New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Ministry of Business, Innovation and Employment

on the

Consultation: Unlocking value from our customer data right

24 July 2023

NEW ZEALAND BANKING ASSOCIATION – TE RANGAPŪ PĒKE
PO Box 3043, Wellington 6140, New Zealand
www.nzba.org.nz

About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following eighteen registered banks in New Zealand are members of NZBA:
   - ANZ Bank New Zealand Limited
   - ASB Bank Limited
   - Bank of China (NZ) Limited
   - Bank of New Zealand
   - China Construction Bank
   - Citibank N.A.
   - The Co-operative Bank Limited
   - Heartland Bank Limited
   - The Hongkong and Shanghai Banking Corporation Limited
   - Industrial and Commercial Bank of China (New Zealand) Limited
   - JPMorgan Chase Bank N.A.
   - KB Kookmin Bank Auckland Branch
   - Kiwibank Limited
   - MUFG Bank Ltd
   - Rabobank New Zealand Limited
   - SBS Bank
   - TSB Bank Limited
   - Westpac New Zealand Limited

Introduction

NZBA welcomes the opportunity to provide feedback to the Ministry of Business, Innovation and Employment (**MBIE**) on its discussion document "Unlocking value from our customer data" (**Discussion Document**) and exposure draft of the Customer and Product Data Bill (**Bill**). NZBA commends the work that has gone into developing these documents.

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
Privacy of natural persons

Sam Schuyt
Associate Director, Policy & Legal Counsel
Privacy of natural persons

Need for ongoing consultation and overview of submission

4. We thank MBIE for its open engagement on the creation of a customer data right (often known as a 'consumer data right') (**CDR**) and on the draft text of the Bill.

5. A successful, well-used and secure CDR will require careful design, with ongoing input from data holders, potential accredited requestors and customers throughout the drafting stage and into implementation.

6. A short four-week consultation has been provided for the Bill, and our request for an extension of this period has not been granted. Noting that we believe further consultation will ultimately be necessary given the long-term direction of the CDR, we have focused this industry submission on key matters relating to banks as data holders and matters that we believe are critical to the success of the CDR.[1] Such matters are by nature expansive in scope and our ability to examine the issues and their consequences has been limited by the time available. **We strongly submit that MBIE should continue to work with interested industry groups and other parties over the coming months and ensure that sufficient time is available to work through these complex matters before a Bill is introduced**.

7. CDRs are being developed in a number of jurisdictions around the world, with a mixture of both regulatory and industry-led designs (including New Zealand's industry-led API Centre initiatives, which are well-advanced). It is clear from international and domestic experience that, to be successful, a CDR must be:

   (a) designed for **certainty**, **efficiency**, **ease of use**, and – above all – **security**. CDRs must allow for standardised, robust and efficient deployment, while also providing customers with utmost confidence to use the system;

   (b) developed in close consultation with relevant industry and interested parties; and

   (c) respectful of customer data and its value to customers, to foster the trust and confidence of customers in using the CDR. A CDR should not require more data to be shared than is necessary to provide the product or service (and use of such data should be restricted to only that purpose).

8. This is a complex area with a material risk of unintended consequences (including relating to security) if it is not well tested and considered before it is put into practice. The effectiveness of a CDR relies on customers voluntarily deciding to use it, so any such unintended consequences or unaddressed concerns when a CDR is first implemented could slow down its uptake by years, or even permanently.

9. Before the Bill is tabled in Parliament late this year, we strongly encourage MBIE to continue working with the banking industry and other interested parties to:

---

[1] Individual submissions by member banks may cover points specific to accredited requestors, as well as member-specific matters and impacts. We support MBIE's close consideration of the usage of Māori data but, given the focus of this submission, do not generally comment on it here (except as specifically noted).

(a) **further develop the draft Bill** (including refining key sections and addressing aspects covered by brief placeholders in the current draft), including its scope, regulator guardrails and settings; and

(b) **advance fit-for-purpose regulations and standards, including scope of initial designations for the banking industry**. This will help test how the framework in the Bill can be put into practice and identify potential drafting issues. It is also extremely important that the banking industry (along with potential accredited requestors and customers) are given the time, information and opportunity necessary to build systems for compliance with the new rules, to consider such scope and appropriately implement it before any set deadline. NZBA also suggests that prioritisation should be given to workstreams already underway, such as the API Centre's development of technical standards for the exchange of payments and transaction information.

10. We welcome further industry workshops in particular as an effective mechanism to share feedback on the implementation practicalities of the reforms.

