RESPONSE ON THE EXPOSURE DRAFT OF THE CUSTOMER AND PRODUCT DATA BILL

ANZ BANK NEW ZEALAND LIMITED

24 July 2023

Public

1. INTRODUCTION

1.1 ANZ welcomes the opportunity to provide feedback to the Ministry of Business, Innovation & Employment (MBIE) on its consultation (the consultation) on the exposure draft of the Customer and Product Data Bill (the draft bill), the discussion document for the draft bill (the discussion document) and the consumer data (CDR) regime more generally. We support the aim and intention of the draft bill, to set standards and safeguards for customer and product data exchange.

1.2 ANZ supports the submissions made by Payments NZ, Financial Services Council and the New Zealand Banking Association in response to the consultation. Given the short window of time to provide a response, the ANZ submission focusses on the key areas that we consider require amendment to ensure the success of the CDR regime.

1.3 ANZ has continued to strongly support the collaborative industry-led approach towards Open Banking through the API Centre. Our approach has been underpinned by extensive customer research which has informed our feedback.

1.4 We are pleased to read that MBIE intends to leverage the significant work already done by the industry. This will increase speed to market, reduce re-work and costs for all participants but only if the initial phase of compliance is aligned to the current standards and sequencing.

2. CONTACT DETAILS

2.1. Please contact [redacted] if you would like to discuss the contents of this response.

3. CONFIDENTIALITY

3.1. ANZ requests that the information identified in this response as requiring confidentiality are kept confidential on the grounds of protection of personal information . If MBIE receives a request to release our response under the Official Information Act, we ask that MBIE consult with us, and our preference is that the information identified is withheld.

4. SUMMARY

4.1. ANZ acknowledge the objectives of the bill and appreciates the complexities and importance of balancing customer expectations and protections necessary to create and sustain customer trust[i] while effectively managing risks and minimising cost to participate[ii].

4.2. In our view, the draft bill does not achieve this balance and some aspects may lead to poor customer outcomes, and potentially jeopardise the success of the CDR regime. Specifically, there are three critical areas where ANZ recommends changes:

4.2.1. Customer protections must go above and beyond the Privacy Act

Customer protections are essential to create and sustain trust, and trust is critical for success of the CDR regime. If customer protections are set too low, there is an increased risk that customer trust will erode overtime and limit customer adoption. The CDR regime in Australia has introduced 13 privacy safeguards[iii] and other prescriptive participation requirements to ensure customers have trust in the CDR regime and control over their data. Some third parties have suggested rules are too prescriptive and costly which has limited third party adoption. The UK experience suggests there is a natural maturity period as propositions are developed and customer trust builds[iv].

ANZ's own research has repeatedly highlighted the complexity of designing for diverse customers who are concerned about the security of their personal information, but have limited knowledge of open banking concepts and may not fully understand the different risks or implications of using open banking services.

It is critical that the draft bill helps customers understand these concepts and ensures clarity in relation to the roles and, responsibilities of each party. Customers must be able to make informed and explicit decisions to participate and know they are protected if things go wrong.

Within the CDR context of data sharing and action initiation services, the Privacy Act alone is not sufficiently sophisticated to ensure the right levels of customer protection are provided. Please refer to section 5 for more details.

4.2.2. It should not be possible for third parties to avoid all CDR obligations by participating via an intermediary

There are no clear restrictions around accredited requestors acting as an 'intermediary' and on-sharing customer data or action initiation rights to non-accredited parties. Please refer to Appendix 1, Figure 3. This introduces a risk that market participants could avoid all CDR obligations and reduce customer protections.

There also appears to be no controls on reusing previously established connections to support on-sharing to additional parties or use cases. Please refer to Appendix 1, Figure 4.

Without changes there is little incentive for parties other than those that plan to be an intermediary to become accredited- please refer to Appendix 2. Therefore, we expect that most participation will occur via intermediaries where requirements are less stringent.

Use of intermediaries also introduces different risks and complexity for customers to understand and navigate, especially when it comes to giving their informed and explicit consent. Please refer to section 6.4 for further details.

The draft bill must acknowledge the role of intermediaries, provide flexibility for different treatment of them and it must prevent third parties from avoiding all CDR obligations by participating via an intermediary. Please refer to section 6 for further details.

4.2.3. The bill must be designed to provide flexibility for collaborative iteration and risk based rules

It is extremely challenging to foresee the complexities and risks associated with the variations and nuances across the different sectors, datasets, use cases and customer expectations. Developing regulations and standards will be complex.

The rapidly evolving landscape for CDR/Open Banking globally, the lack of clear successful precedents to draw from, and a very ambitious scope, means flexibility, continued collaboration with industry and the ability to iterate is key.

Given the natural inflexibility of legislation, we consider that the appropriate place to house the requisite detail, is in the regulations and standards. The draft bill must avoid being too prescriptive, as this may restrict improved collaborative risk-based solutions from being developed and adapted through market introduction of services. Areas where this could become an issue include: consenting rules, ethical use of data, accreditations tiers and requirements and controls when on-sharing of data outside the CDR. Please refer to section 7 for further details.

4.3. In addition, our responses to specific questions raised in the discussion document can be found in Appendix 3.

5. CUSTOMER PROTECTIONS MUST GO ABOVE AND BEYOND THE PRIVACY ACT

The Privacy Act does not provide full coverage in the CDR context and aspects misalign with the draft bill and the CDR regime.

5.1. While we welcome the reliance in the draft bill on the Privacy Act 2020 (the Privacy Act), and its foundations in support of customer protections, this reliance should be framed as broad-based and flexible rather than prescriptive, as we consider that the current Privacy Act and its IPPs do not provide full coverage in the CDR context.

5.2. The Privacy Act only requires organisations to take steps that are reasonable to ensure individuals are aware of the collection, use and sharing of their data. It does not mandate explicit customer consent for sharing of customer data or initiating an action and was not designed for "actions" like making payments, configuring products or switching banks. Furthermore, it is largely principle-based and is not sufficiently sophisticated to deal with legislatively mandated data transfer and action initiation, such as CDR. It doesn't prevent unethical use of data and does not clearly articulate expectations or standards about how data is to be kept safe and secure. These aspects lead each business to make its own judgement.

Additional examples of the misalignment and gaps between the Privacy Act and the draft bill include:

- There are tension points between where the Privacy Act and proposed draft bill intersects, which may impact on the overall MBIE intention of relying on Privacy Act protections where possible. For example, the disconnects between the IPP3 (collection of information from subject) requirements, the bill's 'reasonably informed' requirements, the IPP11 (limits on disclosure) requirements and the bill's lack of any additional authorisation for on-sharing by an accredited requestor.
- Purpose can be difficult to define when a party in the CDR ecosystem acts as a conduit, such as an intermediary.
- Obligations and protections contained in the Privacy Act will not apply to business data, where there is only limited personal information about officers of the business (which may not be being shared depending on the use case).
- There is no proactive assessment of an organisation's judgements or effectiveness and maturity of operational processes, which means issues may only discovered to be insufficient after a breach has occurred or after a customer complaint.

5.3. With reference to points 5.1-5.2, we consider that MBIE needs to give further thought to the Privacy Act and its IPP's in the context of the CDR regime.

