its open banking review, concluded that transaction data should include products relating to the conduct of banking business as defined in its banking act, but only for those products that are widely available to the public. Other jurisdictions are likely to follow a similar approach.

Examples of products generating transaction data (from the Australian Open Banking Review

Deposit Products	**Lending Products**
Savings accounts	Mortgages
Cheque accounts	Business finance
Debit card accounts	Personal loans
Transactions accounts	Lines of credit (personal & business)
Personal basic account	Overdrafts (personal & business)
GST and tax accounts	Consumer leases
Cash management accounts	Credit & charge cards (personal & business)
Pensioner deeming accounts	Asset finance (and leases)
Mortgage offset accounts	
Trust accounts	
Retirement savings accounts	
Foreign currency accounts	

14 Technical Standards

Learnings from PSD2 and UK Open Banking

For anyone to truly understand the challenge of delivering the UK Open Banking environment, they must firstly understand that the level 1 text ‘PSD2’ was written to be technology neutral, and assumed that the TPP would access the customers data, with their explicit consent, but using their secret static passwords to scrape data from their internet banking channel (Screen Scraping).

The development of the plan in the UK to move to an API approach, had an impact which has been little understood. The fundamental shift was not in the technology choice or the security, but in the party responsible for building it. In the credential sharing model (the old technology sometimes referred to as ‘screen scraping’) the design and quality of the technical build was squarely with the demand side - firms who desperately needed it to work because they were consuming the data in their business model.

As we introduced the shift to APIs, the burden of build was shared between the supply side (some of whom were fearful of it working too well in case it created a competitive threat) and the demand side. The only way to neutralise these competing interests is through the development of technical standards, compulsory adopting of these standards across the industry, pass/fail testing of conformance to such standards, and tight regulation of performance. The idea of making harmonisation work through incentivisation alone, is lacking logic, as commercial interests are simply not always aligned by the same incentives and at the same times.

As we can see across the UK (outside the CMA9) and across the wider EU, the execution of APIs to support PSD2 has mostly failed, largely driven by a failure of policy makers to understand - early enough in the policy development - the fundamental shift in technology roles and quality control as we moved to APIs. Outside UK Open Banking, the ASPSPs (supply side) had been left in complete control until it was too late. It is critical that Open Finance takes advantage of this now obvious learning. Design the regime before going live. Don’t attempt to make critical changes at the eleventh hour.

There is tremendous value in establishing technical standards, from both a technology and an implementation perspective. The advantages include:

- Reduced complexity and risk

- Protecting customers and all market participants in a cohesive ecosystem by creating certainty that TPPs can offer a complete service to all their customers
- Reducing the API build and maintenance costs for ADRs and ADHs
- Minimising security costs by significantly reducing the range of penetration testing permutations and audit requirements
- Enabling investment in customer-facing innovation, rather than tying up resources in the maintenance of plumbing
- Making it easier for smaller firms to participate, improving fairness and competition
- Simplifying the ability to trace issues, assess fault and allocate loss, which makes it easier to establish a liability model and better enables cyber risk insurers to assess threats and perform during the underwriting and handling of claims
- Creating clarity for ADHs, ADRs and regulators by providing clear, consistent guidelines for compliance (and simplifying the process of adjusting market standards as time progresses)
- Reducing barriers to innovation, as creating consistency in data output will simplify the development process for ADRs
- Enables more rapid growth and better sharing of best practices across jurisdictions

Although the strengths of establishing technical standards far outweigh the weaknesses, there are cases in which standardising may create complications. For example, if a bank has pre-existing APIs that are materially different from the standard, there may be resistance to re-designing the output. In some cases, banks may have already established an “API strategy” that they feel creates competitive advantage. It may be possible for these firms to comply with the market standards while also offering services that go beyond the standard to encourage partnership models.

Some TPPs have argued that standards reduce their ability to innovate. In certain circumstances, relating to the Consent Flow, there is a danger of standards being used to slow down innovation. This can be mitigated by arranging a governance model enabling Consent access capabilities that give the market clear direction at significant scale. Given that Open market models are inherently two sided, creating common standards on how things connect is a necessity, but must be backed up by diverse stakeholder representation in governance, otherwise one type of actor decides what is good for another type of actor without consulting with them.

Guiding Principles for Establishing Technical Standards

1. Force simplicity as a design principle, as the alternative complexity is unsustainable from a cost, risk, scalability and time perspective
2. Forced simplicity requires compulsion and standardisation, which protects every market participant who wants to see a better market facing outcome
3. Recognise that specification and standardisation are not the same thing
4. Do not let ADHs decide to build their own API specification to comply with minimum described functionality. They can build additional functionality if it suits their business needs.
5. Ensure that regulation requires conformance to the standards. These should be tested using a technical instrument, providing a pass/ fail result.
6. Standardisation is not possible without both an implementation entity and regulatory environment that is capable of imposing it or an ecosystem that understands the mutual benefits of being subject to it.
7. Many of the reasonably expensive tool sets built for Open Banking were designed to scale and to be flexible. They are therefore reusable and considerably reduce the overall cost burden across the ADH and ADR communities.
8. Now that many ADHs are also operating in the ADR role, it is getting easier for them to understand the necessity of standards.
9. Standardisation requires that conformance test suites need to be applied and tested on the ADH test environments or on some intermediate pre-production models and then also in production.
10. ADRs need to also be tested for conformance to the security profile as part of their regulatory journey and thereafter.
11. Test suites need to be applied through the point where the customer Consents, to test functionality and that the API supports the appropriate fields.
12. Optionality does not typically drive innovation in the same way that standardised outputs enable innovation, so the minimum threshold of API data payloads should be clearer.