11. As has been the case for other recent financial regulation consultations (in particular the Deposit Takers Act), such an ongoing engagement process is particularly relevant given MBIE's role as both regulator and drafter of the Bill – particularly active engagement is appropriate to ensure that relevant safeguards, checks and balances are maintained throughout.

12. In the remainder of our submission we consider the following matters:

(a) **Part 1: Scope of the CDR and the Bill – boundaries and need for guidance on regulation-setting in the legislation**.

(b) **Part 2: Interaction with other legislation, MBIE as regulator and determination of liability**.

(c) **Part 3: Appropriate consent settings for the CDR in the Bill**.

(d) **Part 4: Miscellaneous matters – Customer Data Policy, Outsourced Providers, Government fees and Levies**.

Part 1: Scope of the CDR and the Bill – boundaries and need for guidance on regulation-setting in the legislation

13. We appreciate that the Bill is designed as a framework for use in a range of sectors beyond banking, and that to achieve this the Bill must leave certain aspects to be set by future regulation, standards and designations.

14. However, given the requirements for a successful CDR as discussed above, NZBA submits that the Bill needs to provide more certainty in respect of the potential scope of the obligations that may be placed on data holders. This includes setting:

(a) **appropriate and clearly defined boundaries** for what is or may be included and excluded from a CDR, including types of data and data access; and

(b) for matters left to regulation, standards and designations, **appropriate and clearly defined guidance** on what is to be taken into account (as discussed further below),

to ensure consistent and appropriate application across relevant sectors, and to provide a roadmap for data holders and accredited requestors to use when allocating resource to develop systems and innovate. In particular, such an approach would allow banks to undertake early work to facilitate the efficient delivery of this project and to avoid the need to revisit or re-scope work (including work to implement the existing API Centre standards) that may have progressed in the absence of indications that further regulations or standards may impact those workstreams.

15. A priority matter (as discussed in Part 3 further below) will be clear requirements in respect of the expiry of customer authorisation or the occurrence of specific events which may automatically terminate customer authorisation. This is a strong example of a circumstance where early clarity will be required so that automated systems are developed with full knowledge of the prescribed circumstances in which authorisation is terminated and provision of data must cease.

16. In addition:

(a) **Electronic system access should be limited to accredited requestors**: The Bill requires data holders to design and implement an electronic system (clause 26), allowing access to accredited requestors (who will have been security tested as part of their accreditation), but also generally to any other third party, as:

(i) product data must be made available to any person (clause 21), and, under the Bill and Discussion Document, this may potentially include an extremely wide range of data; and

(ii) customer data must be made available to any "customer" (clause 14),[2] which is defined in clause 8 to include any person "seeking to acquire" goods or services from a data holder.

NZBA is concerned about any legislated requirement to provide information to, and open systems to, parties beyond accredited requestors. Any such requestors would not be subject to MBIE's accreditation process and may not have security measures in place to protect the data provided (nor be subject to legislated requirements in respect the proper use of such data). Legislated access would mean data holders are effectively prevented from refusing or managing access based on concerns with the security measures of the requestor, and would be unable to agree contractual terms to manage these risks. Such broad legislated access to electronic systems increases the risks of cyberattack and similar security concerns, and should only be required to the extent that it is necessary for the purposes of the CDR.

---

2 See further comments on this clause below.

Considering the purpose of CDR, there is no clear practical benefit to mandating wider access to data through an electronic system:

(iii) data holders would not generally be expected to hold relevant customer data about a person that had not yet acquired goods or services from the data holder (and, as discussed below, direct-to-customer data access should not be within scope of the CDR); and

(iv) providing product data to accredited requestors would be sufficient to allow those accredited requestors to analyse customer data and give effect to the CDR. Requiring that unaccredited requestors are given access to electronic systems for product data, while restricting them from obtaining customer data, would introduce cost and potential security risk without clear benefit. As discussed below, security concerns increase further if the scope of product data to be made available is not clearly limited to publicly available, non-commercially sensitive information.

If wider electronic system access is considered necessary, then the Bill should provide a tiered approach to accreditation, with persons who are seeking accreditation for more limited data access (such as product data) having lighter accreditation requirements, with appropriate security requirements still being imposed. This would provide a proportionate approach to facilitate such data access. Security risks should also be explicitly required to be taken into account when considering the scope of access to any designated data (i.e. what 'tier' of access would be appropriate for such data).

(b) **Sharing of data by accredited requestors**: NZBA strongly submits that an accredited requestor should only be permitted to share CDR data with unaccredited recipients (other than the relevant customer) in circumstances where similar data protections apply, informed customer consent is provided and the accredited requestor has taken all reasonable action to ensure the ongoing protection of such data.

