Westpac New Zealand Limited

Submission to the Ministry of Business, Innovation and Employment on the Options for establishing a Consumer Data Right in New Zealand

19 October 2020

Mark Weenink
General Manager, Regulatory Affairs and
Corporate Legal Services and General Counsel New Zealand
Westpac New Zealand Limited

1. Background

1.1 This submission to the Ministry of Business, Innovation and Employment (**MBIE**) is made on behalf of Westpac New Zealand Limited (**WNZL**) in respect of the Options for establishing a consumer data right in New Zealand (**Consultation Paper**). WNZL's contact for this submission is:

Mark Weenink
General Manager, Regulatory Affairs and Corporate Legal Services
& General Counsel NZ
Westpac New Zealand Limited
PO Box 934
Auckland 1010
Ph:
Email:

2. Introduction

Objective of the Consultation

2.1 WNZL welcomes the opportunity to provide feedback to MBIE regarding the Consultation Paper, and supports the desired outcomes of consumer welfare and economic development.

2.2 WNZL supports MBIE's preliminary view that a Consumer Data Right (**CDR**) applied to designated sectors across the economy would promote secure data portability. In our view consumers own their data and should be empowered to use it by disclosing that data to accredited participants in a convenient and accessible form.

2.3 Westpac has contributed to, and supports The Data Economy Collective submission.

Key matters for consideration

We make the following points in relation to the Consultation Paper:

2.4 **Consumer education and uptake will be key to the success of a CDR in New Zealand.** Consumers will need easy to understand information around the sharing and management of their data. This will ensure their decisions are well informed and the risks and benefits are understood. There is a role for both Government and industry in providing consumer education on the new services being created.

2.5 **WNZL supports Government and industry collaboration to develop an 'open data' ecosystem.** In our view legislation (such as a CDR) would provide an overarching minimum set of fundamental criteria, with the more detailed design requirements being developed through an industry-led approach at sector level. This aligns with the principles based approach employed in competition law reforms in New Zealand, would avoid an overly complex regime, and is more likely to meet the assessment criteria proposed in the Consultation Paper (in particular flexibility, cost and speed).

2.6 **We submit that a CDR framework for NZ should comprise:** overarching CDR legislation; a guiding designation statement (providing the key purpose for a particular designation); and industry designed rules and standards to bring the consumer benefits into effect. This framework would enable an effective flow of data between consumers, data holders and data recipients.

2.7 **Given the potentially wide range of in-scope entities and data, we recommend a phased approach to implementation.** This would mean starting with lower risk, less complex data and a more confined set of participants initially. A phased approach is more likely to ensure trust between participants is maintained and will allow consumers to realise the benefits of open data more quickly.

3. Our response

3.1 Our specific responses to the Consultation Paper's questions are set out in the attached Appendix.

Appendix 1 - Submission template: Options for a Consumer Data Right in New Zealand

Name: Mark Weenink
Organisation: Westpac New Zealand Limited (WNZL)

Are you requesting that any of this submission be kept confidential? No

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?***

There are no significant omissions from the Consultation Paper. The paper sets out a high-level framework for how a data sharing system could be designed.

WNZL supports the work undertaken by Payments New Zealand API Centre and the Data Economy Collective who continue to progress commercial aspects of open banking and the development of API services.

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

We agree with the potential benefits, costs and risks associated with a Consumer Data Right (**CDR**) as outlined in the Consultation Paper and set out below our comments.

Benefits

Access and inclusion: The COVID-19 lockdown highlighted the digital divide in New Zealand, with a number of households unable to access devices, mobile data or internet connectivity. Ensuring access and inclusion across society will be important in order to realise the full consumer welfare benefits.

Data literacy:

- Whilst a lack of data literacy and understanding around the use of data by consumers is a risk, the introduction of a CDR could provide a structured process to help address this.
- Consumers will need relevant, easy to understand information about the sharing of data to ensure their decisions are well-informed, the risks are understood and benefits can be fully realised.
- To address this we suggest that Government work in partnership with industry to provide consumer education on the new services being created. This will result in greater consumer understanding of data and how they are able to use it.