13. API performances need to be measured and published on a regular basis, showing uptime availability, response speeds, technical fail rates and any rate limiting settings. The published results should also form a single source of truth, whereby the FCA and commercial actors can be confident that firms are being treated in a fair way and that sanctions will be implemented against actors who fail to comply. The test of uptime availability for Open Finance should probably track to the PSD2 test in the short term, of being at least as available as the ADHs (ASPSPs) own customer facing digital channels. Flexibility in the regulation should enable this to be amended in the event that a firm deliberately reduces their digital channels to restrict competition.
14. The investment in standardisation testing tools pays off and does in the long run reduce costs, wasted time and risks, but does require an implementation body to deliver it and some form of independent monitoring or certification capability
15. A directory capable of managing the local and cross border identities of permissioned actors is of key importance, as it will also enable API endpoints to be displayed in a common pattern and enable faster onboarding.
16. For smaller ADHs without the resources to validate thousands of ADRs, this is particularly useful during the period where eIDAS is not widely delivered in all EU markets. The UK should contemplate phasing out eIDAS, which is not fit for purpose, and for UK domiciled businesses to rely on the interplay between the Directory Software Statements, and the regulatory status.
17. Having more than one directory (using the definition of a directory whereby there is a single source of truth of the identity and regulatory status actors, and where that directory is part of the Trust Framework) or a competing dispute management system may prove to be unhealthy competition as it will artificially create a complexity layer without adding value. This is the central infrastructure to protect customers and market participants and needs to be uniform.
18. Enforce testing against the standards and publish the results.
19. Improve the levels of commercial certainty for participants, by undertaking realistic impact assessments and then being explicit with requirements.

International Alignment

Both of these security profiles have been developed and standardised by the Financial Grade API (FAPI) working group of the Open ID Foundation, which is a not for profit organisation sponsored by the world's leading technology companies to drive standardisation and interoperability. The output is Open Source and available to all. International working groups are established to develop threat and vulnerability analysis, developing security approaches which keep current with the threat vectors. In the UK a conformance test was built for the FAPI security profile by the Open Banking Implementation Entity (OBIE), and then gifted to the Open ID Foundation to use in other international deployments.

The Global Open Finance Centre of Excellence (GOFCoE, see below) established in Edinburgh, is providing the secretariat and API curation services for a new international standards body, the Global Open Finance Technical Standards - Working Group (GOFTS - WG) which is co-chaired by FDATA Global and the Open ID Foundation (OIDF). The GOFTS-WG has a remit to seek alignment and convergence amongst the various international initiatives that are working on API technology and security of exchanging financial data.

If successful, not only will it reduce the security risks, but may contribute significantly to improvements in global GDP, by reducing the enormous economic friction of non-standardised ways for sharing data and making connections.

High Level Architecture of the Consumer Data Right

With UK Open Banking having created a number of important infrastructures and capabilities, we can now move to an accelerated cadence of delivery, by creating a federated technology, governance and funding model for UK Open Finance.

From the Customer Data Right, role of Explicit Consent, Liability Model and the Legal and Regulatory Framework, we can easily develop a set of high level and logical market requirements for the technological implementation of the Consumer Data Right in New Zealand.

Market Requirements

1. New Zealand should commit to driving and adopting international standards for APIs, especially in the suite of standardised security profiles. The commitment should be to clearly follow the recommendations of International working groups, such as the FAPI working group, for each security profile method and to play a full role in helping to shape, test, revise and promote these international standards. **This international scrutiny and cooperation are highly beneficial in creating a secure environment for Open Banking and the wider digital economy.**

2. An eKYC federated identity standard (see below) is essential if we are to move Data Portability into financial sectors with low digital penetration, enabling customers to pass through their identity claims to initiate the Consent Flow.
    a. FDATA again recommends that New Zealand uses the Open ID Foundation working group on eKYC as a platform to bring the various competing financial services digital identity schemes together into a common interoperable technical standard.
    b. Open ID Foundation is an international not for profit working on the technical design of APIs to improve security and trust. Their experience and neutrality give the CDR the best chance of aligning identity systems and making them interoperable across market verticals. This will also make it easier for international firms to enter the New Zealand and for New Zealand domiciled firms to internationalise their offerings.

3. All ADHs and ADRs will be regulated actors and must identify themselves and their permissions when connecting to each other to initiate payments or transfer data.
    a. Each regulated actor must present a software certificate when making a connection and must digitally sign the certificate with their cryptographic key when presenting a connection.
    b. The certificates should be issued by the implementation body for the CDR. Reliance on the existing digital systems should be eliminated at the earliest opportunity. The technology and process behind the European system is currently suboptimal, and was adopted by the United Kingdom initially. FDATA has urged the UK to change its course. It is clear that the UK trust framework

for Open Banking was more cohesive without eIDAS and the reliance on Qualified Trust Servicing Providers (across the EU) to issue them.

c. The certificates should clearly show the permissions of each actor, and the financial verticals they are entitled to connect too.
d. All ADHs and ADRs wishing to operate in New Zealand, even if regulated in another domain, must be enrolled on the Directory, a technology and offline process that will be recorded as a shared industry utility.
e. The responsible regulator should develop its own API to enable the Directory to digest and update the permissions of each actor.
f. Each actor will be able to check the validity of the certificate of another actor on the directory. This central authority is a trust framework that reduces certain types of fishing and spoofing attack.
g. Should the regulator decide that an actor be removed or suspended from ecosystem, they simply have to update the API.
h. As New Zealand develops eKYC standards and harmonise it with the Directory, you will naturally extend the Trust Framework beyond the data sharing between the regulated actors, and their TSPs, and out to the clearly identified end customer, creating a chain of identity of the actors who are supposed to have the customers data.
i. In the longer term, the Directory might consider the feasibility of building onto the existing framework a record of the end customer consents that underpins the traceability of data connections between all actors and then connect this to a universal Customer Redress System (CRS) for the Consumer Data Right.
j. Going further, it might be reasonable to require each ADH to provide a Unique Resource Identifier (URI) which is essentially a sequentially generated numeric code for each transaction or value in the payload of a given API. The ADH would send the data payload via their bilateral API with the ADR and send to the central system the unique identifier of the Data Recipient Institution and the Unique Resource Identifier. This would therefore be generating a log file of which regulated actor has particular data without holding the data itself. This would be used in helping to deliver an effective CRS, and aid in more rapidly reaching any settlement of disputes between actors.
    i. From a technology perspective, a distributed ledger might work well to store this information, as it has inherent characteristics of transparency

of activity, privacy of parties, slow rotation speed and longevity which would be required for a such a system.