5.4. By way of comparison to other jurisdictions, we highlight that Australia's CDR regime has taken the approach of setting out 13 express privacy safeguards, which apply to "accredited persons" or "accredited data recipients" instead of the Australian Privacy Principles (APPs). In addition, certain APPs do apply to CDR data that is also personal information (PI) - except for APP10 (quality of PI) and APP13 (correction of PI). Instead, the CDR privacy safeguards apply. This intersect is not made clear in the draft bill. In addition, we note in the European Union, the implementation of the General Data Protection Regulation (GDPR) introduced a stricter privacy standard under which Open Banking in Europe operates.

5.5. As an alternative, we suggest that MBIE consider the option of a specific CDR/Open Banking Privacy Code of Practice, issued by the Privacy Commissioner under s32 of the Privacy Act 2020, similar to that of the Health Information or Credit Reporting Privacy Codes of Practice. This would provide a bespoke set of privacy and data ethics related safeguards based on the IPPs, drafted for easy use and application in a CDR/Open Banking context.

5.6. A full analysis has not been possible in the timeframe for consultation, but we agree with comments in the discussion document at pages 17-20, that further work is needed. We also suggest that a privacy impact assessment is conducted by MBIE as soon as possible and shared publicly so that the appropriateness of the Privacy Act reliance in the manner proposed can be assessed and identified privacy risks mitigated, with iterative versions to follow, as the CDR framework develops.

Customers must be able to make informed and explicit decisions to participate in the CDR.

5.7. Our research has repeatedly highlighted that most customers have limited knowledge of open banking concepts, hold more privacy value in their banking transactions than their contact details[v], are concerned about the security of their personal information[vi], lack understanding of different risks or implications of using open banking services and extend trust in ANZ to any third party, if consenting in an ANZ channel.

5.8. In this context, customers must be able to make informed and explicit decisions to participate. Customer consent should be unambiguous and, freely given by a statement or clear affirmative action in a trusted and secured environment.

5.9. Informed customer consent requires:

- agreement and consent are actively and explicitly given, not inferred from silence or inactivity, or from pre-selected or hidden options.
- disclosure to be a message that is reinforced multiple ways, through all stages of the customers' journey and that it's consistent across multiple touchpoints. e.g. different data holders, intermediaries, and third parties.
- messages to focus less on educating customers and broadcasting information, and more on giving customers the information that best supports the decisions they are trying to make. This could include the use of trust marks to provide legitimacy and trust in the service.

- clear links and pathways to disclosure and service information that describe the nature of the information and its relevance, and where possible, co-located with the corresponding action or function. For example, at the point a customer is approving a request, highlight that it's important they understand how the service works and link directly to content that covers this area.
- consistent experiences to build reassurance and trust in the CDR regime, including clear and consistent plain language.
- explicitly stating how customer privacy is protected, both within and outside service flows or apps.
- upfront and post-consent understanding of:
    - what information third parties want to access,
    - how their information will be used,
    - what they will receive in return for sharing,
    - how their information will be kept safe and who is responsible,
    - what happens when they stop sharing, and
    - how they can seek support if something goes wrong.
- that they must be able to revoke consent as easily as they give it.
- that accountability and liability of each party is clear, especially in more complex sharing models involving multiple parties with different accreditation statuses see Appendix 1. This point is elaborated further in 6.4.1 and 6.4.4.
- that processes and redress are offered for when things go wrong.

6. IT SHOULD NOT BE POSSIBLE FOR THIRD PARTIES TO AVOID ALL CDR OBLIGATIONS BY PARTICIPATING VIA AN INTERMEDIARY

6.1. For the purposes of this submission an 'intermediary' is an accredited requestor that on-shares customer data or action initiation rights to other parties.

6.2. Data and payment connections that involve intermediaries are an extremely common model overseas, in both regulated CDR and unregulated Open Banking systems. Intermediaries create efficiencies by giving participants a single point of access and often provide value-add services. They are a valuable participant and will be critical for promoting usage and maintaining standards and customer protections.

6.3. The draft bill imposes no clear restrictions around intermediaries on-sharing customer data or action initiation rights to non-accredited parties. There also appears to be no controls on reusing previously established connections to support on-sharing to additional parties or use cases. See Appendix 1, Figure 5 for further details.

6.4. The risks this approach poses, includes but are not limited to:

6.4.1. Third parties can avoid CDR obligations by participating via an intermediary.

- If there is no requirement to pass on CDR obligations to non-accredited parties, then CDR obligations incorporated into the draft bill to ensure customers are protected could be avoided.
- Without changes to the draft bill, there would be little incentive for third parties, other than those that plan to be an intermediary to non-accredited parties to become accredited, see Appendix 2.
- We expect that most participation will occur via intermediaries where requirements are less stringent for third parties and where customer protections are reduced.

6.4.2. Intermediaries introduce more complexity for customers when it comes to providing informed consent which may reduce customer trust, adoption and increase customer complaints.

- Intermediaries don't usually offer a customer proposition or acquire customers directly. They are often interjected into the customer's journey when the customer is signing up for a new third-party product or service and are often not known to customers. See Appendix 1, Figure 2 and Figure 3.
- If permitted, situations may arise where customers are required to sign-up for intermediary services in order to use the third-party product or service. The intermediary service can now use the customer's data for their own purpose to the extent their Terms and Conditions and Privacy Statement allow (e.g. to develop aggregated insights, or on share data to other providers).
- Customers may not fully understand how this works, who they have given consent to, for what and who is responsible if anything goes wrong.
- As per section 5.9, standards and rules must be developed to ensure customers are fully informed and provide explicit consent when an intermediary service is used.

6.4.3. Customers may be at greater risk of fraud and malicious scams.

- Without visibility of non-accredited parties and additional information it will be challenging for banks to undertake effective fraud monitoring or distinguish between legitimate customer requests and malicious ones, such as denial-of-service (DDoS) against core banking services, or phishing/scams that attempts to defraud or harm customers.
- Intermediaries should have a role to play in implementing preventative fraud monitoring and subsequent controls (such as blocking, suspending and terminating users or third parties) to prevent malicious requests.

6.4.4. CDR boundaries will be difficult to communicate to customers when one or more party is a non-accredited party, or an accredited requestor is also using non-sanctioned methods to access data (e.g. screen scraping or reverse engineering):

- Educating and supporting customers to recognise trusted and "safer" sharing systems (See Appendix 1, Figure 1) will help them make the best decisions about how and when to participate. Mixed models (Appendix 1, Figures 3, 4 and 5) will make it difficult to educate customers as to the benefits of CDR and implement trust marks.

6.4.5. Intermediaries may become an attractive target for cyber threats.

- Over time, we expect intermediaries to hold large number of customer consents and data covering many customers and many third parties that the intermediary is intermediating for.
- To protect customer data, standards, processes and requirements should be mandated and assessed on an ongoing basis for intermediaries.

6.4.6. On-sharing of data and actions could be initiated without consent or awareness of account owners.

- It is common for multiple individuals to have rights or interests in a single data set. For example, business and personal accounts commonly have multiple owners and/or operators. Consent from multiple parties is also frequently required to operate these accounts.
- Intermediaries do not have awareness of the account ownership or operating structure.
- The is a risk that data or action initiation rights can be on-shared without knowledge or approval of the account owners/operators, this must be prevented. An example is provided in Appendix 1, Figure 6.