This is vital to build customer trust and confidence in the CDR and to ensure its proper use and growth – without such protections, there are incentives on data recipients to remain unaccredited and access CDR data through a small number of accredited intermediaries. Under the Bill as drafted, this would mean that most CDR data is ultimately used outside the CDR ecosystem, with Privacy Act provisions only generally applying.

Relevant protections for inclusion in the Bill could, for instance, include:

(i) measures broadly similar to Information Privacy Principle 12 (but considering whether the recipient is subject to a relevant CDR regime in New Zealand or elsewhere, rather than solely considering disclosure outside New Zealand);

(ii) requiring contractual requirements to be in place for the recipient to protect such data to the same standard as would be required if they were subject to the CDR; and

(iii) requiring explicit customer consent, with a provision similar to clause 35(2), so that such data sharing may only be a condition where reasonably necessary to facilitate the relevant product.

Clear rules for liability for such sharing of data also needs to be clear, so that customers understand who is accountable where they wish to complain (see also paragraph 31 below).

(c) **Outsourced provider concept needs to be further considered and refined**: The Bill currently allows an accredited requestor to outsource any of its 'powers' under the Bill to any other person, which would appear to allow such outsourced provider to exercise the accredited requestor's power to directly access CDR data through data holders' electronic systems. While the Discussion Document states that the outsourced provider would itself need to be accredited in such circumstances,[3] this is not clear from the Bill and should be made explicit. NZBA further submits that:

(i) outsourced providers should be restricted from using CDR data other than for the purpose they have been contracted (i.e. solely for the performance of the relevant power or duty); and

(ii) more clarity is needed in relation to the treatment of 'back-end' service providers, such as data storage providers. It should be clear that such service providers are not captured as 'outsourced providers'; and

(iii) a balance needs to be struck in relation to any customer disclosure of outsourced providers. While it may be appropriate in certain circumstances to disclose that outsourced providers are being used (for instance, where the use of that provider means the provider may have access to that information beyond data storage), data holders and accredited requestors will utilise a range of basic function outsourced providers to help meet their obligations under the Bill. Requiring explicit disclosure of these providers is likely to confuse customers rather than assist.

(d) **Direct-to-customer data access and action initiation is not appropriate for CDR and increases risk**: The Bill contemplates customers[4] accessing data (clause 14) and initiating actions (clause 17) directly, as well as through accredited requestors. As drafted, it appears to be intended that data holders build such access into their electronic system

---

3 Refer paragraph 96, and the top of page 43.

4 See also our comments below about the definition of "customer".

design (clause 26(1)) when designated customer data is specified for a sector.

However, including direct-to-customer data access and action initiation as legislated requirements would significantly increase the complexity and security risks for any electronic system design, and is not well-suited to a CDR generally focused on producing machine-readable data in a standard format. Where customers simply wish to access their customer data or initiate actions, as opposed to taking such action in connection with products or services offered by an accredited requestor, they can do so through existing online and in-app banking services. NZBA believes that the aim of the CDR is best met through the provision of data securely and efficiently through APIs which are regulated through the accreditation process.

We are not aware of any other CDR regime which provides data access and action initiation directly to customers. We note that, while direct-to-customer data access was also initially included in the equivalent Australian legislation, implementation of that element has since been deferred indefinitely for further consideration and consultation of how to 'get the settings right'.[5] Australia's independent Statutory Review of the Consumer Data Right in September 2022 references the dangers of enabling direct-to-consumer data sharing, noting that few submissions received provided examples of tangible customer benefits that justified sharing data in this way, given the relevant risks. Accordingly, it recommended reconsidering the introduction of a direct-to-customer data right at a later point when the CDR has matured.[6]NZBA proposes that Aotearoa New Zealand learn from the Australian example and remove direct-to-customer data access and action initiation from the Bill. Reconsideration could possibly be given to its inclusion in future if a strong customer benefit is established which outweighs associated risks..

(e) **The Bill should provide a clear roadmap for action initiation including a bedding-in period after data access has commenced:** Clauses 17 and 18 of the Bill require data holders to carry out actions where the request meets the relevant criteria. We note that Australia's CDR did not include action initiation from its inception, with a separate Bill for its inclusion now before the Senate.[7]

NZBA strongly submits:

---

5 See the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021 and Australian Treasury announcement (30 April 2021) here.

6 See page 27.

7 In May 2023 the Senate recommended that the separate Bill be passed into law, but noted that extensive consultation and consideration, road mapping and a measured rollout would be required.