4. Each ADH should deliver and maintain the standardised API technology that is agreed for their Market Vertical Initiative (MVI) in the governance model including
    a. A FAPI conformant security profile (the plug socket)
    b. A regular test to ensure conformance to the security profile
    c. Availability of the mandated fields in the data payload
    d. Performance levels (availability, responsiveness, scalability, etc) which are agreed in governance as the acceptable standards and enforced by the regulator
    e. Capacity to enable the ADR to connect multiple times per day
    f. Web hooks to enable the ADR to just request an update to any changes, to reduce the requirement for data polling
    g. A URI system compatible with the guidelines
    h. A method for coping with the agreed Consent Flow, including 'fine grained' consent, which would enable the ADR take clusters of data that they require to perform their business model, but not necessarily all data fields that might be in the payload.
    i. A method of enabling connections by Technical Service Providers
    j. Fully conformant user experience to the agreed Customer Experience Guidelines, including flows that run from Web to Web, App to Web, Web to APP and App to APP
    k. A method of connecting to the CRS and the central directory

5. Each ADH can also choose to be an ADR and build all of the requirements to be an ADR
6. Each ADR must deliver and maintain the standardised API technology that is agreed for their market sector in the governance model, including
    a. A FAPI conformant security profile (the plug)
    b. A regular test to ensure conformance to the security profile
    c. Conformance to Customer Experience Guidelines and ability to manage fine grained consent
    d. A method of connecting to the CRS and the central directory

With both the UK and Australian Open Banking regimes having created a number of important infrastructures and capabilities, we can now move to an accelerated cadence of delivery, by creating a federated technology, governance and funding model.

15 A Phased Approach

There have been different approaches to the introduction of data portability across the globe. One country may choose to focus on the single sector (UK Open Banking), while another country may choose to focus on one form of technology initially, with the intention of adding a further layer of complexity at a later date (Australia with Read/Write Access). While FDATA supports the concept of an economy-wide data portability framework, the ability to conquer one layer of complexity at a time is not uncommon.

Sectoral Approach

In Australia, the CDR is scheduled to be implemented in the banking sector as 'Open Banking'. Unlike similar regimes in the UK and the EU, the Australian approach to consumer data regulation is designed to eventually be implemented on an 'economy-wide' basis. It is currently anticipated that a phased roll-out to the energy and telecommunications sectors will occur following the full implementation of Open Banking, with superannuation and insurance being other probable priority sectors for CDR deployment.

One benefit of implementing the CDR regime sector by sector, and on the basis of specific categories of CDR data, is that the Government and Regulator can learn from the successes and the failures of the earlier sectors to ensure that the regime functions properly.

Despite a phases approach, we believe that a single technical standard, governance framework, liability structure and data standards must be adopted to ensure a cohesive and productive economy-wide implementation.

Read/Write Access

Granting write access would align a New Zealand Open banking regime with Europe's payment services directive PSD2 and potentially the Australian equivalent if adopted in December 2020, and would allow better comparison services and life administration offerings to be created using banks' data.

In its current format, Australia's Open banking regime is limited to "read" access only, meaning that data recipients and customers can not modify existing data, nor alter existing

products directly. By introducing write access, there will be ramifications beyond the banking application. In an energy scenario, enabling write access may allow a customer to open a new account, make changes to their account, or close an account, seamlessly through a third-party. That may be a business, a service or an application. This will enable a greater level of convenience and efficiency in comparing and switching service. Customers will be able to access, in real-time, a personalised offering, or avoid often dreaded cancellations interactions with service providers.

A Scott Farrell issues paper writes, "consumers would be able to see a single dashboard of products and plans they have across banking, energy and telecommunications, such as the cost and time remaining on each account, balances and due dates for bills. Customers could get alerts in real time when better deals become available. The write access would then let them act on such alerts, such as by closing one account and opening a new one with a few button pushes."

The United Kingdom's CMA Retail Banking Market Investigation Order links the delivery requirements for UK Open Banking explicitly with PSD2:

10.1.2 both read and write access, which allows a third party to access account information or initiate a payment on behalf of the customer (subject to the customer's explicit consent), for data set out in Article 14 (the 'Read/Write Data Standard') and which has the features and elements necessary to enable Providers to comply with the requirements to provide access to accounts subject to this Part 2 of the Order under PSD2.

For all the anticipated benefits, including write access does heighten the risks associated with the regime and the players involved. New Zealand must give considerations to time constraints of technical readiness, user demand offsetting technical investment and the potential limitations that will be uncovered within business architecture. Perhaps the most concerning issue of including write access in a Consumer Data Right is the potential for a cyber attacker to exploit the functionality of the system to defraud customers while breaking data holder IT systems.

16 Reciprocity

The regulations of the CDR should have a core principle of enshrining the customer data right in this domain by enabling reciprocity. If the customer is able to choose where they wish their data to be shared there should be a clear two-way technology solution to enable that. Firms wishing to access data held on behalf of their customer with another party should themselves be willing to make data that they hold on that customer available to another party. That does not mean that an actor could keep out of complying with CDR requirements by not choosing to gain data from another party.

The policy should have compulsion as a central artefact where no party pays another for access to data that is the customer's data.

17 CDR Participants

The approaches taken by Australia and the United Kingdom in determining and mandating the accreditation and responsibilities of various Consumer Data Right participants are substantially different. With legislation and approaches differing, each jurisdiction has taken a course of action supported by the catalyst to their regime adoptions.

In the United Kingdom, Open Banking has been largely led by changes to their payment's laws. The CDR participants are separated into four categories with clear definitions and obligations:

- Account Providers – ASPSP – Banks and Building Societies
- Third Party Providers – AISP – Account Information Service Providers – Entities that collect and utilise consumer data
- Third Party Providers – PISP – Payment Initiation Service Providers – Entities that collect and utilise consumer data and initial the movement of consumer funds
- Technical Service Providers – TSP – Entities that work with accredited providers to deliver on their open banking solutions

In comparison, Australia has chosen to take a significantly more complex approach;

- Accredited Data Recipient
- Accredited Person
- Outsource Service Provider
- Authorised Deposit-Taking Institution (ADI)
- Restricted ADI
- Combined Accredited Person Arrangements (CAP) – Principal and Provider
- Intermediary
- Sponsored Affiliate
- Trusted Adviser
- Restricted Accreditation
- Unrestricted Accreditation
- Local Agent

- Foreign Entity

As with the development of any regulatory reform or technology designation, the simplicity of the system may aid with greater compliance and a reduction in perceived barriers to entry.

