paymentsnz

apicentre
paymentsnz

Discussion document: Options for establishing a consumer data right in New Zealand

Payments NZ and API Centre submission to MBIE

October 2020

Contents

Introduction

Payments NZ Limited (Payments NZ) welcomes the opportunity to make a submission to MBIE on the discussion document on options for establishing a consumer data right (CDR) in New Zealand.

Payments NZ is a key stakeholder in the governance of the New Zealand payments system. It has, with the input and support of the payments industry, been responsible for the establishment and operation of the API Centre. The nature and scope of the work of Payments NZ and the API Centre has direct relevance to the current consultation.

In developing this submission, we have extensively consulted our API Centre API Standards Users, our community contributor members, the API Business Working Group, the API Council, the BECS Management Committee and other international open banking experts.

The Payments NZ submission is made in its own right as an industry leader. This submission is not a representative submission and it does not necessarily reflect the individual views of our Participants, API Standards Users, or Community Contributors, rather it is an industry view grounded in the experience and learnings from the API Centre journey to date.

This submission will cover:

- Payments NZ (as background information);
- the API Centre (to illustrate its role and purpose within the ecosystem and its relevance to any potential New Zealand CDR);
- positions and relevant information with respect to key issues;
- responses to the discussion document questions (at Appendix A).

Payments NZ

Payments NZ was established in 2010 with the support of the Reserve Bank and it represented a new model for the governance of payment systems in New Zealand (previously done under the auspices of the New Zealand Bankers' Association). Payments NZ is responsible for setting and overseeing the rules and standards governing the way payment instructions are exchanged and settled and, more generally, for reviewing payment system policies and procedures.

Participants are financial institutions that have joined one or more of the four payment systems in order to take advantage of (and be bound by) the multi-lateral framework of rules provided by Payments NZ. The financial institutions currently are all regulated entities, mostly as registered banks prudentially regulated by the Reserve Bank.

Payments NZ is very much at the heart of the payments ecosystem. It is committed to bringing the industry together to enable inclusion in the ecosystem and to promote interoperable, innovative, safe, open and efficient payment systems for Kiwis. It does this by leading strategic industry initiatives which includes the Payments Direction Programme[1], facilitating industry discussion and providing thought leadership on topical matters. Strategic forums and industry events are regular features of its work programme.

Payments NZ is committed to fostering market-led solutions and innovation. The API Centre is a tangible demonstration of this.

[1] https://www.paymentsnz.co.nz/our-work/payments-direction/

The API Centre

The API Centre is primarily responsible for:

- developing, maintaining and publishing API Standards;
- promoting system efficiency, safety and innovation through the use of the API Standards by registered API Standards Users on agreed terms and conditions; and,
- facilitating API Standards Users entering into partnerships to bring new innovations to market more simply and quickly.

'Open banking' has been at the forefront of discussion in recent years (in New Zealand and internationally). In general terms, it can be described as initiatives that give consumers greater access to and control over their banking data, in particular, through third party products and services. Common or standardised APIs (application programming interfaces) are the key enabling technology to deliver open banking outcomes. They allow disparate systems to connect, interface and action requests with each other.

Greater openness in banking is driven by a range of factors internationally, depending on the outcomes sought in that jurisdiction. Importantly, however, all 'Open Banking' programmes aim to strengthen the control a consumer has over their banking information in order to realise additional potential benefits.

Key Issues

The work associated with the establishment and operation of the API Centre is directly relevant to this consultation. In particular, Payments NZ and the API Centre have hands-on experience with important facets of what can be expected to feature in the context of any potential New Zealand CDR framework. This submission now deals with these key issues.

CDR design fundamentals

The design of a potential New Zealand CDR needs to focus on three fundamentals:

- putting Kiwis at the heart of a New Zealand CDR;
- consumer trust;
- consumer consent.

The following sections explore these CDR fundamental design issues.

a. Putting Kiwis at the heart of a New Zealand CDR

Position statement

Consumer outcomes and benefits need to be the primary focus of what any potential New Zealand CDR regime aims to achieve.

Relevant matters

A potential New Zealand CDR regime would look to solve problems that the vast majority of New Zealanders do not know that they have. International experience points to 'open banking' being the initial cornerstone of a national CDR. At this point in time, New Zealand consumers are not especially

aware of the potential of what a CDR might involve or enable. Our research[2] shows that only 19% of surveyed New Zealanders are aware of the term open banking, with only 6% being confident that they know what it is. This reflects that New Zealand's open banking ecosystem is in its formative phase. Products and services that leverage, for instance the API Centre's standards or other open banking APIs, have not yet taken hold in the market. Experiences in the UK tell us that until consumers can use, trust and experience a product or service enabled through open banking, their awareness will remain low.

Accordingly, there is a risk that technology and commercial interests lead the discussions to formulate and drive any potential New Zealand CDR, instead of focusing first and foremost on the consumers that a CDR should aim to benefit. It is very important that the consumer's genuine needs and interests be placed at the centre of any potential New Zealand CDR. If the priority focus is on putting the consumer at the centre of any potential New Zealand CDR, then opportunities for innovation and commercial enterprise will efficiently follow. Any potential New Zealand CDR must also consider Te Tiriti of Waitangi and ensure Maori consumer interests and outcomes are taken into account, and tangata whenua representatives are active in its design.

We believe that there should be a clear vision and purpose of a CDR. MBIE's discussion document does not appear to feature a clear articulation of a rallying vision, a purpose or the targeted outcomes for the CDR. Initial factors that should be considered when developing the CDR's vision and purpose include:

- empowering consumers to have control of their data;
- only introducing a CDR if it delivers materially better outcomes for consumers;
- placing the consumer's genuine needs and interests at the centre of the CDR;
- providing clarity on what the consumers actual "data rights" are;
- initially, putting greater emphasis on the consumer and the protections over their personal data. Once this is in place, only then focus on competition and facilitating data flows across markets and organisations;
- the objectives and outcomes that a CDR aims to achieve should be well defined and specific. Where applicable, they should be clearly prioritised. In particular, it should feature the following:
    - the defined problems that a CDR aims to solve;
    - the future-state consumer outcomes that a CDR aims to achieve;
    - use cases to illustrate exactly what a CDR regime aims to achieve[3];
- a CDR's objectives and consumer outcomes should be measurable.

We note that the discussion document does not give particular consideration to what the actual "data rights" are to be for consumers (beyond the idea of data portability), and how these data rights might sit in relation to legislation/regulation more generally. This is a fundamental gap. This will need to be considered in any next steps in order to fully understand the scope and framework of what a potential New Zealand CDR might encompass.

Experience/learnings of the API Centre

The API Centre's vision is to enable the industry to deliver innovative API based services to support Kiwis financial wellbeing. Accordingly, we put more emphasis on articulating the consumer benefits

2 Base: Total N=1,012. *Q: Before today, had you heard of the term **open banking**?* Research commissioned by Payments NZ and conducted between 2-16 September 2020.

3 When initially designing the UK's open banking framework, they identified six key customer propositions that they aimed to support and deliver through open banking. See section 6.1, of The Open Banking Standard

and consumer outcomes that our API Standards will need to support. We have learned from our own development processes, and from the UK's open banking lessons, that it is vital to focus on consumers and their journey.

An illustration of this is our Customer Experience Guidelines [4]. These directly address the real-world customer journey between API Provider and Third Party interactions, from establishing the customer's consent and authenticating their identity, through to sharing the customer's data with a Third Party. This provides a starting point for our API Standards Users to create their own customer experience across their products and services that have been built on top of our API Standards.

b. Consumer trust is essential

Position statement

Consumer trust is an essential ingredient of a successful CDR. The more trust there is, the more willing consumers are to share their data and to participate in products and services that leverage CDR arrangements. A strategic and holistic approach to how the values of trust can be purposefully built into any potential New Zealand CDR should be taken.