6.4.7. Intermediaries may be able to control who can and cannot participate in the ecosystem with little or no oversight.

- Non-accredited parties would not be required to meet accreditation criteria when onboarded by an intermediary. This approach is in contrast to the Australian CDR and UK open banking models where accreditation is required for participation; and banks that undertake rigorous third party onboarding and ongoing assessments to ensure third parties:
    - keep customers' data safe,

- operate ethically, and
- comply with the law such as The Anti-Money Laundering and Countering Financing of Terrorism Act 2009, various anti-bribery, and anti-corruption laws (both domestic and international) and regulated information security standards such as APRA CPS234[vii].

- Standards rules and requirements need to be developed for intermediaries onboarding and working with non-accredited parties.

6.4.8. Use of proprietary/non-standard APIs connections by intermediaries may over time reduce competition and increase market power of aggregators by reducing portability for third parties they are intermediating for.

- If intermediaries are not required to offer standard APIs for third parties to connect to, this will likely result in intermediaries using proprietary/non-standard APIs to connect third parties. This will make it difficult for connected third parties to port/move to other intermediary services. See Appendix 1, Figure 5.

6.5. These gaps, risks and effective lack of customer protection must be addressed for the CDR to be a success in New Zealand. We recognise that simply "closing" the CDR ecosystem and preventing any access by non-accredited participants is not a perfect answer either.

6.6. The CDR regime must recognise the different roles of intermediaries and the benefits they can bring, while also creating the right incentives to manage risks and provide the protections customers expect. We believe a more granular and risk-based approach is more appropriate with flexibility built into the draft bill. This approach will allow the appropriate level of controls to be developed and passed on by the intermediary based on the risks that customers are exposed to. Please refer to Appendix 1, Figure 7.

6.7. The existing API Centre work has contemplated these issues already. In Australia's CDR regime, unrestricted accredited parties can now sponsor non-accredited parties but must on pass obligations through commercial agreements[viii]. ANZ's Open Banking Payment Requests service is aligned to the Australian model. Intermediary payment services are contractually responsible for ensuring:

- merchants/businesses are onboarded and managed by the intermediary in line with agreed risk management and eligibility criteria;
- customers receive a consistent experience in line with agreed customer experience requirements which include explicit consent and making customers aware that they are in control and can stop sharing their information at any time;
- customers are made clear of the roles and responsibilities of each party; and
- standards and rules are applied and implemented (as applicable) by merchants/businesses to ensure consistent standards are maintained and risks remain managed.

6.8. Our view is that this approach provides the opportunity to develop the right balance between customer choice, protections and scaling the service without individual merchants/businesses needing to be approved by ANZ.

6.9. Card schemes are another model where strict system-wide rules can be managed by intermediaries/sponsors to lower barriers to entry without compromising overall security.

6.10. The definition of an intermediary should be considered alongside the definition of an outsourced provider to ensure they are clearly differentiated. For example, it is possible for an intermediary to act only on behalf of an accredited party or data holder to simplify connections to other accredited participants, they could also operate as a standalone service in their own right for non-accredited parties as outlined in 6.4.2.

6.11. ANZ use and rely on third party services and products to help us provide services to our customers and meet regulatory/compliance obligations. Third party services and products are selected through a robust process and operate exclusively for ANZ under strict commercial terms. Where appropriate material outsourcing arrangements are covered by BS11.

6.12. We do not outsource our obligations and we remain responsible and obligated for any actions of an outsourced provider (within the meaning we give that term). Customers only agree to and are protected under our Terms and Conditions and Privacy Statement. There is no requirement to disclose a list of outsourced providers for other laws and we don't believe it is necessary for the scenario above.

7. THE BILL MUST BE DESIGNED TO PROVIDE FLEXIBILITY FOR COLLABORATIVE ITERATION AND RISK BASED RULES

7.1. The rapidly evolving landscape for CDR/Open Banking globally, the lack of clear successful precedents to draw from, and a very ambitious scope, means flexibility, collaboration and ability to iterate is key.

7.2. Given the natural inflexibility of legislation, we consider that the regulations and standards should contain the requisite detail. The draft bill must avoid being too prescriptive as this may restrict collaborative risk-based solutions being developed. Areas where this could become an issue include:

- consent rules including timeout, expiry, re-consent timeframes and account mandates/authorities for authorisation,
- privacy controls such as ethical use,
- accreditations requirements including tiers and insurance, and
- on-sharing of data - there is a clear ability to on-share data outside CDR obligations, without scope for considering controls in sector designations or standards.

7.3. Developing regulations and standards will be complex, and due to the maturing nature of the global market there are no jurisdictions that can demonstrate a proven model. It is extremely challenging to foresee the complexities and risks associated with variations across the different sectors, datasets, use cases and customer expectations. For example, the CDR regime will need to have the flexibility and nuance to cover different data sets including financial transactions, health data of all kinds, electricity consumption and more. It will also have to provide for different scenarios in which this data will be required, including making one-off payments and switching banks or utility providers.

7.4. Continuing industry engagement is essential to develop risk-based solutions and standards through collaboration, learning and adapting through market introduction of services.

7.5. The current industry approach through the API Centre has also drawn on the lessons from overseas and includes development standards (technical, operational, customer experience and partnering) and frameworks to support a customer centric, right-sized, incremental, and value-led approach to enable Open Banking.

7.6. In this context we believe the standards definition in the draft bill needs to be broadened 'from technical requirements' to 'service requirements' and should include customer experience and consent requirements, operational and accreditation requirements. These work hand in hand to deliver high quality services, ensure risks are effectively managed and customer expectations are met.

7.7. In parallel an outcome and principle-based governance model should be developed to empower industry and regulators to continue to work together. There should be regular reviews for the regime. This model would provide greater opportunity for expert input and flexibility to learn and adapt.