Confusion has been experienced across multiple jurisdictions in regards to accrediting entities that have several domiciles and mixed business models. Two examples of this include Cloud Accounting Software providers and data aggregators. Excess classification and failure to accept the complexity of business models will lead to additional barriers to entry, or in some cases, severe hardship to trading entities.

18 Submission on discussion document: Options for establishing a consumer data right in New Zealand

Your name and organisation

Name	Jamie Leach
Organisation	FDATA Australia/New Zealand

Responses to discussion document questions

Does New Zealand need a Consumer Data Right?

1. **Are there any additional problems that are preventing greater data portability in New Zealand that have not been identified in this discussion document?**

Overall, FDATA believes that each example disclosed throughout the discussion document highlights the foundational principles of establishing a fit-for-purpose Consumer Data Right. We acknowledge the high-level of details disclosed in the document, and recognise a significant amount of work that will go into investigating and establishing the necessary elements of the New Zealand regime.

The fragmented approaches that the discussion document depicts are not unique to New Zealand, and is it no surprise that singular approaches, by individual groups, have not yet succeeding in delivering a successful working solution.

The Consumer Data Right concept, or its equivalent such as Open Banking, has gathered notable momentum; various markets around the world are assessing, adopting or implementing laws and regulations to support it. In the EU, Canada, USA, Mexico, Brazil, India, Japan, Australia, Russia, New Zealand, South Korea, Singapore and many other significant markets Data Portability is already at varying stages of review, policy development or implementation. And yet, no two jurisdictions have adopted the same approach, legal standing, nor technology.

New Zealand is not alone in attempting to design, develop and deliver a new regime, however, there are considerable advantages to learning from other regions and nations. New Zealand is globally recognised as being agile and nimble, able to create, document and pass legislative changes in only a matter of days, when other countries take years to achieve a lesser result.

In addition to selecting a suitable approach to your CDR design, development and delivery, other barriers present:

- New Zealand currently suffers from a lack of a competitive environment to force greater innovation. A lack of scale, or burgeoning technology partnerships with other jurisdiction hamper this development. The benefits of innovations are not sufficient motivators for large-scale change across traditional industries.

- Data Portability and a Data Right will be a new concept to the majority of New Zealand citizens and extensive Public Awareness and Education will be necessary to achieve the desired outcome that a Consumer Data Right promises.

- Irrespective of the approach that New Zealand adopts there will be significant regulatory and legislative reform necessary to bring New Zealand into a globally competing landscape.

- Designing, developing and delivering a Consumer Data Right will be a costly exercise for all involved. This cost will be borne by Industry, Government and Society in some cases. Large-scale entities will experience substantial costs associated with updating and transitioning technology stacks to embrace nimble and innovative change. Irrespective of whether New Zealand adopt a Consumer Data Right, Industry will be required to make this investment to stay competitive in a constantly evolving technology-driven landscape. There is a trade-off between the costs to existing organisations being balanced by the potential for greater benefits to society. The massive banks of Australia and the United Kingdom presented these obligations as roadblocks to prevent and slow down the

implementation of regimes in each country. While they were able to pivot to support the new regimes, they attempted to delay their regulatory requirements for as long as possible.

2. Do you agree with the potential benefits, costs or risks associated with a consumer data right as outlined in this discussion document? Why/why not?

We agree in principle with the benefits and costs/risks outlined in the discussion document. There are additional benefits and several perceptions of risks that have been experienced by other jurisdictions across the globe.

Additional Benefits:

- Consumer Empowerment and Education
- Increased Innovation and Cross-Sectoral Collaboration
- Facilitation of Competition and Growth
- Increased Privacy Controls and National Data Protections
- Increased Productivity, measured by Economically and through Citizen Welfare
- Greater Technology Interoperability
- Greater National Collaboration with external Trade Partners

Additional Perceived Risks:

- Increased data sharing will lead to increased privacy and security breaches **– False**
- The implementation of a CDR leads to barriers to entry for new players **– False**
- Increased regulatory and legislative oversight strangles Industry **– False**

Each of these perceived risks have been raised as opposition to International Data Portability and Data Sharing regimes. No examples of the above have been registered.

3. Are there additional benefits, costs or risks that have not been explored in the above discussion on a consumer data right?

Based on our International observations, we believe that there are additional benefits that should be considered when designing and implementing a CDR.

A well-designed CDR can;

- Promote Financial Inclusion, (Nigeria, Kenya, Mexico)
- Poverty Reduction, (Nigeria, Brazil, Mexico)
- Greater Access to Technology, (Australia, United Kingdom, Brazil, Japan, Europe, Nigeria, Kenya, Mexico)
- Removing Barriers to Education, (Every jurisdiction – Financial literacy and education continues to rate low on every nations scale), and
- A standardised, unified and interoperable digital identity framework (All)

Additional perceived costs/risks may include:

- Not utilising internationally recognised data standards, prohibiting portability and interoperability
- Not utilising internationally recognised technical standards, prohibiting portability and interoperability
- Failing to balance the framework with disproportionate powers remaining with Industry
- Not allowing technology to solve for a number of issues traditional approaches have presented
- A lack of public awareness and education reducing participation in the CDR (Rated amongst the greatest regrets of the UK and Australian experiences)
- The advent of sectoral differentiation leading to an overtly complex and non-interoperable solution

4. What would the costs and benefits be of applying the consumer data right to businesses and other entities, in addition to individuals?

FDATA believes that all data should be portable, therefore all organisations and individuals should have the right to access, control and retain their data.

In the case of Open Banking, Cloud Accounting Platforms provide services to both individuals and businesses and the ability for a comparative level of service will not only increase useability, but enhance the customer experience further.

In the United Kingdom, artificial intelligence built into applications and platforms are providing personalisation of services for Small to Medium businesses requiring access to loan facilities and enabling the comparing and switching of business obligations, such as power, telecommunications and utilities provisions via a platform approach.