Relevant matters

A person's willingness to share sensitive information is highly influenced by their level of trust. A consumer's starting position is often one of reticence, skepticism and caution. Without consumer trust in the products and services a CDR regime might enable, uptake may be low and the CDR will struggle to deliver its intended benefits.

Security, fraud and privacy will always be uppermost in a consumer's mind and will be key considerations for not providing consent to share data. Our research[5] shows that 84% of surveyed New Zealanders are unsure or uncomfortable about sharing banking data. Their key trust related concerns[6] included:

- Fear of risk/cybercrime/hacking/security breaches:
    - "There is so much fraud and hacking these days that anything that is new and unusual is threatening."
    - "It sounds dodgy, would prefer if my own bank handled everything. Having another company have access to my personal banking details makes twice as many organizations with my bank info! Twice the risk."
- Prefer to stay in control/private:
    - "Your finances are private and not something you want to share. I like being in charge of when things get paid and what amounts etc., so wouldn't want to pass that over to anyone else and trust them."
    - "I like to maintain control myself. No need to involve another party."
    - "Not a fan. Sounds too big brother and easy for someone else to take control of your finances."
- Third party trust issues:
    - "You can never be sure how trustworthy they are."

4 https://www.apicentre.paymentsnz.co.nz/about/news/customer-experience-guidelines-released/
5 Research commissioned by Payments NZ and conducted between 2-16 September 2020. Base: Total N=1,012; Unsure/ Uncomfortable N=845. Q: How comfortable would you be sharing your banking data with an organisation other than your bank for your own benefit? All data would be shared securely and only with your express consent.
6 Q: Thinking about everything you have heard about open banking today, do you have any other thoughts or comments on open banking?

    - "I would be dubious of how the third party is using the data."
- Unwanted data sharing:
    - "Who are they, how secure is the data and what else is done with it? What guarantees do I have that data about my spending habits isn't sold?"
- Accountability for errors / correction of errors:
    - "Sounds complicated. I would need to see hard proof of who is accountable for mistakes."
    - The need to be well informed first:
    - "I would be interested in this way of conducting business but am wary of accepting without fully looking into it. Am sort of person who takes time to read, understand and adjust."

If the main principle behind a CDR is to put consumers in control of their data, then the CDR regime will need to foster trust. In order to grow this trust, consumers will need to *know* that they are in control of their data and that they can have faith in the safeguards.

A holistic view should be taken when developing a framework that can foster, grow and protect consumer trust. A CDR trust framework is likely to be made up of a number of important elements, including:

- the use of clear and consistent language that is easily understood, to help support consumer education and trust. An agreed consumer-centric language taxonomy that is accessible to consumers should be developed in collaboration with industry. Industry should then consistently apply and use this language taxonomy;
- the use of a clear consent framework that follows a consistent consumer interaction flow/process;
- the availability of consumer safeguards such as dispute resolution provisions;
- the promulgation of best practice guidelines;
- the protection of vulnerable consumers;
- strong and meaningful consumer and tangata whenua representation, and;
- communications and education materials for consumers about why they can trust CDR enabled products and services. Government could take a lead role in this regard, with coordinated support from industry.

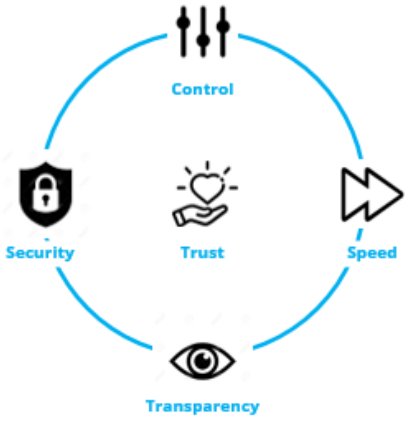
Experience/learnings of API Centre

The API Centre's terms and conditions and API standards hardwire API Standards Users to ensure that their consumers are clearly informed about what they are consenting to, how they can track their consents, and how they can revoke their consent at any time.

The API Centre has developed customer experience guidelines[7] in recognition of the importance of supporting and nurturing the industry with best practice guidelines, and through the consistent use of language and approach when engaging with customers. The guidelines include the importance of trust and how there are four important components to develop trust, being: speed; control; transparency; and security as follows:

[7] https://www.apicentre.paymentsnz.co.nz/standards/using-standards/customer-experience-guidelines/

- *Speed* should be appropriate to the customer and the journey they are undertaking. This is not always the fastest possible time.
- *Control* enables customers to understand and take ownership of the decisions being made through the process.
- *Transparency* of choice, action, and, importantly, the consequences of actions or sharing of data.
- *Security* concerns for customers are fraud and data privacy. It is important to provide clarity and reassurance in relation to data definition, use, security and, above all - protection.



c. Consumer consent is fundamental

Position statement

Having a consistent and strong consumer consent framework is fundamental. The API Centre's consent framework and standardised customer interaction flow, which is based on international standards, should be used as the starting point for ensuring consistency in any potential New Zealand CDR.

Relevant matters

New Zealand's CDR needs to empower consumers to maintain appropriate control over their data, and how they grant and manage their consents. Ticking a 'click to consent' box is not good enough and is unlikely to comply[8] with the Privacy Act's Principle 3 "collection of information from subject" (i.e. individual is aware).

Consent frameworks need to explicitly state what data consumers are being asked to share, how the data is to be used, and who will have access to it. Consumers should be able to easily track their consents and to manage them. Their consent must be explicit and freely given (i.e. not coerced). Revocation of consent must be a simple and fast process, and the consequences of revocation must be explained.

Care should be taken with how the CDR regime aligns with the Privacy Act 2020 so that there is no overlap or conflicts between the two regimes. The Privacy Act[9] already sets out the key foundations required to establish a CDR consumer consent framework. However, once there is clarity on the objectives and outcomes sought by any potential New Zealand CDR, a gap analysis approach should first be undertaken to ensure that any new CDR legislation relevant to consents and privacy do not overlap, conflict, or create gaps (with what is already in place).

Experience/learnings of API Centre

The API Centre has invested in and developed a strong, standardised consent framework, which draws on international principles and best practice. It should be noted that API Standards Users have or are building systems in line with this framework.

The standard for accessing account data[10] puts the consumer in control of data sharing and

[8] "Click to consent? Not good enough anymore", blog by John Edwards - New Zealand's Privacy Commissioner, 2 September 2019.
[9] The new Privacy Act will be in place from 1 December 2020. The Privacy Act already contains most of the elements required to support a CDR consent framework, including for example: 'Principle 1: "purpose of collection of personal information" (only collect necessary information). Principle 3: "collection of information from subject" (individual is aware). Principle 4: "Manner of collection of personal information" (lawfully and fairly collected). Principle 5: "storage and security of personal information" (protected by security safeguards). Principle 11: "limits on disclosure of personal information" (disclosure is authorised).
[10] https://www.apicentre.paymentsnz.co.nz/standards/available-standards/account-information-api-standard/

permissions. It sets out the steps for how data access consent can be granted, how to view consents and how to revoke them at any time (whether with the bank or the third party). The API Centre's terms and conditions set out the obligations[11] that arise in relation to the giving of consent (consistent with privacy and other law).

The API Centre and its API Standards Users have made considerable investment into the design of our consent framework and we believe it would be a useful and time saving starting point for considering the design of any potential New Zealand CDR consent framework.

CDR framework design

The design of a potential New Zealand CDR's framework should;

- follow a principles based approach; and
- have an inclusive approach to governance.

The following sections explore these framework issues.

d. Principles-based approach

Position statement

A principles-based approach should be taken with the design of any potential New Zealand CDR regulation.