(i) that "action initiation" should be delayed until after a well-functioning and well-trusted data-sharing capability has been established; and

(ii) the scope of data sharing and action initiation (when commenced) should also be built up and tested over time, from simple scenarios to complex. In the case of open banking this would start with transaction information and one-off payments, respectively, allowing time to manage complexities relating to, for example, the interaction between account opening actions and other legislative requirements that banks are subject to (as described below).

The Bill should generally require such timing factors to be expressly considered when creating designations under the Bill (in the context of the relative sensitivity of data and potential consequences of unauthorised action), so that customer trust and confidence in the system is maintained.

In the case of open banking, such a staged approach is essential to mitigate against the increased risk posed by allowing third party accredited requestors to operate customer accounts.

(f) **Clear limits should be included on designated product data**: The Bill allows for any data "that is about, or relates to, 1 or more of the data holder's products" to become designated product data (clauses 9 and 21). This is potentially exceptionally broad, and:

(i) could require disclosure of commercially sensitive information and individualised data sets. For instance, disclosure of potential interest rates for all customers (both retail and institutional) could require disclosure of internal credit metrics and analysis. As noted above, the Bill also requires such information to be shared with any person who requests it, whether or not they are an accredited requestor (or even a customer); and

(ii) would require data holders to design their electronic systems with extreme flexibility (and therefore inefficient additional cost and development time) for potential future designations.

While flexibility will be required to allow appropriate "designated product data" to be defined for different sectors, NZBA submits that the Bill should be amended to clearly limit the scope of product data to relevant information and to exclude commercially sensitive information.

For instance, Australian legislation effectively limits product data to data about the eligibility criteria, terms and conditions, price, availability or performance of a product/service (and in the case where the data is about availability or performance, the data is already publicly available).[8]

8 Section 56BF of the Competition and Consumer Act 2010.

NZBA submits that similar and specific limits should be included in the Bill. Where the CDR allows competitors to acquire confidential or other information, data holders will be disincentivised to innovate. Additionally, derived data should be excluded from the definition of product data, as it may include bank intellectual property and could be used to identify individuals through disclosure of matters such as credit scores and material related to complaints resolution, AML and sanctions.

In addition, where anything beyond basic publicly available information is made available, it should also be made clear in the Bill that persons accessing product data should only do so where necessary to provide the product or service that the customer requires, and its use restricted to providing that specific product or service (so, specifically prohibiting its use for other data mining and data analytics purposes).

(g) **General guidance on matters to be considered and timing when making a regulation, standard or designation**: In addition to our comments above, NZBA submits that the Bill should generally include more substantive guidance on what matters should be taken into account when considering a regulation, standard or designation, and the process for doing so. This guidance should focus on relevance, as well as certainty, efficiency, ease of use, and security as discussed above. The Bill should require consideration of:

(i) **Recency of required information**. For instance, supply of transaction records should be time-limited (both on the basis that historical information is of less relevance, and for practical data availability reasons).

(ii) **Targeting of required information**: Rather than requiring "all data" relating to a customer, there should be a focus on (1) what is relevant to the proper functioning of a CDR, including in the context of customers' best interest and respect for data as discussed in paragraph 7(c);[9] and (2) what can be reasonably synthesised into a standardised form for sharing through electronic systems. For instance, in addition to relevant transaction and account information, customer data files may include records of calls and conversations with the customer. This would be potentially harmful to customers, as well as being difficult and potentially costly[10] to provide through an electronic system, and generally beyond the scope of a CDR. NZBA accordingly proposes that they are specifically excluded from the scope of the Bill. Customer data files may also include information held by a bank when providing ancillary services (such as a

9 In addition, as discussed above, the CDR should not require more data to be shared than is necessary to provide the relevant product or service (and use of such data should be restricted to only that purpose).

10 See paragraph 31(b) below.

discretionary investment management service or DIMS) or held in relation to products offered by third parties (such as KiwiSaver or insurance products).[11] Where those ancillary services are not provided by the data holder, or are provided by the data holder as part of its business which is not yet subject to the CDR, the relevant held data should be specifically ruled out of scope.

(iii) **Alignment with relevant industry-led standards**: In the context of open banking, NZBA is supportive of alignment with the API Centre standards that have been developed with considered industry feedback over a number of years. While the scope of industry-led initiatives may not always align with the scope of the CDR for a relevant sector,[12] there should be a requirement to consider such industry-led standards when developing the more detailed standards and regulations contemplated by the Bill and align with them to the maximum extent practicable.