Risks

Security and Cybersecurity:

- The CDR framework will need to balance the market-entry of new participants (which provides competition and innovation) with ensuring that all participants meet appropriate security standards – so as not to expose consumers or other participants to additional security risks. Key areas will include robust consumer authentication requirements and security safeguards to protect personal information on participants' systems.
- Customers could become more vulnerable to phishing attacks if new entrants do not comply with established bank standards and communication protocols (i.e. most banking customers are aware that banks will not email with links or requests for login credentials). Data sharing results in a bigger surface area for cyber attacks and data collected by third parties can be stolen or compromised.
- WNZL would expect data breach notifications to include an interface with agencies such as NCSC and CERT NZ where appropriate.

Data Management:

- *Data Protection:* As more data is shared with more parties, the possibility of a data breach increases and effective data management becomes more crucial. Data protection and leakage prevention will be more complex where multiple parties have access to data.
- *Data ethics:* There will need to be consideration of how consumer data may be used. In particular there is a risk in relation to how third parties may use consumer data (such as information on missed payments, or criminal convictions), and it will need to be clear where liability sits in the event of any misuse of data.
- *Data Lineage:* To support a CDR, data will need to be of sufficient quality, and will need to be accurate, current and fit for use. This will also apply to metadata, which will need to be correct and complete to enable transactions to be completed.

Outsourcing: Registered banks in New Zealand are subject to outsourcing requirements under the Reserve Bank's outsourcing policy BS11. It is possible that a bank's CDR framework could be treated as a "basic banking service" and made subject to these outsourcing requirements. This may have implications for the way in which a CDR framework is developed in New Zealand. It will be important to consider the interplay between the RBNZ BS11 outsourcing policy and the CDR to ensure a banking group remains able to create new experiences as a user of CDR services, or invest in new businesses that are users of CDR services.

Liquidity: One of the intended consequences of implementing a CDR in the banking sector is to increase competition, and make it easier for consumers to switch between banks. This could have implications for the way in which on-call deposits are treated in the Reserve Bank's liquidity policy as set out in BS13.

Time for implementation: The Australian experience shows that implementation will take time. As set out in Q5 below, we advocate a phased timeline to speed implementation.

Other Considerations

Consumer centric design: The design of a CDR needs to be consumer centric and needs to work for consumers first. The success of a CDR will turn on how willing consumers are to use it. Aspects that will help achieve this are: adhering to the data minimisation principle (i.e. accredited recipients only receive the data necessary for them to provide the service to the

consumer); transparency around the use of data by accredited participants; and ensuring consumer consent is informed, express and easy to withdraw. A consumer centric design will create a healthy digital ecosystem that fosters data governance and innovation, competition, fair use and consumer choice.

Privacy: Aligning the CDR framework with existing privacy laws will be important. The CDR-specific rules should address those areas not sufficiently covered by New Zealand's existing privacy law. Duplicating standards already in existence or re-writing privacy law more generally will result in complexity and additional compliance costs. If business users are in scope, the CDR framework will need to include additional safeguards, as current privacy legislation only protects "personal information" relating to individuals.

Costs

We agree that implementation will require significant investment and resources for both data holders and data recipients. For smaller participants the significant set up costs and compliance costs may result in barriers to entry, at least in the short term, which would limit the competition and productivity objectives. We would welcome identification of, and strategies to remove these barriers.

To make CDR Data available, data holders are likely to incur both upfront costs as well as ongoing costs, including:

- technology costs, such as system build and integration;
- business costs, such as change management, risk and compliance;
- industry costs, such as administration of industry-funded or resourced bodies;
- the costs of involvement in the development and maintenance of standards; and
- indirect costs including change impacts, servicing and supporting customers, and dispute and complaints resolution.

This investment needs to be considered within the context of managing current operational, security and financial risks in line with regulators' expectations. In addition, resourcing will be challenging in New Zealand where there is a limited pool of skilled developers, and a large amount of regulatory change underway. Compliance with the RBNZ's BS11 Outsourcing Policy, the Financial Services Legislation Amendment Act, and preparation for negative interest rates are areas of focus for the banking industry.

We submit that costs should be carefully managed and distributed fairly to achieve the full benefits of a CDR for consumers. In our view, a business assessment of the commercial viability and consumer benefit should form part of the CDR design process – this would provide an evidential basis for the economic efficiency and consumer wellbeing gains and would frame the conversation around cost to implement versus the value to gain.

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

WNZL supports applying a CDR to businesses and government entities. We believe that businesses (and in particular small businesses) will benefit from a CDR regime. This will, however increase the burden on participants that are required to disclose data on behalf of those entities.