Relevant matters

The regulatory approach to designing and implementing any potential CDR for New Zealand is important. In particular, it will have a direct bearing on the efficiency, costs and the compliance burden of the regime, and ultimately on whether it delivers the beneficial outcomes to New Zealanders.

A principles-based design approach is strongly preferred. In particular:

- principles are flexible and will endure over time which is especially important in the context of the constantly evolving world of data;
- they ensure the spirit and purpose of the law is not overlooked when efforts are made to technically comply with it;
- they provide a better basis for governmental/regulatory collaboration with industry, consumer, and tangata whenua representatives;
- it allows detailed risk-based and trade-off design decisions to relate back to the overarching CDR principles. For example, principles can help guide decision making when trading off the balance between the appropriate level of security to create a safe ecosystem, and the level of access and compliance that is being required of third parties;
- it follows best practice overseas and better enables the recognition of international principles/practices. Some examples of international data principles can be found at **Appendix B**.

We recommend any future MBIE consultation and collaboration processes are undertaken to

[11] The API Centre Terms and Conditions for a Customer Data Consent requires the Customer to know what they are consenting to, including the nature of the information that may be disclosed, the persons to whom that information may be disclosed and the purposes for what the information may be used for by the person to whom the information is being disclosed to. The customer consent must also be freely given, current, and able to be permitted or constrained according to the Customer's instructions.

consider and design the principles that might form the basis of any potential New Zealand CDR.

Our view is that a prescriptive, hands-on, compliance-driven approach to regulation would be costly to implement and to maintain, and it would risk undermining whatever the objectives of a New Zealand CDR aims to achieve. Taking such an approach would risk introducing unlevel playing fields, unintended consequences, and uncertain consumer outcomes.

Experience/learnings of API Centre

The API Centre has worked with a wide range of stakeholder views and perspectives. There has been high levels of collaboration and common interest in making sure the right progressive, innovative, and trusted API ecosystem is being put in place. Our work has focused on promoting interoperable, innovative, safe, open, and efficient API based services for Kiwis. This can more readily occur when a principles-based approach is taken, as opposed to a more prescriptive and compliance driven approach.

e. Governance inclusiveness

Position statement

A collaborative approach should be taken from the outset to designing the governance of any potential New Zealand CDR framework.

Relevant matters

Governance design makes a material difference to the likelihood and efficiency of a CDR achieving its goals. Governance design will determine how the legislation, regulation, accreditation, industry and consumer and tangata whenua representation will all interact together.

Governance design should reinforce a principles-based and outcomes-based approach. It should encourage positive and balanced interactions between regulators and market participants and avoid establishing an interventionist or overly compliance driven framework. Collaboration between all parties will deliver the best consumer outcomes. Governance design should nurture this collaboration.

The regulatory and governance framework should provide well-defined expectations, especially with respect to accountability for data throughout its end-to-end lifecycle, and across a range of consumer-focused data scenarios.

The potential for a CDR in New Zealand is new and it is evident that the sectors that it could be applied to are among the most highly regulated in New Zealand already. Care needs to be taken with this in mind, to avoid creating overlaps or inconsistencies, and to accommodate existing regulation. This is more likely to be achieved by only having a single regulator responsible for any potential CDR in New Zealand. The Australian experience has highlighted the disadvantages of having a fragmented oversight structure with a move now to consolidation under a single agency.

We recommend that a future MBIE consultation and collaboration process should be used to explore governance design options.

Experience/learnings of API Centre

Appropriate governance structures and processes mattered a great deal when delivering the industry API Standards. The key successes to date have been attributable to balanced representation, the seeking of views from across the ecosystem spectrum, and having robust and transparent processes in place in order to arrive at decisions. Our governance design intentionally balances API Providers, Third Parties, and independent representatives who all have obligations to act in the best interests of the API Centre.

CDR data, security and technology

Considerations of how a potential New Zealand CDR manages data, security and technology should:

- ensure security is inherent;
- empower industry to be responsible for the technology and the technical standards; and
- have clarity on exactly what data is captured by any potential CDR.

The following sections explore these issues.

f. Security must be inherent

Position statement

Security of a consumer's data is a key consideration and data needs to be protected. Ensuring high levels of security should be a collaborative and not a competitive issue. Industry is best placed to design and manage security. The API Centre's 'security profile' could be used as the starting point for considering a consistent and safe approach to exchanging consumer data.

Relevant matters

Consumers need to have confidence that their data is safeguarded at all times, including both when their data is in transit and when their data is stored by authorised organisations.

Strong security requirements need to be in place for any party involved in the handling or keeping of data, as a data provider, a third party, an intermediary or any other recipient of the data. These security requirements need to place protections over a consumer's privacy, and protect the data from abuse, fraud, and criminal enterprise.

Security and data safety issues should be proactively collaborated on as a part of any CDR framework, both initially and on an ongoing basis. Our view is that industry is better placed to set and maintain its security requirements (as opposed to any regulations beyond a high-level principle of requiring the secure management of data). Based on the API Centre's experience in developing its banking data security profile[12], our initial views on how industry could ensure security include that:

- common security profiles and standards should be adopted so that third parties do not have to connect to each data provider using a different security profile;
- minimum security standards for the exchange of CDR data should be adopted, used and maintained. Conformity with these security requirements should form part of any accreditation process and the subject of ongoing certification;
- minimum security requirements should be set for third party accreditation and ongoing certification for their secure storage of CDR data;
- minimum security requirements should balance the appropriate levels of data security, while ensuring they do not impose unduly high or unnecessary compliance burdens and costs on third parties;
- certifications provide evidence of good third party security (for example ISO 27001) and these should be built into the initial accreditation and ongoing requirements. These requirements should be as efficient as possible and should look to re-use existing certifications. A lesson from Australia is that third parties that were already ISO 27001 certified had to be re-certified again under ISO 27001 to meet the CDR accreditation criteria which duplicated time, cost and

[12] https://paymentsnz.atlassian.net/wiki/spaces/PaymentsNZAPIStandards/pages/298909749/FAQs+about+the+v2.0+API+standard#What-does-the-security-profile-do%3F

effort (but it is understood that this is now being reviewed in Australia);

- these security standards need to provide data providers, data intermediaries and third parties with the right tools and information to operate their internal risk-based and fraud detection checks and processes;
- international security best practices and standards are adopted where appropriate and kept under review.

The ongoing certification of adherence to the security requirements by the principal parties in the CDR arrangements will be something to consider, to ensure they maintain vigilance in this regard.

Experience/learnings of API Centre

The API Centre has invested in adopting the NZ Banking Data Security Profile[13], which is based on the OpenID Foundation's FAPI Read+Write specification document (and adjusted to fit the New Zealand market). This security profile stipulates requirements for how API Providers can safely make APIs available for use by Third Parties. This applies to both the Payment Initiation and Account Information API specifications (and could apply equally to any sector). The security profile aligns with best practice overseas (as seen in the UK and Australia).

The API Centre's work has demonstrated that technical and security experts are able to collaborate to produce an appropriate, efficient, and durable model for use in the New Zealand market.

g. Technology and technical standards

Position statement

The industry should be empowered to be responsible for the technology and the technical standards needed to support the delivery of any potential New Zealand CDR.

Relevant matters

As described by Deloitte[14] (in their report on Canada), there are two broad regulatory options when it comes to this:

- "*Centrally defined standards*: Regulators can develop highly prescriptive technical standards that mandate specific technologies and processes for data sharing, while strictly enforcing compliance; or
- *Generator-led standards*: Regulators can define broad, high level data-sharing policies, while allowing financial institutions and third parties to independently develop standards, technologies, and processes to abide by them."

We believe the latter option should be preferred for New Zealand. As such, regulation should be limited to mandatory minimum data sharing criteria (i.e. what, not how), to provide certainty and the basis for interoperability. But the bulk of the technology requirements and detail, and the design choices around them, should be left to be coordinated at an industry level. In particular, to develop right-sized common standards which will work from the point of view of those directly involved.