Appendix 1 - Appendix Sharing/Action Initiation Connection Models

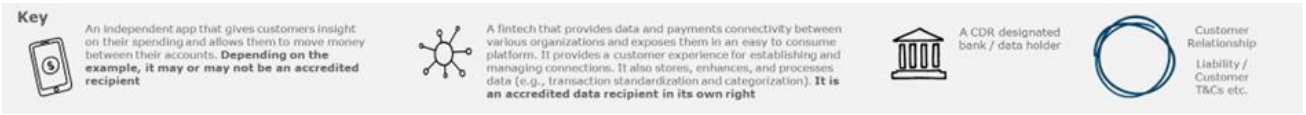


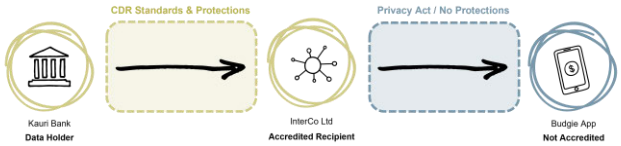
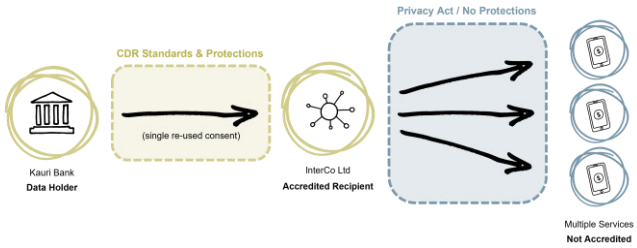
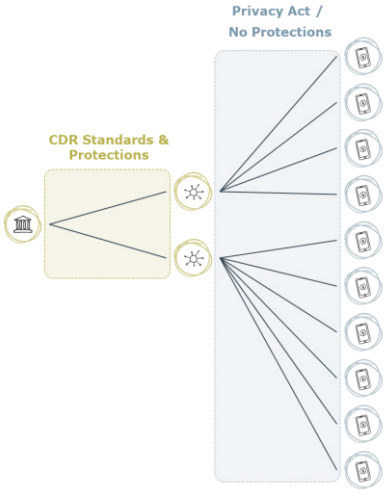
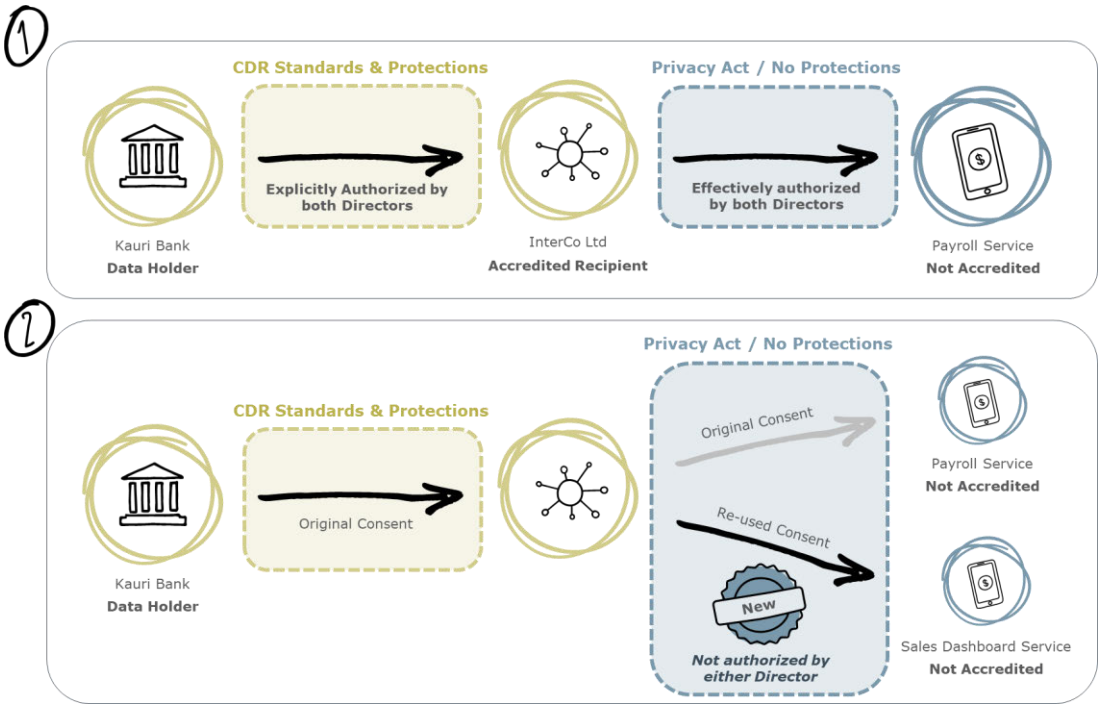
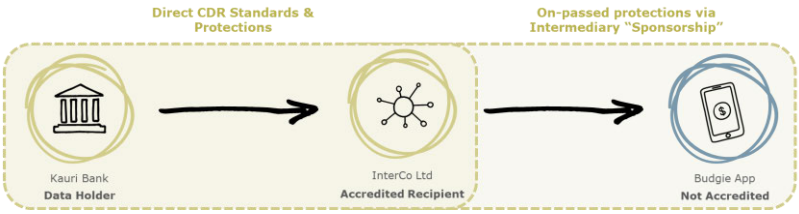
Figure 1	**Participation by two accredited parties** In this model the customer is covered by CDR standards and protections throughout their experience. Intermediaries may participate, but they will likely be fully accredited themselves, and compliant with CDR standards around consent and usage. In this model, the data holder or accredited third party may use an intermediary service as a hidden outsourced provider. If customers are still operating under the terms and conditions of the data holder or accredited third party respectively then we would not expect these to be disclosed, See 6.10 - 6.12. 
Figure 2	**Participation by accredited third party via accredited intermediary.** In this model the customer is covered by CDR standards and protections throughout their experience. The intermediary adds complexity to the customers journey and requires the customer to agree to their terms and conditions. See 6.4.2. 
Figure 3	**Intermediary on-sharing outside of CDR ecosystem** The draft bill contains no controls on accredited recipients on-sharing data or actions with non-accredited parties. This means an intermediary will be able to easily move data and actions outside of the CDR regime and its protections. Some of this on-sharing would fall under the Privacy Act. However, the Privacy Act does not provide protections for businesses or for controlling action initiation rights. See section 6. 
Figure 4	**Intermediary re-using previously shared data or action rights.** The draft bill also contains no controls on Intermediaries re-using data or action rights that have previously been shared with them. This effectively means multiple non-accredited parties can utilise a single underlying CDR compliant connection. 
Figure 5	**Customer Example – The effect on on-sharing and re-use of customer data.** Given the ability for accredited recipient intermediaries to on-share and re-use connections, and the strong incentive for data requestors to use intermediaries, it is very likely that most customer sharing relationships will occur outside the protections of the CDR regime. In this example, a customer with one banking relationship is using 10 CDR powered services that are connected by two intermediaries. This means that of the 12 sharing relationships using their data, only 2 of them are clearly protected by the CDR. Our customer research has clearly indicated that customer expect to be able to manage sharing connections from the original data holder/source. However, in this example the customer would potentially not be able to view or manage their sharing connections for the 10 ultimate services consuming their data from their bank – they would only see two broad sharing relationships with intermediaries. 

Figure 6	**Customer Example 2 – re-use generating disclosure and consent issues.** In this example, a business shares their data with a CDR powered payroll service, via an intermediary. The initial consent is approved by both Directors, in line with the "two to sign" account operating instructions they instructed their bank to use (Step 1). Later, an employee of the business signs up to a new CDR powered sales dashboard service, that uses the same Intermediary (Step 2). The Intermediary already has access to the data from the first consent, so re-uses this data and on-shares to the new service. Given the Intermediary is unaware of the underlying account ownership structure and operating agreement, this data is re-used and on-shared without the either Directors' knowledge or "two to sign" consent. Our research with business customers has clearly indicated their sensitivity regarding disclosure of their business data. They have a very strong desire to have clear, consistent, and effective controls regarding its disclosure and use. Situations where their controls are circumvented will not be tolerated. 
Figure 7	**Example of CDR rules and standards 'customer protections' passed on (as applicable) by the Intermediary** 

Appendix 2 – Participation requirements by accreditation or via an intermediary

	via Accreditation 	via Intermediary (With no obligations on-passed e.g. Privacy Act only) 
Accreditation requirement	Required	Not Required
Who can participate	Set by accreditation rules	Intermediaries set the rules
Insurance requirement	Required	Only if intermediary requires
Data and actions accessible	"Raw" and as per standards only	As processed and potentially value add services such as enriched by intermediary
Compliance costs	Must comply with CDR standards and accreditation conditions	Low – only as required by intermediary
Customer experience flexibility	Low – must comply with CDR disclosure & consent standards	High – Privacy Act significantly more flexible around disclosure & consent
Technical complexity	High – multiple connection to each data holders	Low – single connection to Intermediary
Disputes and liability exposure	High – must support CDR disputes system, with higher penalties	Low – exposed to Privacy Act dispute systems and penalties only
Additional services and support	None – only as per standards	Extensive – intermediaries frequently add additional services and support
For Third Parties	**Less attractive -** Higher obligations and costs.	**More attractive -** Lower obligations and costs, higher value.
For Customers	**More customers protections**	**Less customer protections**

Appendix 3 – Responses to questions in the discussion document

How will the draft law interact with protections under the Privacy Act?