We note that business accounts differ from individual consumer accounts. Business customers often have very complex mandate and consent requirements. For payment authorisation there may be multiple parties involved and payment is based on the client relationship, rather than being simply rule based and automated. WNZL supports a phased approach to implementation whereby a CDR applies to individual consumers first and then extends to business customers and government.

It would be useful to clarify if "businesses and other entities" will include entities such as trusts, associations, partnerships and societies.

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')?***

Consumer data: With respect to including or excluding 'derived data' a key consideration will be the outcomes and objectives that a CDR is seeking to achieve. We acknowledge there will need to be an element of caution in this area as a 'data right' will be a new concept for New Zealand and a clear definition of 'derived data' will be required.

Whilst there may be some 'derived data' which should be in scope in order to meet the objectives of a CDR, we submit that data which has been *materially* enhanced should be excluded from the scope of a CDR. This will protect a data holder's investment in value-enhancing data insight, analysis and transformation tools and activities.

If derived data is included in a CDR, we submit that data holders should be able to recover their costs from data recipients in relation to this data.

A further consideration is the extent to which historical data should be subject to a CDR. Processing historical data into an accessible, machine readable form will be a significant and costly undertaking. We submit that an appropriate balance between the cost to data holders and the benefit to consumers would be to place a limit on the depth of historical data (e.g. within 12 months of the implementation of a CDR regime in New Zealand).

Product Data: Product data is distinct from consumer data. Defining product data is complex and we would welcome further discussion on the benefits and use case of including product data in a CDR.

Defining in-scope data: We submit that in-scope data should be defined and set out in the sector-led and designed frameworks. This will provide certainty and clarity around the type of data that a CDR will apply to for each sector (e.g. particular account types and banking products for the banking sector).

Phasing: We recommend phasing the implementation of data sharing, with an initial focus on individual information followed by small business information. Likewise, more simple transaction account data should be introduced first, followed by more complex products such as mortgage and investment products.

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

There will need to be a clear definition and understanding of what 'write access' entails – i.e. what is the purpose of write access, what type of data would it relate to and what are the associated risk and liability considerations.

Write access commonly means 'make a payment' and enables consumers to automatically act on CDR data to instruct third parties to initiate payments, transfer funds or change providers. However, if write access was also intended to mean 'open a product' (i.e. allows a consumer to initiate a request to create a new account or open a term deposit), this would trigger AML processes and verification checks and would have significant implications for banks, data providers and custodians.

If write access was included in a CDR, MBIE could consider if different accreditation standards would be required, depending on the risks involved.

The benefits of write access would need to be balanced against the security risks and the costs involved in going live with both read and write access at the same time. In particular, the updating of contact details or personal information could present significant risks to data integrity, as the edits or changes may not be able to verified by the original data holder.

If MBIE does include both read and write access, we recommend starting with read access only to mitigate the security risks for customers and to reduce costs and complexity.

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?***

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

Westpac supports the outcomes that MBIE is seeking to achieve and agrees with the proposed criteria for assessing the options. We note that of these criteria, trust and speed will be critical to consumer uptake and ensuring the success of a CDR framework. Having a clear framework and a correctly phased roll-out will assist with timely implementation. We note that an overly complex system will take much longer to roll out.

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

In our view, in the absence of an overarching CDR framework, it is unlikely that maintaining the status quo will fully realise the outcomes and benefits for consumers. However, as noted in Q1 there has been progress on Open Banking initiatives in the current environment.

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

We agree that Option 2 is the most likely to achieve the best outcome using the assessment criteria. This is a sector-neutral approach, which provides flexibility and can apply to sectors such as energy, health, insurance, telecommunications, superannuation as well as banking.

We support the establishment in legislation of a high-level framework that would apply across the entire economy – this would establish a right to data portability and define a clear framework with high-level principles and concepts. We submit that this high level framework should be supported by a guiding policy statement for each designated sector/area, as well as sector specific rules and definitions for implementation.

We submit that responsibility for determining the detailed rules and definitions for implementation (e.g. data-scope and sector outcomes) should rest with industry sectors. In particular, sector-specific binding rules and/or codes of practice could be developed by industry participants and administered by an independent organisation.

This approach would allow sector-led solutions to be implemented. With respect to the banking sector, the work already undertaken by the API Centre could be leveraged, and existing industry participants could work together to define: technical standards; operating procedures; best practice for the interchange of data between participants; and domain/industry specific rules (similar to those in place for managing change in payments).

This aligns with the regulatory approach to competition law in New Zealand, whereby high-level principles are set out in legislation for implementation by industry. It also aligns with and links into the work underway within other key organisations such as Digital Identity NZ. We have set out below our thoughts on the key components of a CDR framework.