However, constructs should be put in place so that any industry base common standards that are developed and agreed are enforceable under the CDR regime.

There is a risk that regulatory prescribed technical standards or technology approaches become outdated and restrict organic innovation. There is also a risk that pre-emptive assumptions are made about sustainable business models which turn out not to be the case. Technology evolves over time and standards will need to do the same, so enduring frameworks will need to be put in place to

[13] https://paymentsnz.atlassian.net/wiki/spaces/PaymentsNZAPIStandards/pages/294486919/NZ+Banking+Data+Security+Profile+v2.0.1

[14] Deloitte's Creating an open banking framework for Canada - Considerations and implications of key design choices, page 39

support and facilitate standards evolution, standards maintenance, managing the lifecycle of a standard or technology, and developing new standards or technologies as required. All this underscores the need for direct industry involvement and management.

While technical standards will likely form a part of any potential New Zealand CDR regime's landscape, the standards should align with and have their scope informed by clearly defining the consumer outcomes and use cases that the CDR aims to achieve. Accordingly, if a CDR is principles-based and focuses on the clearly defined consumer outcomes (i.e. use cases that describe what you want New Zealanders to be able to do with their data), then industry will be able to design the technology and technical standards that best delivers this.

We suggest that all designated sectors should strive to use the same common core technical standards base where it makes sense to do so, e.g. use the same security profile[15]. International standards should be leveraged as much as possible, and then tailored to fit the New Zealand environment.

Experience/learnings of API Centre

Industry has shown itself to be organised and capable of collaboratively delivering strong standards under the banner of the API Centre. There has been a significant investment of time, expertise (both business and technical) and resources in developing the existing API standards that support and enable New Zealand's open banking outcomes.

To avoid unintended damage, this investment in API standards needs to be protected and leveraged in any future New Zealand CDR regime. It is likely that it will take time to design and enact any New Zealand CDR legislation. During this transition period, the industry would benefit from having regulatory certainty as soon as possible on any expected impacts or overlaps that a CDR might have on the API Centre's standards and on our ongoing efforts to develop standards and an API ecosystem.

The standards, processes and institutional knowledge built up in the API Centre is an asset for the future of New Zealand's open data economy. If it is designated under any CDR regime that asset should continue to be protected and nurtured through any CDR transition period. Further, the API Centre's API Standards contain many elements, tools and approaches that could be applied to any sector context and help New Zealand's open data economy, i.e. they do not exclusively apply to just payments (e.g. security profile, the sandbox, the API Centre Register, the customer experience guidelines, standards development methodology, the technical design of standards, etc.)

The API Centre would, of course, need to review its standards in light of any potential CDR arrangements that ultimately emerge from the current consultation. It will be important to ensure that its standards (and its operations) align with any future legislation. It is our view, however, that what is in place with the API Centre currently is broadly appropriate and in line with what is needed for New Zealand.

h. Data clarity

Position statement

There needs to be clarity on exactly what data is captured by any potential CDR and, with that, clarity on how data is managed through its lifecycle.

Relevant matters

How data is defined and managed will make a material impact on the efficiency and workability of

[15] The NZ Banking Data Security Profile v2.0.1 is based on the OpenID Foundation's FAPI Read+Write specification document, and applies this standard to the New Zealand market context. This specification is used to help define requirements for how API providers can safely make APIs available and connect with third parties.

the CDR regime. The main focus should be on specified raw data (i.e. primary data that has not been augmented, derived, or enhanced).

Different types of raw data carry different levels of risk. This should be recognised and any applicable requirements should be made proportionate to the degree of sensitivity of the data. For example, payments initiation (if it falls under any potential CDR's scope) is a 'move money event' and may result in immediate financial loss if the authorisation process is compromised. Where there is higher risk, the third party accreditation requirements should be tiered in proportion to that risk.

An end-to-end lens should be applied to the data through all the stages of its life cycle (from granting access to the data, through to the treatment of data once the consumer's consent expires or is revoked). The consumer needs to have a clear understanding of what their 'data rights' are across all of these stages. This includes having absolute clarity on what third parties can do with CDR data that the consumer has granted consent for them to access.

It will be important to clarify whether there are any data management obligations or restrictions on what third parties are able to do with any consumer data obtained in accordance with the consumer's consent. For example, must consumer data stored by an organisation, be logically separated from other internal data sets, or is it able to be merged?

Our view is that enhanced or derived data should be out of scope and left in the commercial domain. This is because there needs to be the right mix of incentives to innovate and create value from the raw data, without the resulting value-added data then falling into the scope of the CDR regime.

Principles of data reciprocity and data equivalency are more complicated and risk unintended consequences. In light of this their consideration should be deferred, until any potential CDR is more established and it is clear what the consumer benefits would be.

Experience/learnings of API Centre

We have learned that there is a lot of complexity in the detail, particularly with regards to data-related risk, compliance, formats, and data access. This was evident when it came to development of our Account Information API standard and the defining of the raw data for the purposes of that standard. Consumers need to know exactly what data they are giving their consent to.

i. Product data, opening accounts and switching banks

Position statement

Bank switching rules and processes (from a current bank to a new bank) work well today. While bank 'product data' information and standardised product APIs could be included in any potential New Zealand CDR, our research and experience to date leads us to believe there is lower demand for these use cases. We have doubts on the relative levels of consumer benefit that might be realised from bank product data, compared to other consumer/personal data areas. The opening of bank accounts should be out of scope due to compliance considerations/complications.

Relevant matters

A theme of MBIE's discussion paper focuses on comparing product offerings and switching of product providers. In a bank account context, this can be broadly broken down into the following three steps:

1. the consumer identifying the preferred bank product, e.g. an account;
2. the consumer opening a bank account product at the new bank;
3. the transferring of history and arrangements from the old bank to the new bank, and potentially closing the old bank account.

For the purposes of the first step (the consumer identifying the preferred product) while we acknowledge the theoretical benefits of product comparison data being available, we have doubts as to the effectiveness and level of consumer benefit provided by a CDR regime requiring product comparison data to be available. This is due to:

- our understanding that the experience in the UK requiring bank product data to be made available has had limited impact and this has not been the area where innovation has best occurred;
- consumers often have accounts at more than one bank already (unlike other utility markets such as the telecommunications or electricity markets where consumers only have one provider);
- questions as to whether product comparison tools would actually address the root cause of any perceived or actual lower levels of bank switching activity;
- our research[16] indicates that bank product comparison was rated as having the lowest appeal of potential new products and services that could be enabled by open banking. Only 29% of those surveyed found appealing the "ability for a third party to make product comparisons and recommend the one that is the best fit for your needs, i.e. using your transaction history." This was significantly less appealing than all other consumer/personal data focused ideas such as the ability to see multiple transactions in one place (45%), more advanced budgeting tools (40%), analysis of your savings and money use to provide customised savings (37%), and easier credit/finance approvals (34%).

With respect to the second step of opening bank accounts (as a new customer to a bank or an existing customer accessing new credit products), we note that this is already a highly regulated area. Opening a bank account as a new customer requires the bank to undertake AML/CFT and 'know your customer' checks. Accessing credit based banking services requires a bank to exercise a duty of care to ensure the product is appropriate for the customer. The Credit Contracts and Consumer Finance Act requires lenders to act responsibly when offering debt/credit products. Having third parties digitally intermediating the opening and closing of bank accounts and products could complicate the bank's existing obligations. We also note that increasingly banks offer digital processes to open accounts and access products. This is expected to become easier over time as New Zealand's digital identity frameworks and solutions are implemented and potentially make it a simpler onboarding process for customers. Again, the theme here is that there are significant questions as to the level of consumer benefit that a CDR regime could offer if it required new processes on the opening and closing of bank accounts and other banking products.