1	**Does the proposed approach for the interaction between the draft law and the Privacy Act achieve our objective of relying on Privacy Act protections where possible? Have we disapplied the right parts of the Privacy Act?**

Please refer to section 5, Customer protections must go above and beyond the Privacy Act.

In our view, the current Privacy Act and its IPPs do not provide full coverage in the CDR context, and adaptations and modifications are required to address this. Please see paragraphs 4.2.1 and 5.1 to 5.6 of our submission for more detail, with additional points outlined below:

1) **Designated customer data vs personal information scope**

Under the draft bill, we note the following:

- "customer data" is defined as data about an identifiable customer that is held by or on behalf of a data holder (including, for example personal information within the meaning of the Privacy Act and s8(2) of the draft bill).
- a "data holder" is required to provide customers with "designated customer data" (ss14 and 15). The type of data that is "designated customer data" will be defined in the subsequent regulations, which are yet to be drafted. For the purpose of this questionnaire, we are assuming that New Zealand will follow the Australian CDR approach, which defines "CDR data" for the banking sector as:
    - information about the consumer or their associate (for example, contact details)
    - information about the use of a product by a consumer or their associate (for example, transaction data)
    - information about a product, for example, terms and conditions.
- To ensure that customer data requests under the draft bill are able to be responded to and processed efficiently and in the minimum time possible - which will be necessary to give effect to the benefits the bill intends to support - the scope of "designated customer data" will need to be very clearly defined in any subsequent regulations, including whether specific types of "customer data" are within scope in the banking context (such as court proceedings, personal insolvency information, credit reports). The definition of "personal information" in the Privacy Act is deliberately broad, so as to give maximum effect to an individual's privacy rights, but the flip side of this broad definition is that it can often be a difficult and at times lengthy process to determine whether specific data is or is not personal information about an identifiable individual. Ensuring that the definition of "designated customer data" is clearly delineated and specific will ensure that requests for such data are able to be processed swiftly by the data holder.
- In particular, it will be important to resolve whether bank customer numbers and IRD numbers, for example, are considered part of this "customer data", noting that they are "unique identifiers" under the Privacy Act but excluded under the Australian CDR regime.

2) **Proposed Intersect of the Privacy Act and the draft bill**

We highlight some of what we see as potential tensions across the related IPPs as a start.

- IPP1: Purpose of collection of personal information

From a privacy perspective, one of the main differences in approach between the Privacy Act and the draft bill is that under the Privacy Act, when assessing whether an agency has the right to collect personal information, the Privacy Act relies on there being a lawful "purpose" that is connected to an agency's functions and activities. In most circumstances under the Act, agencies have clear functions and activities.

For example, banks collect personal information to provide banking products and services and to meet regulatory requirements.

On the other hand, the draft bill aims to enable customer data sharing capabilities in a controlled and secured environment, with "customer authorisation" being the foundation of the ecosystem. The Discussion Document provides that the draft bill relies on existing Act protection; however, there are considerable differences between "purpose" and "authorisation". "Purpose" can be difficult to define when a party in the CDR ecosystem acts as a conduit, such as an API provider. Therefore, existing protection offered under the Act may be insufficient for the purposes of CDR.

Further, IPP1 also prohibits the collection of identifying information where this is not necessary, providing customers with a right to be pseudonymous/anonymous in their interactions in such circumstances, and therefore in respect of what data is collected about them. We note the Australian CDR requires covered entities to invest in functionality that facilitates this right, and suggest this should also be a considered as an option under the NZ CDR regime in order to allow agencies to comply with their IPP1 obligations.

- IPP2: Source of personal information:

  This IPP is centred around collection from the individual. While IPP2(2)(c) does allow "authorisation" as a basis for collecting from a third party this "authorisation" is on based on the collecting entity having "reasonable grounds" that such authorisation exists. Under the draft bill, authorisation has a specific meaning (s30) and any collection of personal information about a customer by an accredited requester must meet that standard for this to be a lawful collection, rather than the less specific requirement under IPP2(2)(c) i.e., s30 of the draft bill acts as a statutory override of the Privacy Act.

- IPP3: Collection of information from subject:

  There is no "authorisation" requirement under IPP3. IPP3 currently stipulates that individuals need to be made "aware" of certain information, including the fact that information is being collected, the purpose of the collection, the intended recipients, the name and address of the agency that is collecting and holding the information, and their rights of access and correction.

  The draft bill, however, currently requires "authorisation" (for example by a customer to an accredited requester) to be given "expressly" and customers have to be "reasonably informed" about the matter to which the "authorisation" relates to (s30). The draft bill does not specify what is meant by "reasonably informed". While we note that regulations and standards may prescribe "certain steps" to "facilitate" a customer being "reasonably informed", we consider that if the current IPP3 is to be relied upon here, then "data holders", "accredited requestors" and "secondary

users" should provide customers (via their website or app) with the information listed in IPP3(1) as a bare minimum.

However, in our view, IPP3(1) as currently drafted is arguably insufficient for CDR purposes in terms of setting out the elements required to ensure a customer is "reasonably informed". In our view, the draft bill, or through regulations and standards, should make it clear that for "authorisation" to occur the customer should be made aware of exactly what data is being shared, how it will be used, who will have access to it, how long they will have access to the data for and how they can manage and withdraw "authorisations". Customers should also be provided with more information when their data is collected.

For example, if a customer wants to sign up to a budgeting app to share their banking transactions and the app is only required to make customers "aware" of certain information under current IPP3(1) privacy requirements, the customer will only be made "aware" of:

- Banking transactions being collected;
- It is for the purpose of providing budgeting information;
- Who might the personal information be disclosed to;
- The app's company information.

For the purpose of CDR, the customer should ideally be informed of additional information, via the relevant privacy policy or app, such as (but not limited to):

- How long their "authorisation" will last;
- How they can amend or end the "authorisation";
- What happens to the data that has already been shared prior to ending the authorisation;
- How they will be informed if data is on shared to other parties, and how the customer can stop any such sharing.

It is also necessary to note that other subsections of IPP3 should arguably not be applied to the draft bill (i.e. similar to how s46 of the draft bill excludes Privacy Act provisions). This is to ensure that agencies are accountable in being transparent in the way the draft bill expects. For example, IPP3(4) provides exceptions for when agencies do not have to provide information to the individual. The aim of the draft bill is to allow customers to understand with whom they are sharing their data with and for what purpose, and to then provide express authorisation for that sharing. If agencies relied on IPP3(4) and did not inform an individual appropriately, customers will not be able to make a "reasonably informed" decision.

Similarly, IPP3(2) allows notification after collection where this is not reasonably practicable to do before collection, but we consider that in the context of the collections under the draft bill this information should always be provided prior to collection.