(iv) **Proportionality of obligations**: The design of regulations, standards and designations for each sector should be required to consider expected cost and benefit (both in terms of the inclusion of relevant information and features, and the impact of obligations on both small and large data holders in the sector) to ensure they are not unduly burdensome, particularly at a time of significant regulatory change for banks as a result of, for example, the Deposit Takers Act and the Conduct of Financial Institutions regime, as well as implementation of the climate-related disclosures regime. Care should be taken in the design and delivery of the CDR to avoid inadvertently stifling competition and innovation by imposing disproportionate expense and administrative burden on industry participants.

(v) **Territoriality**: With respect to the territorial application of the law, as set out at clause 11 of the Bill, we note that officials may wish to revisit the territorial application once the Reserve Bank of New Zealand (**Reserve Bank**) has finalised its review of New Zealand branches of overseas banks has concluded to determine whether any amendments to the scope may be warranted.

(vi) **Requirements of other legislation**: The requirements of other legislation applying to the relevant sector (such as anti-money laundering requirements), as discussed further below.

---

11 Consideration of other special cases will also be needed. For instance, customer loans may be held by a securitisation vehicle; relevant designations would need to include usual customer data relating to such loans, but should not capture the securitisation vehicle itself as a data holder (or, consistent with other legislation such as the Credit Contracts and Consumer Finance Act 2003) require disclosure of the relevant assignment of the loan.

12 For instance, the API Centre standards do not allow for direct-to-customer access to data.

(vii) **Timing requirements for consultation**: To ensure that key matters are identified and considered when developing regulations/standards/designations, the Bill should include clear timing and process requirements, including statements of intent, clear timetables for consultation and response periods. To this end, Australia's independent Statutory Review of the Consumer Data Right[13] notes industry concerns in relation to difficulties of consultations involving multiple regulators and technical complexity, particularly among smaller businesses which have more limited resources. Accordingly, there was a resulting recommendation for increased transparency on CDR consultation processes and a timeline that outlines expected future development to provide greater clarity and certainty to participants.

17. The above examples are not exhaustive. Similar consideration of scope (whether through direct limits in the Bill or additional explicit considerations for the scope of future designation, standard and regulation) also needs to be given to a significant number of other regulations and standards that must operate in connection with each other.[14] We would welcome the early analysis of the potential landscape for further regulation and standards to ensure that their development is appropriately sequenced to take into account points of interdependency.

Part 2: Interaction with other legislation, MBIE as regulator and determination of liability

Conflict with other legislation

18. While the Bill has been aligned with elements of existing legislation (such as the Digital Identity Services Trust Framework Act 2023 and the Accreditation and Standards Act 2015), there are further legislative provisions that overlap with the content of the Bill that need to be considered – particularly in the context of clauses 17 and 18,[15] which require data holders to perform certain actions on request.

19. As drafted, clauses 17(2) and 18(2) provide an absolute obligation on data holders to comply with requests from an accredited requestor (provided the technical requirements in clause 17(1) or 18(1), respectively, are met).[16]

---

13 Available here: https://treasury.gov.au/sites/default/files/2022-09/p2022-314513-report.pdf

14 For example, see provision made for regulation and standards at clauses 26(2), 27, 29, 30 and 33 of the Bill.

15 Noting the submission above that clause 17 and direct-to-customer data access/action initiation should be removed.

16 We note that clauses 17(1)(c) and 18(1)(d) limit the requirement to comply to situations where "the data holder would ordinarily perform actions of the type to which the request relates in the course of the data holder's business". However, this appears to have been drafted to

20. It is important that complying with the obligations imposed on data holders under the Bill does not conflict with data holders' obligations under other legislation. Without considering these overlapping provisions, the Bill could be unworkable for data holders, including the banks as the first designated data holders.[17]

21. Examples of situations where complying with the obligations imposed on data holders under the Bill may conflict with requirements elsewhere in law are:

    (a) loan/mortgage applications and the overriding need to comply with obligations under the Credit Contracts and Consumer Finance Act 2003 and the Responsible Lending Code, including suitability and affordability assessments;

    (b) obligations under 'Conduct of Financial Institutions' legislation and the relevant bank's fair conduct programme under the Financial Markets Conduct Act 2013 not being aligned to undertaking the action requested by the customer or the accredited requestor;

    (c) the need to conduct customer due diligence on a customer under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 before opening an account, which may cause a delay or require more information before performing the action under clauses 17 or 18;

    (d) the need to consider sanctions legislation before giving effect to a transaction under clauses 17 or 18; and

    (e) requirements to comply with the Reserve Bank's cyber-resilience requirements, which may require certain actions not to be performed where a bank has formed a view that the valid requests are fraudulent or part of a distributed denial-of-service (**DDoS**) attack.