The third and final step focuses on the switching/transferring of history and ongoing arrangements from the old bank to the new bank, and potentially closing the old bank account. Payments NZ already has inter-bank rules in relation to switching from one bank to another bank[17]. These work well and the customer only needs to deal with the new bank and fill out a one-stop form to complete the switching process. Payments NZ's account switching rules allow a customer to complete a one-stop form with their "New Bank" that:

- authorises the "New Bank" to contact their "Current Bank" to: obtain balances; obtain details of existing payment authorities; to close an account; to transfer the balance to the "New Bank"; and to cancel any automatic payment and/or direct debit authorities operating on an account;
- instructs their "Current Bank" to execute all of the above mentioned actions;

[16] Research commissioned by Payments NZ and conducted between 2-16 September 2020. Base: Total N=1,012. Q: Below are some ideas for new products/services that could be created with open banking, how appealing are each for you?

[17] See https://www.paymentsnz.co.nz/resources/switching-banks/

- instructs the "New Bank" to establish equivalent payment authorities on the new account;
- puts in place an indemnity for the switching process; and
- for all of the above to occur within 5 business days.

The existing switching process is fit for purpose and protects consumers and, as such, it is unclear what additional value a CDR regime could bring to this. We again emphasise the need to identify the consumer outcomes that need to be achieved, and we can then assess any gaps and what role, if any, a potential New Zealand CDR regime might play in this area.

We also note that the API Centre's existing Account Information API allows the ability for a party to access transaction history. We note that in the UK, some 'new' banks use their equivalent account information API, with the customer's consent, to download the 'old' bank's transaction history and make that data available again to the customer within the 'new' bank.

In summary, our view is that while there are some benefits of product comparison data being available, we have material doubt as to the real-world effectiveness and level of consumer benefit that focusing on this area will achieve. We suggest that should this area warrant further investigation, a detailed assessment of the 'customer journey' and a deeper understanding of any barriers or points of friction need to be better understood, before any obligation is made on the banking sector in this area by a potential New Zealand CDR regime.

Experience/learnings of API Centre

It should be noted that the API Centre's soon-to-be released v2.1 Account Information API standard aims to provide guidance on what types of accounts the standard applies to e.g. current accounts, savings accounts, credit card accounts, loan accounts, etc.

CDR implementation

Considerations of how a potential New Zealand CDR could be implemented include:

- phased implementation;
- write API's being left for later phases;
- payments initiation needing separate consideration and not being included in any initial New Zealand CDR; and
- the need for all Third Party actors to be taken into account

The following sections explore these issues.

j. Phased implementation

Position statement

Any potential CDR is not a quick win and its implementation should be phased.

Relevant matters

As is evident from the experience in other jurisdictions, the scale and complexity of CDR should not be underestimated. The likelihood is that it will take time to establish a New Zealand CDR framework, to design and run accreditation processes, to build and implement the necessary systems infrastructures, to test and establish interoperability, and then to develop and build a mature market that is extensively used by consumers. If New Zealand attempts too much, too soon with a lack of clarity or understanding on measurable outcomes and consumer benefits, then sub-optimal outcomes are more likely.

A pragmatic and outcomes driven phased approach should be taken to any potential implementation. Consumer outcomes should be the driver of any phased implementation (and consideration needs to be given to how this input is provided). It is important to understand also that there are significant timeframe tensions between different sets of stakeholders. Generally, data providers would prefer longer timeframes whereas third parties would prefer shortened timeframes. A phased approach would help to resolve or manage these differing expectations. A high level of consultation and collaboration should go into setting the phases to help ensure outcomes that carry the highest consumer benefits with the lowest cost and risks can be targeted first.

Functionality that has higher risk or greater complexity (such as write APIs) should not be tackled in the early stages of any implementation but kept for later consideration.

Ideally, a phasing roadmap should be laid out. This should include when consideration will be given to unresolved issues. Stakeholders would then have future certainty as to what is to be delivered and when, so they can make accurate and timely investment decisions. The roadmap will need to have a well-articulated timeframe for implementation. This will need to balance providing adequate time for organisations to allocate their resources in order to implement complex change, while at the same time ensuring there is positive momentum.

Experience/learnings of API Centre

The API Centre has adopted a phased approach with its standards. This has made things much more manageable. A key lesson has been that functionality that carries a higher level of inherent risk, takes considerably more time to develop and implement.

k. Write APIs to come later

Position statement

'Read' first – 'write' later. Any potential New Zealand CDR should first focus on consumers accessing and sharing their readable data. While there is potentially significant value in 'write' APIs being widely available in New Zealand, the marked step-up in complexity, risk, cost and overlapping regulatory regimes all point to consideration of 'write' APIs being deferred to later phases.

Relevant matters

There is no doubt that there is third party demand for 'write' permissions (e.g. opening or closing new products or accounts, changing consumer details, etc.). However, there are some key reasons to defer the consideration of write permissions until later phases of New Zealand's CDR development process:

- *Higher risk and complexity*: Write permissions have significantly more risk and complexity;
- *Tiered accreditation*: Australia's CDR and the UK's open banking regime provide the accreditation and access framework that grant third parties the right to connect with data holders. If this connection included 'write' access, then the accreditation requirements would likely need to reflect the higher level of risk by potentially adding increased third party controls and liability obligations (compared to that of 'read' APIs);
- *Generally lower consumer demand compared to read data use cases*: Our research (described later in this submission) indicates there is a significantly lower level of consumer interest in some use cases that require 'write' access, than in use cases that require 'read' access;
- *Overlapping regulations*: The use cases that are often referenced as a part of 'write' access, in most cases, are already highly regulated. For example, in relation to the opening of accounts or payments. The degree a CDR framework might overlap with existing regulation and add complexity is more likely under 'write' permissions than 'read' permissions;

- *Phasing*: All of the above point to 'write' permissions having higher levels of complexity requiring greater consideration and care in order to protect consumers. The recommended phased implementation approach should reflect this and focus first on enabling 'read' data consumer outcomes. The scope, cost and effort of implementing readable data will be in itself a very significant implementation task for the industry. This is consistent with the Australian approach where they followed a 'readable data' first approach and are only now considering 'write' APIs. This Australian phased approach managed the size of scope that was first being implemented.

If phased implementation of any potential CDR is preferred, it would likely be phased across two dimensions: a) sectors and b) consumer outcomes and the data required to support those outcomes. If banking is a designated sector, we suggest that the first implementation should be focused on the consumer outcomes that can be supported by the 'readable data' that is contained in the API Centre's Account Information API standard[18]. This standard covers the likes of: account balances; transaction history; statements, payment beneficiaries; current direct debits and automatic payments; future scheduled payments; and information about the account holder such as name, email, phone etc. The scope of the Account Information API standard provides a head-start for any potential CDR's designation of the banking sector, and it also has potential to have its approach leveraged for New Zealand's open data economy.

Experience/learnings of API Centre

As noted, the API Centre's Account Information standard focuses on readable data. A significant amount of effort and investment was needed for both the creation of this standard, and for API Standards Users to commit to and implement this standard. This is valuable work and represents a significant head-start on what might be needed for any potential CDR that has application to the banking sector.

l. Payments initiation considerations

Position statement

Consideration of payments initiation being included in any potential New Zealand CDR should be deferred until after a read CDR has been implemented and has been in operation for a meaningful amount of time. Payments should be considered by itself, separate to consideration of "write" permissions. Industry will continue its current efforts to further maintain and enhance the Payments Initiation API standard notwithstanding any potential New Zealand CDR's initial implementation.

Relevant matters

While our Payments Initiation API standard is technically a "write" API, we contend that bundling payments generally into the "write" data group is misleading and fails to take important differences into account. Given the purpose of Payments Initiation is to move money from one bank account to another, its nature is completely different to the notion of changing consumer data through "write" permissions. Payments should be considered and approached separately to the general "write" question.