Key components of a CDR framework

Overarching CDR legislation: in our view this should be overarching, principle based legislation that is general enough to be applied to different sectors of the economy.

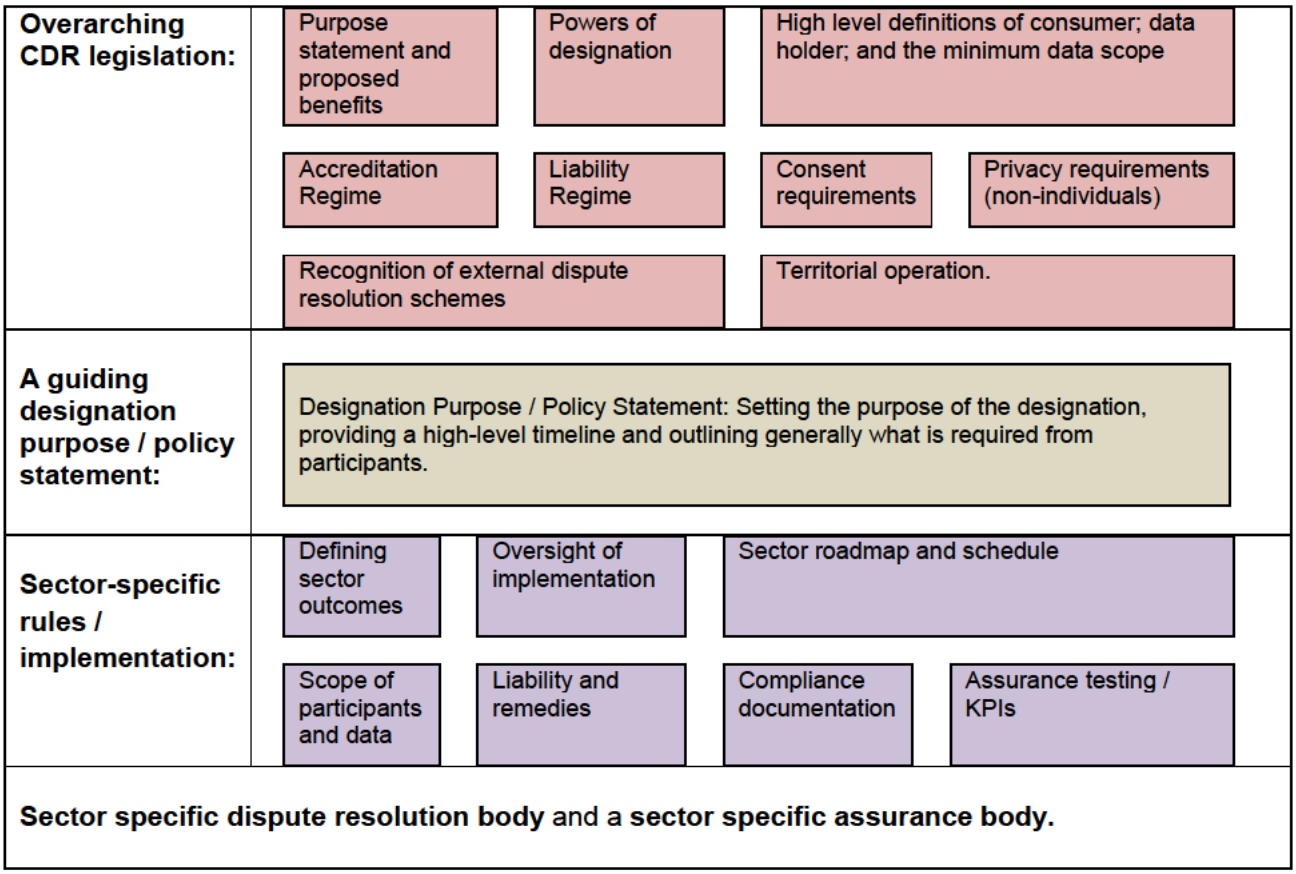
A guiding designation purpose/policy statement: this would set out the purpose and high-level guidance in relation to a specific designation. This could be a sector designation (such as energy or banking) or an area designation such as "consumer wellbeing" or "small business growth". The guiding statement would set out the purpose, the information to be captured from specific groups and would provide a high-level timeline. For a "consumer wellbeing" purpose the following might be in scope:

- Banking transaction data
- Energy consumption
- Grocery purchase summaries

This cross-sector information would provide a richness of data to inform the overall purpose.