22. As the Bill is currently drafted, there does not appear to be an ability for a data holder to decline to provide the relevant data or to decline to perform the requested action for any of the above reasons – although we expect the intention is that those laws should be complied with in priority to the CDR - or for general fraud detection or similar. In practice we expect there are many practical reasons that requests should not be honoured in specific cases, in line with normal business practices. Consideration should also be given to ensuring that data holders are provided with all relevant information necessary to assess and comply with such other laws – such as for customer due diligence purposes, suspicious transaction reporting and risk assessments (such as accreditation and other features of the requestor).

23. In addition, NZBA proposes that provision is made in the Bill for leniency in emergent or high stress scenarios or situations where data holders experience an

---

exclude situations where a data holder would not perform such actions due to specific laws applying in the relevant circumstances.

[17] The concern here is heightened by the omission of an equivalent to section 56GC of the Australian Competition and Consumer Act (which as mentioned in paragraph 223 of the Discussion Document provides protection from liability where an entity complied with the CDR requirements).

increase in data requests at the same time as experiencing a reduced ability to respond to these. For example, the early stages of the COVID-19 pandemic resulted in concerns among customers that may have provoked data requests or action initiation had the CDR been in place, at the same time as operational and staffing demands may have reduced a data holder's ability to respond.

24. These issues could be largely addressed by:

(a) allowing the data holder to decline to process a request if it forms the view that to do so would be contrary to applicable law. Such other laws should also be explicitly considered when developing regulations, standards and designations as discussed above; and

(b) including provision for an appropriate limit to be imposed on the number of requests per day (for instance in relation to particular data). We understand similar limits have been implemented in the United Kingdom.

Overlap with other legislation

25. The Reserve Bank's recent consultation on its Cyber Data Collection Proposals included a proposed requirement to report all material cyber incidents to the RBNZ as soon as practicable, but within 72 hours. It is foreseeable that the systems operated by banks to meet the proposed requirements of the Bill, may be subject to material cyber incidents that are reportable to the RBNZ. Consideration should be given to any reporting requirements in relation to such incidents to ensure that Banks are not subject to the potentially conflicting requirements of two regulators, particularly at a time where focus should be on limiting and addressing the impacts of any such incident.

26. NZBA also notes:

(a) The proposed reliance on the Privacy Act and the incorporation of the Information Privacy Principles into the Bill in certain clauses.[18] NZBA is concerned that the Privacy Act, as a set of principles-based rules, may lack the precision necessary in places to effectively address mandated data sharing and action initiation, given the broadened data and scope of usage of CDR compared to the Privacy Act. A full analysis has not been possible in the timeframe for consultation, but we agree with comments in the Discussion Document that further work is needed, including a gap analysis of the Privacy Act to ensure that the appropriateness of the proposed reliance on the Privacy Act is fully assessed. The Bill should also provide flexibility to apply further usage/holding/sharing restrictions for recipients of CDR data (including application to non-accredited persons). This could be included in relation to the regulation making powers in clause 84(1), for example.

(b) Section 55 of the Privacy Act has been disapplied in responding to an Information Privacy Principle 6 request for access to personal

[18] See, for example, clauses 45, 47 and 48.

information.[19] Currently banks may rely on section 55 of the Privacy Act to exclude personal data relating to its staff members where they are identified in documentation provided, such as notes. NZBA's concern here would be reduced where the definition of designated customer data is narrowed to transaction data and excludes broader information, as discussed in more detail at paragraph 16(g)(ii) above.

(c) Information Privacy Principle 8 is not one of the disapplied provisions of the Privacy Act. This requires a data holder to check the accuracy of personal information before disclosing that information. In the context of the CDR, this is neither possible nor practicable, particularly given the speed with which a data holder must comply with a request and given the likely volume of requests. NZBA submits that Information Privacy Principle 8 should also be disapplied in the context of the CDR regime.

(d) Information Privacy Principle 9 (that personal information must not be kept longer than is necessary) should also be considered for all CDR data. It should be clarified how this interacts with the record-keeping requirements in clauses 41 and 42 of the Bill. The Bill should also address requirements to delete customer data (whether or not personal information) where the customer's authorisation has been revoked.

(e) Further questions remain about the overlap with the Privacy Act 2020, and how, for example, a notifiable privacy breach 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 potential any accredited requestor's outsourced provider, who will be required to notify the privacy breach?

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.

27. We note MBIE's stated intention to continue work to align the CDR with relevant aspects of the single customer view (*SCV*) requirements for the depositor compensation scheme under the Deposit Takers Act. NZBA would welcome and recommend strong engagement between MBIE and the Reserve Bank to ensure that in the interests of efficiency and to the extent possible, a single system change to accommodate SCV and CDR can be made.