The movement of money (payments) is treated separately in Europe and in the UK. Payment System Directive 2 (PSD2) has a payments-specific accreditation and access framework. Australia's CDR regime also currently excludes write APIs including payments initiation. However, Australia is currently consulting on "*on how the Consumer Data Right could best enable payment*

[18] https://paymentsnz.atlassian.net/wiki/spaces/PaymentsNZAPIStandards/pages/298909721/Overview+of+the+v2.0+standard#Account-Information

initiation[19]*."*

The payments industry, through the API Centre, has made significant strides towards enabling payments-based innovation through the use of the Payments Initiation API standard[20]. We believe there is a need to articulate exactly what problem a potential CDR would aim to solve in relation to payments, as this is currently unclear. For example, is the problem timeline driven (i.e. "very limited implementation of the standards or partnerships between API providers and third parties"[21]), or is it something more fundamental about the payments initiation model that the industry has developed?

The following important issues arise when it comes to considering payments initiation in the context of any potential New Zealand CDR:

- whether payments would require its own sector designation such as in the UK (given its different function and purpose of moving money);
- the management of risk, liability, consumer protections, fraud controls, and loss allocation;
- how regulation would work in the context of the current rules of Payments NZ and in the context of the future designation of Settlement Before Interchange (SBI) and High Value transactions under the Financial Market Infrastructures Bill; and
- what it means more generally for the future of New Zealand's payment systems.

Experience/learnings of API Centre

The API Centre does have a Payments Initiation API standard[22] that allows for Third Parties to offer secure payments services, with consumer consent. The API Centre is committed to the ongoing development of this standard, and our API Standards Users are also committing to its adoption.

m. Third parties

Position statement

Any potential New Zealand CDR needs to accommodate all types of third parties and scenarios.

Relevant matters

The transfer of data may not simply involve the banks and the third parties. Other parties may be interposed in the arrangements such as data intermediaries that connect with multiple data providers and then provide a single point of technical data access for a range of accredited third parties. There is also the possibility of third parties outsourcing to technology support companies (i.e. "powered by…"). Data providers and/or third parties may also enter into agency arrangements to manage or process data under a CDR regime.

The CDR needs to cater for these different arrangements to ensure it is fit for purpose. This particularly applies to the role of data intermediaries. For example, should intermediaries be able to read or store the consumer data? What should be conveyed to consumers about their involvement? What needs to be put in place in terms of cascading obligations when outsourcing is undertaken?

The design of any potential New Zealand CDR should accommodate the various arrangements and provide certainty in relation to them. The Australian experience bears this out, as they are only now looking to address the role of data intermediaries more explicitly.

Given the portability of consumer data, there needs to be clarity on what is permissible under a CDR

[19] The inquiry considers how the CDR, were it expanded to enable write access, could relate to or interact with existing and future payments systems and infrastructure, such as the New Payments Platform (NPP), Bulk Electronic Clearing System, and EFTPOS.

[20] https://www.apicentre.paymentsnz.co.nz/standards/available-standards/payment-initiation-api-standard/

[21] MBIE's discussion document for "Options for establishing a consumer data right in New Zealand", page 8.

[22] https://www.apicentre.paymentsnz.co.nz/standards/available-standards/payment-initiation-api-standard/

regarding the transfer of data from a CDR accredited third party to a non-accredited data recipient, i.e. data leakage from within the CDR framework to parties outside the CDR framework. The design of any cascading obligations and any resulting implications of any consumer protections provided by a CDR framework need to be carefully considered in this area.

There should a level playing field across all third party segments, e.g. from FinTech, enterprise level companies through to global BigTech players. Efforts should be made to ensure that domestic third party organisations are prioritised, or at least not disadvantaged relative to global players by any potential New Zealand CDR.

Experience/learnings of API *Centre*

The API Centre worked with industry to design a framework to provide certainty when (with the consumer's consent) a third party passes data to another party (termed a Permitted User). The API Centre's Terms and Conditions put cascading obligations[23] onto a registered Third Party with respect to the transfer of data (which is in line with Privacy Act obligations). This ensures there are consistent obligations and liabilities through any chain of data exchange.

Conclusion

Payments NZ and the API Centre team welcome the opportunity to make this submission. We will continue working and consulting with MBIE over the coming period to ensure we can collectively deliver the right outcomes and benefits for all Kiwis.

Steve Wiggins

Chief Executive, Payments NZ Limited

20 October 2020

[23] In the API Centre terms and conditions a "Permitted User" is a person given access to Customer Data/initiate a payment through an arrangement with a Third Party. The Third Party has cascading obligations to ensure the Permitted User: complies with Customer Consent obligations; ensuring it has adequate security measures in place to protect Customer Data; and any acts/omissions of the Permitted User in relation to Customer Data / payment transaction through the use of a standardised API.

Appendix A

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

Name and organization:

Name	Steve Wiggins
Organisation	Payments NZ Limited and the API Centre
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?*
	Refer to key issues a) and b) in our submission for our detailed response. In summary, in order for any potential New Zealand CDR regime to be successful, the consumer needs to be at the heart of New Zealand's CDR's design. It is important that the consumer's genuine needs and interests be placed at the centre of any potential New Zealand CDR and are not trumped by the commercial and technology interests in the sector. If New Zealand's CDR is well designed and has the consumer at its heart, then this will lead to opportunities for businesses to develop or further improve the products and services they offer to customers. There is ambiguity in the discussion document about the relationship between data portability and the consumers "data rights". It is not yet clear whether the data rights are to be focused just on data portability, or if these data rights also include other considerations as well. Any next steps should define what "data rights" actually include. We believe that: • consumer and tangata whenua interests should be at the centre of discussions when considering the development of any potential New Zealand CDR; • a New Zealand CDR should only be introduced if it delivers materially better outcomes for consumers; • consumer interests should be put above the interests of commercial parties; and • a greater emphasis is put on the consumer and the protections over their personal data, than on facilitating data flows across markets and competition.
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?*
	Refer to key issues b), d) and j) in our submission for our detailed response. In summary, yes, we agree with these, which is why we believe a principles-based approach should be taken in the design of any potential New Zealand CDR. If the main purpose of a

	potential New Zealand CDR is to put consumers in control of their data, then the CDR regime will need to foster the consumer's trust. In order to grow this trust, consumers will need to know that they are in control of their data, understand what data is portable and to whom, and that they can rely on the system's safeguards. Accordingly, a holistic view should be taken when developing a framework that can foster, grow and protect consumer trust. We believe that the benefits and costs/risks outlined in the discussion document are very generic. Their emphasis and importance changes significantly depending on what sector is being considered, and what the end consumer benefit or outcome is that is being assessed. There is a risk in assuming that these blanket benefits and costs/risks will equally apply across all potential sectors, scenarios and consumer use cases. In addition to this, a phased implementation must be taken. The reality is that it will take time to establish a CDR framework that will deliver consumer outcomes, to design and run accreditation processes, to build and implement the necessary systems infrastructures, to test and establish interoperability, and then to develop and build a mature market that is extensively used by New Zealanders. If New Zealand attempts too much, too soon with a lack of clarity or understanding on measurable outcomes and the consumer benefits being targeted, then sub-optimal outcomes are more likely.
3	*Are there additional benefits, costs or risks that have not been explored in the above discussion on a consumer data right?*
	See the response to question 2.
4	*What would the costs and benefits be of applying the consumer data right to businesses and other entities, in addition to individuals?*
	There should not be a difference in the data rights framework for entities and natural persons. We note that the API Centre's standards work to support and enable open banking outcomes that do not distinguish between categories of consumers, including between natural persons, businesses and entities. We do note however that from a technology and implementation perspective, there is significantly more complexity involved if more than one authorisation needs to be obtained in order to grant a consent. Common scenarios where multi-authorisations need to be obtained include: • over joint bank accounts (depending on the respective account authorities put in place by each account signatory); and • business accounts that require more than one account signatory to authorise a payment or allow data access. While there are technical solutions and international standards exist to cater for multi-authorisation scenarios, there is more complexity and cost for data providers to manage the customer experience and the state of a data consent request as it is passed from one account signatory to another. We therefore suggest that any potential CDR implementation approach for the banking sector takes a phased approach by first focusing on accounts requiring single authorisations, followed by a later phase focusing on multi-authorisation use cases. We note that the API Centre's current API standards do not cover accounts that require multi-authorisation. This is a known gap that is being investigated for possible inclusion in future standards versions.