With the omission to a reference for businesses having control and a right to access over their data, the Privacy Act 1993 (2020) can be amended to include entities and individuals accessing associated data.

5. Do you have any comments on the types of data that we propose be included or excluded from a consumer data right (i.e. 'consumer data' and 'product data')?

For clarity, it's simple to consider data in four categories:

1. **Customer-provided data** – provided directly by customers to their bank

Examples: contact information, financial history, payee lists for bill payments, demographic details, etc.

Customers clearly 'own' this data and should be able to dictate it be shared without restriction. The repetitive process of continually providing this information can be a barrier to switching providers; if a customer opening a new account could simply direct their current provider to share their personal details with a new provider, it may significantly reduce the friction of switching. The sharing of Customer-provided data, or Personal Information will lead to new innovative products designed to enhance the customer experience and add to the competitive environment of financial services and digital identity frameworks.

2. **Transaction data** – generated through transactions made by a customer's account

Examples: withdrawals, transfers and other transactions; account balances, interest earned and/or charged, etc.

Transaction data should be shared, at the direction of a current or former customer. Regulators need to consider the amount of historical data that may be required; an open-

ended period would put an excessive burden on data holders and we can expect advancements in digital archives and records as time progresses. In many jurisdictions, regulators have determined that a pragmatic approach is that data holders may only be obliged to transfer data for the same period they are required to hold it for existing regulatory obligations.

3. **Value-added customer data** – data that results from an effort by a data holder to gain insights about a customer

Examples: credit scores; income/assets verification; customer identity verification; data on an individual customer that has been aggregated across the customer's accounts and standardised, cleansed or reformatted.

While the primary data was likely provided by the customer or generated by the customer through transactions, the true value is being derived through actions taken by the data-holder. Sharing this data would represent a transfer of value from the data-holder to the customer (or a TPP) and may breach intellectual property or commercial agreements. **Generally, this is outside the scope of open banking. For similar reasons, pre-aggregated data sets should also be considered outside the scope of Open Finance.**

4. **Product data** – Financial data for which there are no CDR consumers

Examples: eligibility criteria, terms and conditions, pricing, performance of a product or instrument, accessibility, process or procedure, etc.

Determining the products scope is also critical. The Australian government, in its open banking review, concluded that transaction data should include products relating to the conduct of banking business as defined in its banking act, but only for those products that are widely available to the public. Other jurisdictions are likely to follow a similar approach.

Examples of products generating transaction data (from the Australian Open Banking Review

Deposit Products	**Lending Products**
Savings accounts Cheque accounts Debit card accounts	Mortgages Business finance Personal loans

Transactions accounts Personal basic account GST and tax accounts Cash management accounts Pensioner deeming accounts Mortgage offset accounts Trust accounts Retirement savings accounts Foreign currency accounts	Lines of credit (personal & business) Overdrafts (personal & business) Consumer leases Credit & charge cards (personal & business) Asset finance (and leases)

6. What would the costs and benefits be of including both read access and write access in a consumer data right?

As depicted under segment A Phased Approach, granting write access would align a New Zealand Open banking regime with Europe's payment services directive PSD2 and potentially the Australian equivalent if adopted in December 2020, and would allow better comparison services and life administration offerings to be created using banks' data.

In its current format, Australia's Open banking regime is limited to "read" access only, meaning that data recipients and customers cannot modify existing data, nor alter existing products directly. By introducing write access, there will be ramifications beyond the banking application. In an energy scenario, enabling write access may allow a customer to open a new account, make changes to their account, or close an account, seamlessly through a third-party. That may be a business, a service or an application. This will enable a greater level of convenience and efficiency in comparing and switching service. Customers will be able to access, in real-time, a personalised offering, or avoid often dreaded cancellations interactions with service providers.

A Scott Farrell issues paper writes, "consumers would be able to see a single dashboard of products and plans they have across banking, energy and telecommunications, such as the cost and time remaining on each account, balances and due dates for bills. Customers could get alerts in real time when better deals become available. The write access would then let them act on such alerts, such as by closing one account and opening a new one with a few button pushes."

The United Kingdom's CMA Retail Banking Market Investigation Order links the delivery requirements for UK Open Banking explicitly with PSD2:

10.1.2 both read and write access, which allows a third party to access account information or initiate a payment on behalf of the customer (subject to the customer's explicit consent), for data set out in Article 14 (the 'Read/Write Data Standard') and which has the features and elements necessary to enable Providers to comply with the requirements to provide access to accounts subject to this Part 2 of the Order under PSD2.

For all the anticipated benefits, including write access does heighten the risks associated with the regime and the players involved. New Zealand must give considerations to time constraints of technical readiness, user demand offsetting technical investment and the potential limitations that will be uncovered within business architecture. Perhaps the most concerning issue of including write access in a Consumer Data Right is the potential for a cyber attacker to exploit the functionality of the system to defraud customers while breaking data holder IT systems.

The United Kingdom's CMA Retail Banking Market Investigation Order links the delivery requirements for UK Open Banking explicitly with PSD2:

10.1.2 both read and write access, which allows a third party to access account information or initiate a payment on behalf of the customer (subject to the customer's explicit consent), for data set out in Article 14 (the 'Read/Write Data Standard') and which has the features and elements necessary to enable Providers to comply with the requirements to provide access to accounts subject to this Part 2 of the Order under PSD2.

For all the anticipated benefits, including write access does heighten the risks associated with the regime and the players involved. New Zealand must give considerations to time constraints of technical readiness, user demand offsetting technical investment and the potential limitations that will be uncovered within business architecture. Perhaps the most concerning issue of including write access in a Consumer Data Right is the potential for a cyber attacker to exploit the functionality of the system to defraud customers while breaking data holder IT systems.

A phased approach may mean differing 'live' dates for the read and write access parameters, but verifying their inclusion from the start can alleviate cost associated with retrofitting technology stacks and the need for large-scale alterations to technology platforms as a number of participants and banks are experiencing in Australia.

DOES NEW ZEALAND NEED A CONSUMER DATA RIGHT?