---

19 See clause 46(h).

28. These points should be addressed in the legislation so that there is clarity upfront as to what is required of data holders and accredited requestors in such situations so that entities know what their compliance obligations are. This supports the principle that the law be certain so that people can ascertain their obligations.

MBIE as regulator

29. NZBA notes the proposed role of MBIE as regulator under the Bill. NZBA submits that the Bill should:

    (a) set out MBIE's objectives and purposes as regulator, to provide guidance to both MBIE in its actions and to relevant sectors. For instance, the objectives and purposes of FMA and Reserve Bank as regulators are set out in the Financial Markets Authority Act 2011 and the Reserve Bank of New Zealand Act 2021, respectively;

    (b) expressly require MBIE to act independently in its role as regulator, similar to section 20 of the Privacy Act. Ideally this would be through a separate team at MBIE. The bank sector currently frequently engages with MBIE and care should be taken not to adversely affect the level of open, independent engagement as result of overlap with regulatory roles; and

    (c) add further clarity, including for the reasons outlined at paragraphs 26 to 0 above, as to the interaction between the Office of the Privacy Commissioner (*OPC*) and MBIE as regulators. For instance, will OPC act as main regulator with MBIE's role limited to regulation of breaches of general CDR requirements only, or is it intended that MBIE become the primary regulator?

30. We also note that the Discussion Document anticipates that dispute resolution schemes will play a primary role in managing disputes involving customers. NZBA submits that regulator involvement will be key in disputes between data holders and accredited requestors, as well as in ongoing testing, monitoring and re-confirming accreditation.[20]

Liability regime

31. A robust liability regime needs to be included in the Bill that recognises the limitations, including inconsistency in quality, of customer data and product data, as well as the speed with which data holders are being asked to provide it and the potential quantities that they may be asked to provide from time to time. As outlined at paragraph 16(b) above, it is important that clear rules apply to ensure that customers understand who is accountable in circumstances where they wish to complain. This will also help to ensure that risk is equitably distributed through the CDR ecosystem. In the absence of this clarity, there is a risk that certain

---

20 As a related point, the Bill should provide further seek clarity on the accredited requestor verification process, particularly if it must be repeated periodically or on an ongoing basis.

participants or classes of participants are required to bear a disproportionate or asymmetrical level of risk.

(a) **Proper authorisation**: The Bill should clearly establish that data holders will in no case be liable to customers where they have properly verified the customer and the accredited requestor, where relevant,[21] confirmed the customer's authorisation[22] and provided the data pursuant to clause 14, 15 or 21 of the Bill.

(b) **Good faith disclosure to accredited requestor**: Currently customer data can be checked by data holders before it is disclosed or otherwise transferred to a third party. Under the proposed system in the Bill, there will be no opportunity for the data to be checked before it is provided in response to a request. Much of this data will be historic data stored by Banks in potentially legacy systems in a different format to what is contemplated by the electronic system established under the Bill.

If there is an unidentified error in the data provided to the accredited requestor or to the customer due to the nature of the data being requested and the speed with which it must be provided, then data holders should not be liable provided they have acted in good faith and have proper processes and systems in place. In the absence of such a provision, the compliance costs of the regime and the cost for banks to review all customer data on their systems and ensure it is correctly formatted[23] (including and particularly in respect of free form text notes on a customer's file, if these are deemed to be within the Bill's scope) will outweigh the benefits of the regime and slow provision of data.

(c) **Liability for misuse of data or incorrect instructions**: The Bill should also address liability where (for example) an accredited requestor is the subject of a cyber-attack or other event (including indirectly through an event suffered by a third party non-accredited provider), and provides instructions to a data holder that are contrary to the customer's instructions to the accredited requestor (such as moving money to an account with another bank). In such cases, it should be clear that the data holder is not liable to the customer or any other party for following such instructions.

In this regard, we note that paragraph 223 of the Discussion Document refers to section 56GC of the Australian Competition and Consumer Act (which provides protection from liability where an entity complies with that Act in good faith), and notes that MBIE does not "consider this provision to be necessary as compliance with an Act should not, as a matter of law, create liability". NZBA submits that such an explicit provision is in fact vital to the proper functioning of a CDR.