We also note that this consultation on the draft bill is being conducted before a firm decision on amending IPP3 in respect of indirect notification is made by the Ministry of Justice, which has itself been the subject of public consultation.

- <u>IPP5: Storage and security of personal information:</u>

For CDR context, we believe it important to call out expressly CDR specific privacy-related safeguards that exist under the Australian regime, which could also usefully apply here, such as options to not identify yourself as individuals or allow the use of pseudonyms and destroying unsolicited information specifically.

- IPP6: access to personal information:

  The draft bill generally intends that requests under the draft bill for personal information (i.e. requests from an identifiable individual for information about them) should be treated as requests under IPP6 of the Act, though it excludes many of the procedural provisions contained in Part 4 of the Privacy Act. In this regard, the draft bill specifies if a data request made under ss14 and 15 relates to personal information they are to be treated as IPP6 requests (s45), with specific Privacy Act provisions excluded (s46

  Quite apart from the fact that requests from companies will not benefit from existing Privacy Act provisions, the way the various Privacy Act provisions have been applied or excluded in the draft bill will need careful thought to ensure it is workable. For example, the draft bil does not exclude the application of the withholding grounds contained in ss 49-53 of the Act. This makes sense in that the draft bill should not be a way to subvert the ability of an agency to lawfully refuse access to personal information, but could complicate and slow down what is intended to be an automated and relatively swift process.

  It will also be important to ensure customers are not confused in their rights, for example, if they have an expectation of the request being treated urgently under the Privacy Act but the request is treated as a CDR request, this may increase unnecessary complaints.

- IPP7: correction of personal information

  For CDR purposes, IPP7 will apply to customer data requests as it would to any other correction request relating to personal information. It will need to be responded to in accordance with the procedure set out in the Privacy Act and steps taken to correct or add a qualifying statement to the data to ensure it is not misinterpreted.

  Corrected data must be provided to all prior recipients of it, including presumably any recipients who received it under the draft bill such as accredited requesters. This potentially raises issues in respect of the customer's authorisation to that accredited requester to process their personal information, including retaining it. A data holder needing to provide previous recipients with corrected personal information will not necessarily know whether that previous recipient is still "authorised" by the customer to process their information, or even whether the previous recipient still holds it.

- IPP8: accuracy of personal information to be checked before use or disclosure

  Ensuring accurate data is shared will be key to the CDR regime's success. However, if data holders are going to be asked to provide straight through electronic access to customer data, then that must be how customer data is currently held in our systems at a point in time – data holders won't be looking at verifying any data provided, it will be as posted.

- IPP9: agency not to keep personal information for longer than necessary

For CDR purposes, it should be expressly stated:

- Any customer data that is no longer needed for "scope of authorisation" must be deleted or permanently de-identified, unless agreed exceptions apply.
- Any customer data received without "authorisation" must be destroyed, unless a law or court order requires it to be retained.

- IPP13: unique identifiers

  In keeping with the Australian CDR, we would recommend that designated regulations should prohibit the adoption, use and disclosure of certain unique identifiers, such as government identifiers, by data recipients unless required or authorised under law, court order or privacy regulation. Noting IPP13 would still apply, however, whereby an accredited requester can use an identifier, such as an IRD number if their use is sufficiently linked to the purpose it was assigned e.g. to manage tax obligations.

3) Proposed exclusions of the Privacy Act

Section 46 of the Privacy Act allows agencies to make a decision to refuse access to personal information, and ss 49-54 provide reasons for doing so. These provisions of the Privacy Act are not excluded pursuant to s46 of the draft bill, and so presumably prevail.

On this basis a "data holder" can refuse access to personal information under s46 of the Privacy Act, even if the request was made under ss14 and 15 of the draft bill. However, the current wording of ss14 and 15 provides that the "data holder" "must" provide data to the customer or the "accredited requestor", with s47 of the draft bill setting out that a breach of section 24 para 15 is a breach of IPP6.

Further the commentary in the discussion document (at paragraphs 166/167) indicates that the intention is that the draft bill does not anticipate that a data holder can refuse a request made under ss14/15 of the draft bill.

It is not sufficiently clear how these provisions are intended to interact in circumstances where a "data holder" has a proper basis under one of the Privacy Act withholding grounds to refuse an IPP6 request. One interpretation (and seemingly the one intended by the Bill) is that pursuant to s24 of the Privacy Act, ss14/15 of the draft bill will override the Privacy Act, essentially meaning that a "data holder" cannot refuse such a request. If this is intended, then we would suggest clarifying this by adding the relevant ss46-54 to the list of non-applicable Privacy Act provisions in s46 of the draft bill.

However, we consider that removing the ability of a "data holder" to refuse a request made under the draft bill on the basis of the Privacy Act withholding grounds may have a negative effect, resulting in the disclosure of personal information that could be withheld for good reason if the request had been made outside of the CDR regime.

For example, currently banks rely on section 55 of the Privacy Act to exclude personal information relating to where it would be likely to prejudice the maintenance of the law by any public sector agency. Although it remains to be seen what will constitute "designated customer data", it is important for this right to be retained. We address this issue further in our responses to questions 23 and 24.

Section 57(a) provides that an agency may only give access to the personal information if the agency is satisfied of the identity of the requestor. The draft bill requires the identity of the customer and the "accredited requestor" to be

authenticated prior to the release of customer data (s37). **Notifiable privacy breaches**

We also remain concerned with how notifiable privacy breaches will be treated. There could be a situation where a customer's data is provided to an "accredited requestor" and there is a notifiable privacy breach in respect of personal information, but the data involved additionally involves non-personal information.

Since the personal information will belong to a person who is a customer of both the bank and the "accredited requestor" and potentially any accredited requestor's outsourced provider, who will be required to notify the privacy breach? As we understand it, the agency holding the personal information is responsible for the privacy breach, so if an accredited requester has a privacy breach, it will be responsible for managing it and the required notifications. The data holder would have no liability/responsibility and there would be no obligation on the accredited requester to advise the data holder of such a privacy breach. However, ideally, this should all be made clear.

The outcome if there is also non-personal information will additionally need to be considered. Will the data holder be required to notify MBIE and the Privacy Commissioner and work with the accredited requestor if the breach has been caused by the accredited requestor? The greater the personal information is proliferated and transferred the greater the risk of a notifiable privacy breach occurring if the information involved is personal information.

4) **Approach to certain contraventions of the draft bill**

We also note that in the draft Bill, at ss47 and 48, it is noted that if a "data holder" breaches ss14 or 15 or the CPD storage and security requirements, this will be treated as a breach of an IPP, however, consideration is being given to whether this will instead be treated as an interference with privacy under s69 of the Privacy Act. It's not very clear what exactly this would mean but presumably this would mean there was no requirement for any such contravention to have caused harm (re an IPP5 breach at least, as there is already no requirement for harm in regard to IPP6 breaches). In our view, the IPP5 breaches would be unreasonable as it essentially requires the "data holder" to have bullet proof information security, a higher standard than the Privacy Act's "reasonable security safeguards" threshold.