7. Do you have any comments on the outcomes that we are seeking to achieve? Are there any additional outcomes that we should seek to achieve?

We support the intended outcomes for a New Zealand Consumer Data Right. All actions contributing to the design, development, delivery and administering of this regime must keep these objectives centre of mind.

The global digital transformation, the creation and deploying of data-related technologies, can drive and support the desired impacts for delivering a CDR. By considering the best possible framework, the CDR process may increase the necessary access to funds, talent and ideas to enhance innovation and competition on an economy-wide basis.

All stages of the CDR development and implementation must be agile and nimble and technology agnostic. A balance between technology enablement, digital identity inclusion and legislative reform will affect both the consumer and the government, and may lead to an improved service provision and enhanced customer experience.

Industry and government must work together to reduce barriers to entry and to promote regional and international flows. The New Zealand Productivity works have specifically called out the Financial Services sector as a pivotal industry, the potential for enhanced economic outcomes and consumer welfare far exceed a singular sector with additional sectors and industries being considered.

FDATA supports the initial outcomes of:

Consumer Welfare:

- Strengthening existing privacy rights and giving consumers greater choice and control of their data.
- Enabling innovation that provides consumers with a wider range of products and services that better meet their needs.

- Increasing access to more affordable products and services by facilitating competition, and reduced search and switching costs.

Economic Development

- Increasing business productivity by accelerating the velocity with which data moves through the economy.
- Contributing to the growth of the digital economy by enabling the development of new and innovative sectors of the economy (e.g. fintech) that use consumer and product data.

We concur that the following criteria for establishing the framework of a CDR be observed as an initial guidance in addition to initial principles:

a. **Trust.** How well will the option strengthen privacy rights and maintain the security of consumer data while it is being used and shared?

b. **Reach.** How well will the option enable multiple sectors to become 'open'6 thriving data sharing economies? An option which enables multiple 'open' sectors presents significant economic development opportunities, greater competition and productivity for the long-term benefit of consumers.

c. **Speed.** How quickly will data portability become widespread throughout the economy, allowing the benefits to be realised?

d. **Cost.** How well will the costs of implementing a CDR be minimised so that the costs do not outweigh the benefits?

e. **Flexibility.** How well will an option allow for solutions to be tailored to the needs of a sector, and allow sector-led solutions to be developed before regulatory intervention?

8. Do you have any comments on our proposed criteria for assessing options? Are there any additional factors that should be considered?

There are a number of essential facets to a Consumer Data Right that have been omitted in the assessment of options. These include, but are not exhaustive:

- CDR Participants
- Liability Modelling
- Customer Experience
- Existing Privacy Parameters
- Technology Enablement – Technical Standards, Participants, Timeframes for development and implementation
- Accessibility
- Sector Specific Requirements – Historical data vs Real time reporting
- Room for Innovation
- Global Learnings

9. Do you have any comments on the discussion of Option one: Status quo?

In addition to a number of incorrect assumptions and statements around regulatory intervention or investments, option one / the Status Quo has failed to produce progress despite concerted efforts by numerous entities and groups.

For all of the work that has occurred and is currently occurring across several sectors, such as the Financial Services sector, a suitable outcome has not been reached. Irrespective of the work that has been done by the API Centre, and the encouragement of Open Data production, a Consumer Data Right equivalent is yet to be designed or realised.

Caution needs to be granted to individual approaches, the duplication of a solution, or the ability for early adopters to host disproportionate power over other participants and the customer.

10. Do you have any comments on the discussion of Option two: A sectoral-designation process?

Whilst this option has demonstrated considerable pros and cons, FDATA does not concur that it alone will see the creation and implementation of the best-practice solution that will fit New Zealand's requirements.

The overall concept of option two is to be commended, but the statement of "CDR would only apply to sectors or markets that had been designated through secondary or tertiary legislation. This option is a sectoral designation approach similar to the ACDR", is concerning. Currently, the sectoral designation approach in Australia is largely still under planning with roadblocks between the first and second sectors already creating hurdles from a legislative and regulative perspective.

In addition, a sectoral-designation process will slow down the economic benefit of establishing an economy-wide solution by potentially omitting economically linked sectors, emerging sectors, or those sectors that are yet to embrace the full digital transformation, i.e. health, education and agriculture.

FDATA does concur that option two shows potential to removing barriers over bi-lateral arrangements with data holders, but option three also solves for this issue through a centrally regulated and administered framework.

Option two is also not the only solution that would promote alignment with the Digital Identity Trust Framework, nor admit data-sharing for both individuals and business entities. Option three allows for both of these issues also.

11. Do you have any comments on the discussion of Option three: An economy-wide consumer data right?

As explored in the A Global Approach and Digital Identity Framework segment of this submission, digital transformation is occurring at a startling rate on a Global Scale. Examples out of the United Kingdom, Europe and North America are in complete contradiction to the cost/risk statements of the discussion document. New additions to the technology landscape take the highest level of commercial and legal responsibility for privacy, security, digital

identity, data sharing and access rights into consideration. The issue of data collection and sharing has come under extreme scrutiny in several National Enquiries and Legal Processes. In a number of cases, the claims of identity breaches and mis-appropriation of data is supported by existing legislation or interpretation of historical legislation that has failed to keep up with digital transformation and reform. In many cases though, access to data and the consumer's right to control their data is covered within existing privacy Acts and regulations.

New digital technologies are being built with the required governance, security and legal standing required to supply consumer-centric services in an accountable and compliant manner. No longer serving individuals only, the design of unique identifiers is transforming the digital identity framework to include provisions for both incorporated and unincorporated entities. Commonly utilised traditional identifiers include: business numbers, tax file numbers, trading names and place of business. Due to the evolution of technology platforms, there is no significant legislative change required, the only change would be to add the ability for data to be shared via well-formed APIs.

These systems exist in multiple markets today, via access to API's and Machine-Readable formats. All of these options require the same approach and Option three would potentially solve for these inclusions.

12. Do you have any comments on the discussion of Option four: Sector-specific approach?

Any attempt to customise differing regimes or frameworks on a sector-by-sector basis should be discouraged. That being said, there will be specific nuances around the processes, systems, and types of data held that may be different per sector. Careful research and design thinking should be employed in order to create a single, centrally administered Consumer Data Right for the nation.