Sector-specific rules/implementation: Once a function, area or sector has been designated, there would be an industry-led approach to define sector specific rules and technical standards which would provide the necessary structure to enable a CDR to function within that sector.

Further components of a CDR framework would include a **sector specific dispute resolution body** and a **sector specific assurance body.** Set out below is an illustration of these components.



Governance Structure: having the right governance structure in place will be critical to the success of a CDR in New Zealand. We note that internationally there are divergent opinions on what the best governance arrangements are. We would welcome further dialogue on how Open Data could be governed, and submit that New Zealand can take an iterative approach towards establishing an optimal governance structure. Ultimately, there may be a case for the establishment of a new independent entity, to act as a leadership centre for the Open Data economy in New Zealand.

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

It is unlikely that a GDPR-style right of data portability would achieve the objectives set out in the Consultation paper. This is more of a 'one size fits all approach' and may not contain sufficient detail to fully enable the implementation of data portability across a variety of sectors. A GDPR model is unlikely to lead to scaling up of open banking in New Zealand as it is insufficiently targeted.

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

This option has the potential to create sector silos, as opposed to an overarching framework which can be applied across a range of different sectors.

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

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

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

As set out at Q10 WNZL agrees with the assessment that Option 2 is the most likely to achieve the best outcome using the assessment criteria. We do not have any further comments on the initial analysis of the four options against the assessment criteria.

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?***

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

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

We make the following comments in relation to the key elements of a data portability regime:

Designation

We agree that designation powers should be contained within the overarching CDR legislative instrument. As set out in Q10 a designation could be supplemented with a designation statement setting out the guiding purpose or aim of the designation. With respect to the scope of designation, we submit that the specific types of data and types of data holders within a sector should be determined by industry on a sector by sector basis.

Rules, Data Standards and Reciprocity

Developing data, security and accreditation standards will be a significant workstream. As set out in Q10, we submit that industry has a significant role to play in developing data, security and accreditation standards for each sector. The work that Payments NZ has undertaken in relation to the API workstream will be highly relevant in the banking sector.

The concept of reciprocity should be included in a CDR for New Zealand. This would mean that an accredited third party who receives data from WNZL is also required to make available to WNZL the data it holds, in line with CDR standards. This concept promotes fairness and equality amongst participants in the CDR framework. This could be included in a CDR framework at the option of the consumer, rather than an absolute right.

Accreditation and Consent

WNZL supports the development of an accreditation regime with CDR participants required to meet minimum accreditation criteria in order to ensure:

- appropriate consumer protections for disclosure,
- consumer privacy and data security;
- interoperability with key trading partners; and
- a consistent approach for all users.

As a further consideration, third parties accredited by the ACCC could potentially receive mutual recognition in New Zealand.

In our view, there should be a unified consent model. Consumer consent should be informed (based on transparent disclosure), express, able to be actively managed, and easily monitored and revoked. Consideration should be given to the duration of consent, the process for withdrawing consent and what should happen to a consumer's data once consent is withdrawn.

There will need to be measures in place to protect minors and vulnerable persons. Managing consent where data relates to multiple parties (e.g. joint accounts or trust arrangements) will also need specific consideration. As mentioned previously, we support a phased approach whereby more complex arrangements, such as joint accounts, are brought into scope at a later stage.

Liability, Enforcement and Redress

Accountability and liability are critical elements of a data portability regime and will need to be clear in order for the system to function. We note in particular:

- A liability framework is required to support the flow of large amounts of sensitive information between participants. (e.g. who is responsible for the security of data when it is in transit between businesses).
- Assigning liability in the event of financial loss, or loss of sensitive data will be more complex as more parties are involved.
- Legislation governing customer redress may need to be updated to take into account new open data/open banking business models.
- The liability regime will need to strike the right balance between potential liability to encourage compliance, and sensible defences so as not to deter participation in a CDR framework. The right allocation of risk across ecosystem participants will drive the desired outcomes.

An effective liability regime will link closely with other aspects of a CDR such as accreditation, security, role of intermediaries, fraud and privacy.

The liability regime will need to be very clear in order to provide certainty to participants about where liability will lie - uncertainty as to liability is likely to limit uptake of the CDR. WNZL submits that a level playing field should be established using a fault-based system that

incentivises all participants to secure and protect CDR Data. This will ensure that participants remain liable for their own breaches of the regime, but not those of other participants.