In summary, we consider that the application of the Privacy Act should be captured at a framework level in the draft bill, with the CDR context and additional detail to be provided via the ensuing regulations and standards. Our view is that consideration needs to be given to the adoption of a CDR specific Privacy Code of Practice under the Privacy Act, which captures CDR specific privacy and data ethics safeguards. In this way, this will assist all stakeholders and the wider public easy access and understanding of how these privacy and data safeguards apply.

Consent settings: respecting and protecting customers' authority over their data	
2	**Should there be a maximum duration for customer consent? What conditions should apply?**
	Please refer to section 7, The bill must be designed to provide flexibility for collaborative iteration and risk based rules.
3	**What settings for managing ongoing consent best align with data governance tikanga?**
	Section #43 of the discussion document refers to the Māori Data Governance Model developed by Te Kahui Raraunga, published in May 2023. This report helps with setting the context of expectation in relation to Māori data governance. We believe it is important to highlight the need to understand the importance of Māori data and we welcome MBIE's

	clear desire to get this right for the CDR. However, there needs to be more work done from an ANZ perspective to understand what Māori data means in a private financial context vs the govt social context. We would welcome the opportunity to be involved in future consultation and discussions as we work towards getting this right for ANZ, in line with our Tākiri-ā-Rangi Te Ao Māori Strategy. https://www.anz.co.nz/about-us/corporate-responsibility/maori-strategy/
4	**Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?**
	Please refer to section 7, The bill must be designed to provide flexibility for collaborative iteration and risk based rules.
5	**How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?**
	Please refer to question 3.
6	**What are your views on the proposed obligations on data holders and accredited requestors in relation to consent, control, and accountability? Should any of them be changed? Is there anything missing?**
	Please refer to section 5, Customer protections must go above and beyond the Privacy Act.
Care during exchange: standards	
7	**Do you think the procedural requirements for making standards are appropriate? What else should be considered?**
	Please refer to section 7, The legislation must be designed to provide flexibility for collaborative iteration and risk based rules.
8	**Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?**
	Please refer to section 5, Customer protections must go above and beyond the Privacy Act. Additionally: • The draft bill does not seek to change the IPP legal settings around storage and security requirements. However, this raises concerns about increased privacy risks as the draft bill will enable large amounts of personal information to be shared between different entities. • Our understanding is that the draft bill intends to allow various processes, powers and remedies under Part 5 and 6 of the Privacy Act to be triggered if there are any contraventions of storage and security requirements prescribed by the draft bill, if the contraventions are in relation to personal information. • Section 43(1)(a) of the draft bill provides that data holders and accredited requestors must have a process that allows customers to make complaints. It is unclear how this interacts with s72(1) of the Privacy Act, where complaints must be made to the OPC orally or in writing. Further clarity is required on how customers should make a complaint. We assume data holders or accredited requestors will be required to have an internal complaints process that the customer can follow in the first instance and are required to make clear to the customer the escalation process to the correct regulatory body should the customer be unsatisfied with the outcome of the internal complaints process. o Are customers expected to follow the data holder's complaints process for all non-personal information customer data and make a separate complaint to the OPC in relation to personal information? Noting the

	customer may have made the complaint with the data holder in the first instance and did not receive a satisfactory response. o How should complaints be treated if it involves both personal and non-personal information? • Section(1)(b) of the draft bill provides that data holders and accredited requestors must have a process that provides how complaints must be investigated. It is unclear how this interacts with s74, where the OPC has the power to decide not to investigate. And Part 5 – Subpart 2 of the Privacy Act, which sets out how the OPC may conduct investigations. Further clarity is required on how data holders and accredited requestors should conduct investigations under s43(1)(b) of the draft bill. o If the customer has made a personal information- related complaint and the OPC has made a decision not to investigate a complaint under s74 of the Privacy Act, are data holders and accredited requestors still require to conduct an investigation as outlined in their complaints process under s43(1)(b)? • Please refer to response to Question 1 around the lack of clarity on how notifiable breaches will be managed and with whom the obligation lies.
9	**From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards1 are suitable for use in other sectors, and which could require significant modification?**
	ANZ has not had sufficient time to form a response to this question.
10	**What risks or issues should the government be aware of, when starting with banking for standard setting? For example, could the high security standards of banking API's create barriers to entry?**
	Please refer to section 5 (5.7), Customer protections must go above and beyond the Privacy Act. Please refer to section 6 (6.4), It should not be possible for third parties to avoid all CDR obligations by participating via an intermediary.
Trust: accreditation of requestors	
11	**Should there be a class of accreditation for intermediaries? If so, what conditions should apply?**
	Yes, please refer to section 6, It should not be possible for third parties to avoid all CDR obligations by participating via an intermediary.
12	**Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?**
	Yes, with the level of insurance should be dependent on level of risk exposure. Please refer to section 7. The bill must be designed to provide flexibility for collaborative iteration and risk based rules.
13	**What accreditation criteria are most important to support the participation of Māori in the regime?**

[1] New Zealand API standards to initiate payments and access bank account information. They are based on the UK's Open Banking Implementation Entity standards but tailored for the New Zealand market. Market demand has driven development and led to the creation of bespoke functionality for New Zealand.

	Please refer to question 3.
14	**Do you have any other feedback on accreditation or other requirements on accredited requestors?**
	Yes, please refer to: • Section 5, Customer protections must go above and beyond the Privacy Act. • Section 6, It should not be possible for third parties to avoid all CDR obligations by participating via an intermediary.
Unlocking value for all	
15	**Please provide feedback on:** • ***the potential relationships between the Bill safeguards and tikanga, and Te Tiriti/the Treaty*** • **the types of use-cases for customer data or action initiation which are of particular interest to iwi/Māori** • **any specific aspirations for use and handling of customer and product data within iwi/hapū/Māori organisations, Te Whata etc, which could benefit from the draft law.**
	ANZ has not had sufficient time to form a response to this question.
16	**What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?**
	ANZ has not had sufficient time to form a response to this question.
17	**What settings in the draft law or regulations should be included to support accessibility and inclusion?**
	ANZ has not had sufficient time to form a response to this question.
18	**In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?**
	ANZ has not had sufficient time to form a response to this question.
Ethical use of data and action initiation	
19	**What are your views on the proposed options for ethical requirements for accreditation? Do you agree about requirements to get express consent for de-identification of designated customer data?**

	• Although our overarching view is that this level of detail should not be in the draft bill, our preferred option is to impose additional ethical requirements for accreditation (Option 1). Our preference is for these ethical requirements for accreditation to be dealt with as data ethics and disclosure/consenting standards, as per s87 of the draft bill.
	• We agree with the additional accreditation criteria set out in the discussion document:
	  ○ Fit and proper person test: Suggest we follow a similar approach as Rule 1.9 of the Australian CDR, where the fit and proper test is specific to CPD;
	  ○ Demonstrated information protection and security measures – suggest as part of the renewal of accreditation process (s 71), accredited requestors are required to demonstrate their security capabilities again;
	  ○ Evidence of appropriate insurance.
	• Imposing additional ethical requirements will increase customer trust in the CPD ecosystem, because the regulators have done additional screening in their

approval process. Customers will also benefit from additional protection of their data.