The lack of continuity is in direct opposition to the intended outcomes of data portability and consumer rights. In addition, by extending the current sector-led initiatives, that are yet to achieve any desired CDR outcomes, the cost, time and input will still not result in a fit-for-purpose outcome for New Zealand.

13. This discussion document outlines four possible options to establish a consumer data right in New Zealand. Are there any other viable options?

FDATA believes that there are elements from the first three that can be combined to deliver a best-practice outcome. By employing international standards and solutions, increased interoperability and reduced timelines may be achieved.

An extensive research, collaboration and exploration phase must be engaged prior to any decisions around technology or legislation can be made.

14. Do you have any comments on our initial analysis of the four options against our assessment criteria?

There are elements of all four scenarios that we agree with, and elements that are incorrect or unrealistic in their depiction. FDATA supports a mixed-solution as explained in our response to Question 15.

15. Do you agree or disagree with our assessment that Option two is most likely to achieve the best outcome using the assessment criteria?

We do not agree that any one option will achieve the world-leading CDR solution that best suits New Zealand. There are elements of three of the options that have the makings of a best-practice framework.

Trust – A combination of options two and three deliver the necessary Trust elements to succeed. By creating a regulated, unified and accredited solution, trust and transparency will be paramount.

Reach – New Zealand has the ability to create an open sectors solution that includes both data pertaining to individuals, but also to businesses. This is a departure from the Australian and initial UK regimes. This can include our recommended data types for inclusion: Personal, Transaction and Product, but should exclude additional data such as derived, associated and assumed. Options two and three when combined can achieve the desired outcome.

Speed – While option two will deliver a speedier outcome than the Status Quo, option three when utilising existing technologies and improving on in-market solutions will present the greatest speed-to-market solution. Another option is for the participants of Option one to be included in the sectoral steering committees to ensure that continuity of the Industries is maintained.

Cost – Every solution considered will result in a cost for development, implementation and regulation. We believe that option three, in the long run will not only be lower, but by adopting and adapting existing technologies, will result in a more appropriate economic outcome for New Zealand.

Flexibility – We do not see why option three will result in economy-wide inconsistencies with consumer data portability. The implementation of such technologies across the United Kingdom and Europe has seen secure and high-quality outcomes for data sharing and the control of consumer data. Option three will realise an economy-wide solution in the quickest and most effective manner.

Overall Assessment – We acknowledge that both options two and three will achieve the desired consumer welfare and economic benefits are stated in the discussion document. The inclusion of Industry groups in steering committees will see the Intellectual Property and Industry Knowledge currently experienced is transferred across to the future Consumer Data Right.

How could a Consumer Data Right be designed?

16. Do you agree with the key elements of a data portability regime as outlined in this section? Are there any elements that should be changed, added or removed?

Consideration must be given to, but not exclusively to:

- A global approach
- A customer-centric design
- The potential value of a CDR
- Digital Identity Frameworks

- Governance
- Liability
- Accreditation
- Types of Participants
- Types of Included / Excluded Data
- Principles
- Consent
- Privacy and Security by Design
- Technical Standards
- Data Standards
- Sectoral Inclusions and Timeline
- Read/Write Access and other Phased Approaches

When designing a suitable solution, a starting point must be the needs and benefits to the consumer. Consideration must be given to real-world examples of consumer experience and thought given to enhancing that experience, through improved process and technology implementation. Consideration must also be given to the existing participants in Industry, and with the focus on enhancing the outcome, avoiding as much disruption to commercial enterprises whilst balance the intended aim.

It is critical that solutions are not explored without industry participation, nor solely by industry. Consumer Advocates, Regulators, Industry (Including various elements of Industry from large, medium and small participants), to Privacy experts should all be involved.

The best solution will come from an Industry-led, Government Regulated, Consumer-Centric framework, facilitated by an independent facilitator with explicit knowledge of Data Portability.

17. Do you have any feedback on our discussion of any of these key elements?

In addition to the information supplied within this submission, FDATA concurs with the overall design framework for the CDR:

a. establishing a CDR that can be designated to specific sectors – design first, legislation second

b. providing for the type of data and the types of data holders within a sector, included in the CDR to be set during the designation process

c. providing for detailed rules for accessing and transferring data to be set during the designation process

d. establishing an accreditation regime for third parties

e. strengthening privacy safeguards

f. establishing an enforcement regime and methods for consumer redress.

Great learnings of what has worked and hasn't worked in other jurisdiction should be an initial consideration in the design process. Ensuring that the consumer, their rights, and the benefits of them utilising the Right should be central to all design and development process. That being said, it is important to recognise the commercial disruption to Industry and the potential for new business models to enter the marketplace.

18. Are there any areas where you think that more detail should be included in primary legislation?

The formation of CDR legislation, where it sits, with whom oversees the Act, and the specificity of the legislation will determine whether more detail will need to be included in the primary legislation. FDATA advises the New Zealand government to focus on the design, componentry, principles and standards before apportioning the legislative requirements of enforcement, ownership and formation.

19. How could a consumer data right be designed to protect the interests of vulnerable consumers?

It is important to acknowledge that vulnerability can arise from personal circumstances or from features of a technology or system.

Vulnerabilities from personal circumstances may include:

- Age – Minors / Seniors, etc

- Social Economic
- Education
- Disability
- Language
-

Vulnerabilities from features of technology or systems may include:

- Complexity
- Poor Product Design
- Poor Service provision
- Deliberate exploitation of consumer behaviours or biases
- Deliberate exploitation of consumer groups, particular communities, age or language skills
- Information Visibility or Asymmetry

Steps that can be taken to identify potential vulnerability and to combat potential issues may include:

- Tackling vulnerability at multiple stages through the design, development, delivery and ongoing phases
- Utilise data to identify areas of most pressing need, prioritise regulators' vulnerability and accessibility works
- Identify consumers that are at risk of exploitation
- Develop a comprehensive vulnerability strategy
- Include protections within the regulation through safeguards and penalties

Continue to identify risks and impacts of a changing demographic and technology market

20. Do you have any suggestions for considering how Te Tiriti o Waitangi should shape the introduction of a consumer data right in New Zealand?