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')?*
	Refer to key issues h) and j) in our submission for our detailed response. It is important when designing the CDR that there is a clear articulation of the outcomes that need to be achieved in order to put consumers in control of their data. The focus needs to be on where consumers will realise the greatest benefits and the role, if any, that a potential New Zealand CDR regime might play in this regard. With this in mind, we suggest that rather than focusing on what types of data should be included or excluded in a CDR, it would be better to focus on what consumer outcomes and use cases are being targeted. Once these outcomes are defined, the data elements needed to support those outcomes will become easier to identify and determine. At a more technical level, industry should be empowered to guide exactly what and how data should be captured and managed in order to meet the consumer outcomes. The primary focus should be on specified raw data. Different types of raw data carry different levels of risk. Risk tiering should be recognised and the applicable accreditation requirements made proportionate to the degree of sensitivity of the data. Payments NZ is doubtful of the relative benefits that might be realised from a product data capability, compared to other consumer-focused data areas. The existing switching process appears to be fit for purpose. We have significant doubts about whether there is any material value that can be gained by bringing bank switching into a potential CDR regime for New Zealand. Opening accounts should be left as out of scope for compliance reasons. We believe there is significantly more benefit to New Zealanders by focusing on 'consumer data', rather than 'product data' (see issue (j) in this regard).
6	*What would the costs and benefits be of including both read access and write access in a consumer data right?*
	Refer to key issues k) and l) in our submission for our detailed response. In summary, the CDR should take a phased approach, focusing on 'read access' first and on 'write access' at a later stage. This is due to the increased complexity, risk, cost and overlapping regulatory regimes involved with 'write access'. If the banking sector is designated, the first phase of implementation should be on the 'readable data' that is contained in the API Centre's Account Information API Standard. This involved a considerable amount of time and effort by the industry to develop. It represents a significant head-start on what may be needed for a CDR that has application to the banking sector. There is a significant amount of value and potential benefit to New Zealanders in the 'read' data functionality. Payments should be considered by itself, separate to any consideration of "write" permissions. The purpose of payments initiation is to move money from one bank account to another and its nature is completely different to the notion of changing consumer data through "write" permissions. However, the industry should continue its current efforts to develop and implement the Payments Initiation API standard, notwithstanding the CDR's initial implementation.
What form could a consumer data right take in New Zealand?	
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?*

	Refer to key issue a) in our submission for our detailed response. In summary, we believe the objectives and outcomes that a potential New Zealand CDR regime aims to achieve should be well defined, specific, measurable, and where applicable, clearly prioritised before designing the CDR framework. At present, the consumer outcomes that are being considered by a potential New Zealand CDR regime are somewhat unclear and there needs to be significantly more effort and emphasis put into defining: • the problems that a CDR aims to solve; • the future-state consumer outcomes that a CDR aims to achieve; and • the use cases that illustrate the consumer benefits that the CDR regime aims to enable. All of the above points should then be measurable. There needs to be clarity on what the "data rights" actually are, and whether these apply only to the portability of a consumer's data. The following initial factors should be considered when developing a CDR regime: • **Control:** empowering consumers to have control of their data. • **Better outcomes for consumers:** it should only be introduced if it delivers materially better outcomes for consumers. • **Consumer is at the heart of the CDR:** the consumer's genuine needs and interests should be the focus of any potential New Zealand CDR, over the interests of commercial parties. • **Consumer protection:** greater emphasis is put on the consumer and the protections over their personal data, rather than on competition and facilitating data flows across markets and organisations.
8	*Do you have any comments on our proposed criteria for assessing options? Are there any additional factors that should be considered?*
	See the response to question 7. Also, refer to key issue c) in our submission for further detail. In summary, having a consistent and strong consumer consent framework is fundamental. The API Centre's consent framework and standardised consumer interaction flow, which is based on international standards, should be used as the starting point for considering an approach to a potential New Zealand CDR.
9	*Do you have any comments on the discussion of Option one: Status quo?*
	See the response to question 10.
10	*Do you have any comments on the discussion of Option two: A sectoral-designation process?*
	Refer to key issues g) and l) of our submission for more detail. In summary, Payments NZ supports ongoing work to determine if a potential New Zealand CDR would best deliver public policy outcomes and lay the foundation for a digital economy. The discussion document appears to indicate that a sectoral-designation approach would be a good starting point for considering a CDR. However, it is our view that it is not as simple as selecting one option and designing a CDR regime on that basis. There are elements of option one (and perhaps in option three) that should also be considered, particularly in light of the

	extensive industry work that is currently underway through the API Centre. We also believe that there are some significantly important questions that remain unanswered with respect to the breadth of sectors that option two might encompass. If this option is proceeded with, MBIE should make it explicit as to what sectors the outer boundary of the CDR's sectoral designation regime might encompass. This includes confirming whether or not public sectors could potentially be designated. This would provide certainty to all sectors as to where they could sit in relation to a potential New Zealand CDR, which in turn will have a material impact on who actively engages in the CDR consultation and in the development process. For example, the discussion document mentions personal health data – having clarity as to whether health data falls within MBIE's ambition for a CDR would have material impacts on how a CDR is designed, who is involved in CDR consultations, and the impact on the public sector as potential data holders under a CDR.
11	*Do you have any comments on the discussion of Option three: An economy-wide consumer data right?*
	See the response to question 10. If option two is not more definitive about the scope of sectors to be covered, there is a risk that becomes option three by stealth, as more and more sectors are brought in.
12	*Do you have any comments on the discussion of Option four: Sector-specific approach?*
	See the response to question 10.
13	*This discussion document outlines four possible options to establish a consumer data right in New Zealand. Are there any other viable options?*
	See the response to question 10.
14	*Do you have any comments on our initial analysis of the four options against our assessment criteria?*
	More emphasis needs to be given to the role and involvement of industry under option two, based on what has already been achieved by the API Centre.
15	*Do you agree or disagree with our assessment that Option two is most likely to achieve the best outcome using the assessment criteria?*
	See the responses to questions 7 and 10.
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?*
	We think the elements outlined are key elements of any CDR regime and we largely agree with the commentary against each one. However, we also note that at this early stage the discussion document remains very high level. There are a significant number of issues to be considered (a number of these are highlighted in our submission) before the design of any legislative framework can be determined. A potential New Zealand CDR should include high-level definitions of key concepts such as: data rights; accreditation; consent requirements; the liability regime; and designation powers.