- In our view, obtaining express authorisation from customers for de-identification and using customer data for research or statistical purposes will increase confusion and operational complexity. This is bearing in mind the fast-paced nature and volume envisaged of the data sharing requests in the banking context. It will also add compliance burden to what are already complex data sharing processes.
- Prior to collecting the customer's data, as part of their privacy policy or via their app, accredited requestors should, in any event, provide sufficient information to the customer, to inform them that their data will be de-identified or used in research or for statistical purposes. The authorisation provided by the customer at the beginning of the journey, should include all uses of their data, including where that data is deidentified/used for research purposes. In our view, there is no need for this to be done again, which would only add in further complexity to the process envisaged.
- De-identification of data should be recommended as part of a CDR privacy specific safeguard requirement, where accredited requestors are required to de-identify designated customer data when it is no longer within the scope of the authorisation. The extent and/or process(es) of de-identification could be included in standards to ensure consistency across the ecosystem.

20	**Are there other ways that ethical use of data and action initiation could be guided or required?**

As mentioned above, in our view, consideration should be given by MBIE to the issue of a CDR specific privacy- and data ethics-related Code of Practice. This would call out the following:

- Fairness
- Transparency – the authorisation concept, where customers have to make reasonably informed and expressed authorisation. It is paramount that the customer is aware of the exact scope of their authorisation.
- Accountability – the accountability and responsibility that each party (data holder or accredited requestor) owe to the customer when they collect, use or share their data.

Preliminary provisions

21	**What is your feedback on the purpose statement?**

ANZ has not had sufficient time to form a response to this question.

22	**Do you agree with the territorial application? If not, what would you change and why?**

ANZ has not had sufficient time to form a response to this question.

Regulated data services

23	**Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?**

- Sections 14 and 15 of the draft bill provides that data holders "must" provide customer data to customers and accredited requestors, if the request is a valid request made by the customer (s14) or if the request is made by an accredited requestor and the customer authorised it and it is a valid request (s15).
- Section 25 of the draft bill defines "valid request", however, only focuses on the method of how the request is made but not the legitimacy of the request.
- Under s24 of the Privacy Act, nothing in IPP6, 11 or 12 limits or affects a provision contained in any New Zealand enactment that authorises or requires personal

information to be made available. Is the draft bill's intention to supersede the Privacy Act, where data holders must disclose personal information even if access could have been refused under the Privacy Act?

- Sections 49-53 of the Privacy Act provides specific reasons that agencies can rely on to refuse access to personal information. These reasons are largely concerned with the safety and protection of the individual, and, in our view, should be upheld when considering whether a data holder can deny a valid request.
- There are many valid reasons why data holders should be allowed to deny data requests, such as:
    - Fraudulent requests, e.g. phishing or scams;
    - Cyber attacks;
    - Coerced requests.
    - Account status – e.g. suspended.
    - Frequency of requests – In the UK there are agreed limits as to number of times a 3rd party can request data for a customer within a 24 hour period.
- The draft bill should not be used as another channel to allow access to personal information which could lawfully be refused under the Privacy Act.

24	**How do automated data services currently address considerations for refusing access to data, such as on grounds in sections 49 and 57(b) of the Privacy Act?**

- Under the current s49 and s57(b) of the Privacy Act, agencies could refuse access to personal information, if the criteria provided are met. For example, certain criteria require subjective assessments, such as where banks look to rely on these withholding grounds: "likely to pose serious threat to life, health or safety of any individual" (s 49(1)(a)(i)), and "must not give access to personal information if the agency has reasonable grounds to believe that the request is made under the threat of physical or mental harm" (s 57(b).
- When subjective assessments are required to be made, it will be difficult to implement a truly automated data service; a level of human intervention will always be required to determine the likelihood of the threat.

A truly automated data service for providing access to personal information will likely have been configured to only include information or scenarios that would not need a withholding ground. For example, Meta have an automated access request functionality whereby one of the sets of information an individual receives are photos that they themselves uploaded. It is unlikely a withholding ground would exist in this instance. Similarly, if there were to be an automated system for downloading transaction information on a joint account, this is on the basis that both parties are likely to be aware of the information and that a withholding ground would not apply. It may be hard for agencies to prove a request was made under a threat of physical or mental harm and would require each request to be manually reviewed, increasing headcount and inefficiencies.

Protections

25	**Are the proposed record keeping requirements in the draft law well targeted to enabling monitoring and enforcement? Are there more efficient or effective record keeping requirements to this end?**
	ANZ has not had sufficient time to form a response to this question.
26	**What are your views on the potential data policy requirements? Is there anything you would add or remove?**
	In line with recommendations made in 5.9. The data policy must be an integrated part of the customers' disclosure and consenting experience.

	The requirement to list outsourced providers should be removed, see 6.10 - 6.12.
Regulatory and enforcement matters	
27	**Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?**
	ANZ has not had sufficient time to form a response to this question.
Administrative matters	
28	**Are the matters listed in clause 60 of the draft law the right balance of matters for the Minister to consider before recommending designation?**
	ANZ has not had sufficient time to form a response to this question.
29	**What is your feedback on the proposed approach to meeting Te Tiriti o Waitangi/Treaty of Waitangi obligations in relation to decision-making by Ministers and officials?**
	Please refer to question 3.
30	**What should the closed register for data holders and accredited requestors contain to be of most use to participants?**
	ANZ has not had sufficient time to form a response to this question.
31	**Which additional information in the closed register should be machine-readable?**
	ANZ has not had sufficient time to form a response to this question.
32	**Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?**
	ANZ has not had sufficient time to form a response to this question.
33	**Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?**
	ANZ has not had sufficient time to form a response to this question.
34	**What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?**
	ANZ has not had sufficient time to form a response to this question.
Complaints and disputes	
35	**In cases where a data holder or requestor is not already required to be member of a dispute resolution scheme, do you agree that disputes between customers and data holders and/or accredited requestors should be dealt with through existing industry dispute resolution schemes, with the Disputes Tribunal as a backstop? Why or why not?**
	ANZ has not had sufficient time to form a response to this question.

References

[i] Boston Consultancy Group, *Building Trust in Business Ecosystems*, February 2021, https://www.bcg.com/publications/2021/building-trust-in-business-ecosystems.

[ii] Boston Consultancy Group, *How Do You Manage a Business Ecosystem*, January 2021, https://www.bcg.com/publications/2021/how-to-manage-business-ecosystem.

[iii] The Office of the Australian Information Commissioner, Consumer Data Right Privacy Safeguard Guidelines, November 2022, https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/consumer-data-right-privacy-safeguard-guidelines.

[iv] Open Banking Limited (OBL), *New Impact Report sees significant growth in open banking payments and increased business use Open Banking Impact Report*, March 2023, https://www.openbanking.org.uk/news/new-impact-report-sees-significant-growth-in-open-banking-payments-and-increased-business-use/.

[v] Digital Identity New Zealand. *Digital Identity in Aotearoa,* 2023, P15-16, https://digitalidentity.nz/wp-content/uploads/sites/25/2023/02/Digital-Identity-in-Aotearoa-Report_final-1.pdf.

[vi] InternetNZ, *New Zealand's Internet Insights 2022*, December 2022, https://internetnz.nz/assets/Uploads/Internet-insights-2022.pdf.

[vii] Australian Prudential Regulation Authority (APRA) (July 2019), *Prudential Standard CPS 234 Information Security,* https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf.

[viii] The Office of the Australian Information Commissioner, *Sponsored accreditation model: privacy obligations of an affiliate*, December 2021, https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/privacy-obligations/sponsored-accreditation-model-privacy-obligations-of-an-affiliate