FDATA agrees that no new regime or legislation should contradict existing requirements. We applaud the discussion documents commitment to work with the Māori people to establish trust, understanding and the sympathetic design of a system that supports not only the rights and beliefs of the Māori people, but all citizens in regards to the ownership, control and access to personal data. The MBIE should give consideration to the existing works on Digital

Trust Frameworks and Digital Identity that is well underway with the assistance of a number of groups and co-operatives.

21. How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?

With approximately one in four New Zealand residents identifying as having a disability (Disability Survey 2013), it is crucial that any technology environment and associated policies are designed, reviewed and regulated accordingly.

On a Global scale, technology is being built using thoughtful design and assisted componentry. Inclusions such as Artificial Intelligence, Machine Learning, Virtual Reality and Augmented Reality are opening up access to users that would normally be excluded. Such inclusions are being mandated sporadically across Nations and use-cases.

FDATA acknowledges that accessibility issues will not only exist in the technology design, but within the overall regime. Organisation, such as the W3C Web Accessibility Initiative publish a guide for common accessibility standards recognised by governments around the globe. These include:

- Web Content Accessibility Guidelines
- Authoring Tool Accessibility Guidelines
- User Agent Accessibility Guidelines
- Referencing Guidelines for the creation of standards
- Defining Conformance Levels
- Defining the scope of policy in regards to accessibility
- Consideration of third-party content in accreditation.

22. To what extent should we be considering compatibility with overseas jurisdictions at this stage in the development of a consumer data right in New Zealand?

New Zealand must equally focus on creating the best solution for its economy, and being mindful of New Zealand's place on a global stage. The opportunity for data sharing and increased productivity leading to both consumer welfare and economic benefit is substantial.

While no one jurisdiction have created a similar regime, the ability for New Zealand to not only create a world-leading solution, but also tailor it to be able to connect to international offerings via technology options such as APIs is substantial and should be a main prior for the design and development of the CDR.

Numerous private and public offerings exist that transcend borders and continents. Examples such as payment provision, Covid applications surrounding contact-tracing and traveller's status, and anti-money laundering/counter terrorism funding mechanisms all showcase the potential for technology design on a global scale.

New Zealand's legislation, regulations or policies do not need to mirror the rest of the world, but the standards, principles and technology can be sympathetic.

23. Do you have any comments on where a consumer data right would best sit in legislation?

FDATA does not have an immediate suggestion for where the Consumer Data Right would best sit. The focus on legislative enablement and oversight must come after any design and development of the CDR, not proceed the works. The ability to cohesively work with technology and learn from other jurisdictions will flavour the legislative requirements going forward.

The Consumer Data Right will spread across existing legislation. FDATA does not support the amending and altering of the existing Competition, Consumer and Privacy laws. We believe that the current objectives of the regime denote the creation of a standalone legislation, and retrospective reformation of contradictory terms throughout the existing Acts. Other jurisdictions have chosen to alter/amend various existing pieces of legislation to the detriment of the design, development and delivery of their Consumer Data Right equivalents. Contradictions, duplications and redundancies are being currently worked on by both the Australian and the United Kingdom governments.

24. Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?

The introduction of any large project or policy requires several parts to ensure effective launch and continued success:

- Project Owner: NZ CDR should be owned by a single government department to ensure desired resources, timeframes, milestones and goals are achieved.
- Project Sponsor: The Minister responsible for that portfolio.
- Project Advisers: The Industry / Sector steering committees that are formed to ensure the best solution is designed, developed and delivered.
- Project Steward: The single regulator that is appointed to run the CDR.
- Project Champions: Industry Groups and Associations, and Consumer Advocates.

The multi-sectoral nature of the regime may make it difficult to decide on the final allocation of regulator. Regardless of the approach taken by the government, the following requirements must be considered:

- To provide a simple regulatory oversight
- To provide a central point of reference for all participants
- To provide clear and concise requirements to adherence and penalty for none conformity
- To provide sectoral leadership and insight
- To lead public awareness and education
- To manage all accreditation and administrative requirements

25. What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?

The international experience, both from a data portability perspective, and from an industry continuity standpoint supports the creation of a single, independent regulator that has overarching authority for the Consumer Data Right within New Zealand. This would transcend industry specifications and participants. By appointing a single central point of regulation, continuity of technical and data standards, the rights and responsibilities of participants, the protection of consumer privacy and principles for the right can all be coordinated effectively.

In regards to separate regulators providing knowledge and expertise, the creation of steering committees or working groups could bring the aspect to the central regulator, without the need for duplication or competing adjudications.

A recent senate enquiry into the Consumer Data Right in Australia has made recommendations to establish a single, independent regulator to find continuity and ensure service delivery going forward.

26. If government decides to establish a consumer data right, do you have any suggestions of how its effectiveness could be measured?

Aside from measuring general customer sentiment and feedback, the evaluation of new services offering innovative products and expanding business numbers signalling competition across the region, the most basic level of evaluating economic benefit from a Consumer Data Right would be the Gross Domestic Product (GDP).

All instances of the afore mentioned measurements will find their way into the GDP. International Trade both Exports and Imports, Consumption both Private and Government, Investment both Private and Government, and changes to Broad Money across the economy.

The team at FDATA support New Zealand's endeavour to design, develop and deliver a fit-for-purpose Consumer Data Right. The CDR is a key opportunity to promote digital transformation enhancing New Zealand's economy and highly encourage the CDR exploration to be swiftly commenced to achieve these objectives.

Please do not hesitate to contact me should you have any questions or request for further input.

Kind regards,

Jamie Leach
Regional Director
Financial Data and Technology Association | Australia/New Zealand

Mobile: +61 413 075 671
Email: Jamie.leach@fdata.global | Web: fdata.global | Twitter: @FDATAglobal

Acknowledgements:

Authors: Jamie Leach, Gavin Littlejohn

Editor: Jamie Leach, Richard Prior

Design: FDATA ANZ

Published October 2020.

Cover quote credited to: https://blog.hubspot.com/service/customer-centric-design