An accreditation regime will assist by vetting participants before allowing participation, to mitigate against the risk of claims occurring, and ensuring that parties have adequate insurance in place to compensate consumer for losses.

Consumers will need to have a clear understanding of what they should do and who they should contact when they feel something has gone wrong. This will form an important part of the overall consumer education on a CDR.

Establishing an external dispute resolution regime will be important. For the financial services sector the existing framework under the Financial Service Providers (Registration and Dispute Resolution) Act provides a useful starting point.

Further considerations

Ethical safeguards in addition to privacy safeguards: There need to be controls in place to ensure this remains a 'responsible technology' that will drive a fairer society. The data exchanged will be used to power machine learning and other decision making technologies. This can assist with increasing financial wellbeing and access to new services. However, there are likely to be concerns around ensuring this data is used fairly. Contemporary ethics including respect, privacy, fairness and transparency should be taken into account to prevent public trust from being eroded.

Digital Identity: The ability to identify consumers through verified and authenticated digital identification will become increasingly important. A NZ Digital Identity will enable not only the services offered by Open Banking, but also a wider open data economy – in particular the integration of data sets across industry categories. We submit that the work underway on developing a Digital Identity Trust Framework should link in with the establishment of a CDR for New Zealand.

Assurance testing: A thorough assurance testing programme should be agreed with industry participants to ensure that there is trust in the efficacy of the framework. The Assurance strategy developed by the Australian competition regulator may provide a helpful starting point.

Territorial scope of a CDR framework. The Australian framework applies to data that is generated or collected in Australia, or which otherwise relates to an Australian person, or goods or services offered to an Australian person wherever they may be located. We submit that New Zealand adopt an equally broad formulation which should simplify administration from a participant's perspective, and ensure that New Zealand consumers are given equal opportunity to access the benefits of a CDR.

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

Protecting the interests of vulnerable consumers requires a combination of factors including:

- CDR participants who recognise and understand the needs of vulnerable consumers – including the drivers and impact of vulnerability and the effect it can have on consumer outcomes;

- staff who deal with vulnerable consumer having the right skills and capabilities;
- product and service design which considers and incorporates the needs of vulnerable consumers; and
- providing clear customer communications through a variety of mediums (e.g. written, verbal, pictorial and in different languages).

In terms of designing a CDR, security protocols, robust accreditation and consent regimes and consumer education will be key aspects for the protection of 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?*

WNZL agrees that the principles of Te Tiriti o Waitangi should guide the establishment of a CDR in New Zealand, and we note the importance of Māori data sovereignty. A further exploration of data as taonga would be of value in the development of an open data regime and may assist with best practice for data stewardship in particular.

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

To assist with digital accessibility the design of websites, tools and technologies should incorporate the needs of people with disabilities or accessibility issues. The use of design principles such as: simplicity; use of colour (e.g. specific colour schemes to aid the visually impaired); and the use of diagrams in addition to text can help achieve this. Compatibility with assistive technologies such as screen readers, keyboard navigation, closed captions and text zoom would also assist with accessibility.

Specialist organisations could be engaged to provide expert input and advice from a consumer point of view, as well as external testing of accessibility.

We would note that any process or design established specifically for vulnerable or disabled customers must meet the same (or higher) protections and standards that are in place for the overall regime.

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?*

Compatibility with overseas jurisdictions should be considered at the outset. One option for this is passporting, which would allow New Zealand companies to interact in Australia. In addition, API standards could align with Australia to allow for interoperability.

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

We support the development of a stand-alone Act. If a CDR was implemented across a number of Acts this could lead to inconsistencies and gaps in regulation.

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

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

We do not believe that a new regulatory body would need to be established. However, due to the wide-ranging subject matter areas of the CDR, there will need to be coordination and communication between existing regulators.

Having multiple regulators involved enables each regulator to bring their specific expertise to the regulation of a CDR, however this has the potential to add further complexity and give rise to inconsistency. This could also lead to confusion around scope and jurisdiction. Establishing a lead regulator would assist with streamlining decision making, give clarity on roles and scope, and provide one touchpoint for industry. Utilising a model along the lines of the Council of Financial Regulators would also be useful.

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

Relevant metrics for measuring consumer outcomes will need to be established to ensure effective monitoring and evaluation of a CDR. Data points for consideration could be the number of consumers sharing data and surveys could be used to determine consumer awareness and trust in the CDR.