	More granular aspects such as privacy and security safeguards, and technical standards etc., should be defined at an industry level within sector specific frameworks.
17	*Do you have any feedback on our discussion of any of these key elements?*
	See the response to question 16. Additional key elements could usefully include: • determining what the "data rights" are; whether they are just about portability or whether other matters are contemplated in this regard. This needs to be recognised and included in consultation; • what the consumer trust framework is; • articulation of a problem definition and the consumer outcomes that are being sought to resolve it; • the scope of sectoral designation and how it will be applied; • the liability framework and how risk is assessed and managed (as part of the accreditation regime).
18	*Are there any areas where you think that more detail should be included in primary legislation?*
	Refer to key issue d) in our submission for our detailed response. We are not in favour of a prescriptive approach. A principles-based approach is preferred to facilitate more sustainable and long term outcomes for all stakeholders.
19	*How could a consumer data right be designed to protect the interests of vulnerable consumers?*
	Protecting vulnerable consumers must be provided for in the CDR's design. Start with existing guidelines such as: The Human Rights Commission's best practice guidelines for the prioritisation of vulnerable customers[24] for the insurance sector; and the API Centre's customer consent guidelines[25] section on vulnerable customers.
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?*
	Te Tiriti o Waitangi should shape the introduction of any consumer data right in New Zealand and Māori must be included in its design and in decision making.
21	*How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?*
	See the response to question 19.
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?*
	We recommend that we should first look to use what we already have in New Zealand, and only then look overseas to fill gaps or to refine. New Zealand would not want to extensively adopt another's regime, as each will have its own

[24] https://www.hrc.co.nz/files/5114/7426/1153/HRC_Vulnerability_Guidelines.pdf
[25] https://www.apicentre.paymentsnz.co.nz/standards/using-standards/customer-experience-guidelines/

	pros and cons. There is in fact no consistent approach overseas, as each CDR or open banking type regime will reflect its own domestic circumstances. Aligning with another jurisdiction risks inheriting undesirable elements or adopting features that were designed to fit that jurisdiction's circumstances. Conversely, there are potential benefits by understanding and leveraging the work of other jurisdictions once our own objectives and outcomes have been settled and our preferred CDR framework is designed. Consideration should also be given to any undertakings or principles considered in any of New Zealand's digital economy based trade deals such as the recently signed Digital Economy Partnership Agreement[26] with Chile and Singapore. Through this agreement, New Zealand has obligations around promoting online consumer protections, protecting personal information, data flows, and more. We have the benefit of not starting from scratch in New Zealand, especially in the banking sector. Use should be made of the building blocks that we have already, and then draw on lessons from overseas to inform and improve its design. Ideally, it is desirable to have alignment internationally when it comes to the more technical standards, but at the same time they need to fit and be appropriate for New Zealand's circumstances. The API Centre's API Standards and support tools already provide building blocks for a CDR regime in New Zealand. They have been put in place by the industry after full consideration and are extremely valuable because of this. The API Centre has already made use of what has been done in other jurisdictions. This has occurred in relation to technology standards and with the customer experience guidelines. In each case, they have been 'kiwi-ised' to fit the New Zealand market and culture. This has worked well.
23	*Do you have any comments on where a consumer data right would best sit in legislation?*
	It should be a stand-alone Act. The relationship with other legislation should be clear. Care should be taken with how the CDR regime aligns with the Privacy Act 2020 to ensure that there is no overlap or conflicts between the two regimes.
24	*Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?*
	Refer to key issues e) and g) in our submission for more detail. In summary, we think a single regulator should be responsible for CDR's regulation. We do not have a view as to whether this is an existing government organisation, or a new one. Governance design should reinforce a principles-based and outcomes-based approach. It should encourage positive and balanced interactions between regulators and market participants and avoid establishing an interventionist or overly compliance driven framework. Collaboration between industry, government and consumer representatives will most likely deliver the best consumer outcomes. Governance design should nurture this collaboration. We believe that the industry should be empowered to be responsible for the technology and, with that, the technical standards needed to support the delivery of any New Zealand CDR. Once the shape of any CDR becomes apparent, the industry will then be able to consider how to best organise itself, and whether this should be done sector by sector or by taking a more centralised approach. At the moment, it is too soon in the process to give any further views

[26] https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement/

	on this issue.
25	*What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?*
	Refer to key issue e) in our submission for more detail. In summary, we think having multiple regulators is not desirable. As a CDR regime is new, care needs to be taken to avoid creating overlaps or inconsistencies, and to accommodate existing regulation. This is more likely to be achieved by only having one regulator responsible for CDR. The Australian experience has highlighted the disadvantages of having a fragmented oversight structure with a move now to consolidation under a single agency.
26	*If government decides to establish a consumer data right, do you have any suggestions of how its effectiveness could be measured?*
	All outcomes that a CDR aims to achieve need to be clearly stated and measurable. The most effective measures need to be tied to the consumer, and the consumer outcomes and use cases that a CDR is aimed at. In particular, consumers take-up, their usage, and their satisfaction should be monitored and measured. The API Centre has developed a reporting framework that tracks defined monthly usage metrics, including capturing a variety of useful operational information on usage. We would be happy to share this with MBIE separately. Another key area to monitor effectiveness is around resilience. Incidents are likely to happen e.g. service disruptions, outages, data theft, cyber attacks, fraud, consumer complaints/disputes. The CDR regime will need to be designed to reduce the likelihood of these occurring, but it also needs to be able to proactively manage material disruptions/issues if they do arise. This will serve to engender trust and confidence in the arrangements on the part of consumers. Having measurable objectives in this area is worth exploring. The performance of, for example of the APIs, is also an area worth exploring. There are a range of automated performance tracking tools available in the market that provide insight into the technical performance of APIs, and the functions that support a CDR's outcomes. Obligations on any accredited data providers or third parties to provide notifications of material risk events or non-compliance etc., should also be considered as a part of any CDR regime. The API Centre's terms and conditions provide for notification of material risk events, and they also include provisions on dispute resolution and on non-compliance more generally.

Other comments

Please refer to the covering submission of Payments NZ and the API Centre that accompanies these responses, and which elaborates on matters concerning the consultation.

Appendix B

Case study on international examples of data principles

Drawing from internationally developed data principles would be a useful starting point and provide insight when establishing a principles-based New Zealand CDR regime. These principles then must be aligned, as applicable, with New Zealand laws such as the Privacy Act. A future MBIE consultation process could be taken to pinpoint the principles that might form the basis of a New Zealand CDR. A quick recap of examples of some international data principles follows:

- OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data[27] – Part 2 Basic Principles of National Application. These principles include: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability;
- Consumer Financial Protection Bureau's (USA) Consumer Protection Principles[28] (2017) build on the OECD's principles, but place greater emphasis on financial data and data sharing. The principles include: access; data scope and usability; control and informed consent; authorising payments; security; access transparency;
- The U.K.'s Open Banking Implementation Entity adopted broad design principles including: leveraging international standards; supporting evolution; supporting interoperability. They provide that third parties should not be forced to adopt each major bank's different security profiles (i.e. they have to adopt a common security profile);
- Google's Framework for Responsible Data Protection Regulation[29] (2018) has principles including: collect and use personal information responsibly; mandate transparency; reasonable limitations; data quality; individuals in control; security; accountability; focus on risk of harm (and more);
- NTIA (National Telecommunications and Information Agency, USA) proposes consumer privacy principles[30] centred on: transparency; control; reasonable minimisation; security; and more. They propose taking "principles-based approaches to privacy", and "An outcome-based approach emphasizes flexibility, consumer protection, and legal clarity can be achieved through mechanisms that focus on managing risk and minimizing harm to individuals arising from the collection, storage, use, and sharing of their information";
- The World Economic Forum's Customer Data Governance Principles[31] (2018) developed a set of data principles that could be used as the basis of global harmonisation. Their one-pager set of principles cover: consent; control; security; transparency; and reciprocity;
- Australia's CDR is based on four key principles[32]: being consumer focused; encouraging competition; creating opportunities; and being fair and efficient.

[27] https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part4
[28] https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/
[29] https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf
[30] https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf
[31] http://www3.weforum.org/docs/WEF_FSIEG_Customer_Data_Preamble_And_Principles.pdf
[32] https://treasury.gov.au/sites/default/files/2020-03/200305_issues_paper.pdf