---

21 Pursuant to clause 37.

22 Pursuant to clause 33.

23 See our comments at paragraph 16(g)(ii) in relation to the scope of the Bill.

(d) **Steps to avoid loss or damage**: Clause 56 of the Bill requires data holders and accredited requestors to take steps to avoid, mitigate, or remedy loss or damage a customer has suffered, or is likely to suffer, as a result of the data holder or accredited requestor's contravention of a duty imposed by the Bill or under regulations. The specific steps to be taken by data holders and accredited requestors are to be prescribed by regulation (subject to clause 86(3)). In its current drafting, clause 56 provides for MBIE to impose broad requirements and potentially significant costs on data holders and accredited requestors, with no legislative guidance on appropriate parameters. NZBA is concerned that this represents a potentially material devolution of power from Parliament.

Part 3: Appropriate consent settings for the CDR in the Bill

32. The Bill provides that designated customer data may only be shared where the customer has provided consent (referred to as 'authorisation' in the Bill) that is express and informed. The establishment of authorisation by a customer is also dependent on establishing that the customer is reasonably informed about the matter to which the authorisation relates. NZBA is supportive of an approach that ensures customers understand the risks and opportunities of authorising access to their data (or action initiation, if included in the Bill) and that they clearly appreciate the implications of doing so.

33. Detailed guidance providing clarity on how express and informed consent is established is required to ensure requests are able to be verified and responded to efficiently. For example, NZBA cannot identify in clause 30 (or elsewhere) provision for the accredited requestor to advise the data holder of the scope of the authorisation they believe the customer has provided, in order for the data holder to verify this with the customer. Nor can NZBA locate provisions clearly setting out how a data holder is advised of modification to customer consent, where the customer notifies the accredited requestor.

34. While these matters are likely to be dealt with in regulations or standards (the Discussion Paper talks of an accredited requestor notifying a data holder of a change in customer consent), clarity in this respect and consistency in the customer experience will be vital to removing friction in administration and increasing the efficiency and timeliness of response which will, in turn, increase customer trust in, and desire to use, the CDR. We note that specific customer experience guidelines (providing general minimum standards without being so restrictive as to stifle innovation), may be as important in ensuring the success of the CDR as technical API standards,

35. Clause 31 of the Bill contemplates three ways to manage ongoing customer consent/authorisation, potentially through **time-limited authorisation, events-based withdrawal of authorisation** and a **time specified by the customer**.

(a) **Time-limited authorisation**: A twelve month consent expiry date is common in both Australia and the UK. NZBA submits that an expiry date of up to twelve months will be often be appropriate in New Zealand as well, to balance the interests of continuing access and ease of use against the

possibility that customers have low motivation to verify their settings and ensure that access granted continues to align with their needs. However the appropriate expiry dates will ultimately depend on the type of data/actions the authorisation relates to and regulations setting out sector-specific expiry limits may be appropriate, taking into account the nature of the information or action being authorised and, further, different expiry dates may be appropriate for different levels of access (eg. read-only access may be maintained for longer than access granted for action-initiation purposes, if action initiation is included in the Bill).

(b) **Events-based withdrawal** of authorisation in prescribed circumstances. NZBA agrees that events-based termination of authorisation is appropriate in the circumstances proposed by MBIE at paragraph 65 of the Discussion Document.

(c) The **time specified by the customer.**

36. NZBA is supportive of clear and timely guidance in respect of circumstances where authorisation is automatically terminated, to allow members to build systems and processes to support these requirements and to allow banks to limit exposure to unintended data and other breaches.

37. Paragraph 162 of the Discussion Document notes that regulations will be developed to set out detailed requirements for the functionality of the systems and processes for dealing with joint account holders and secondary users.[24] The operational considerations behind processes and systems for joint account holders and secondary users can be complex, for example where multiple parties may be required to provide express and informed consent to an action.

38. NZBA welcomes the suggestion that consideration is given to banks' existing systems and processes in place for dealing with joint account holders and secondary users in developing the detailed regulatory requirements for functionality in respect of these accounts. We note that this a particularly complex area of operation and suggest that banks' existing consent arrangements should be included in the consideration process, as well as the API Centre's Customer Experience Guidelines and its Principle of Equivalency.

39. NZBA notes that the Discussion Document does not specifically propose an approach in respect of the designated data of customers under the age of 18. As set out at paragraph 38 above, NZBA proposes that banks' existing systems and processes (including in respect of consent) for these accounts are designated as acceptable to the extent possible, to avoid specific and bespoke requirements resulting in inefficiencies or delays in implementation with respect to younger customers.[25]

---

24 We note that clause 22(3) provides for secondary users to give authorisation for the purposes of clauses 14 to 18, but not in respect of clause 32. We propose that reference to clause 32 should be included in clause 22(3) or consistency.

25 NZBA suggests that an approach may be to exclude account holders under the age of 18 from the definition of 'customer', although further consideration would be required in the

40. Clause 30 provides the requirements for ensuring a customer has appropriately authorised an action, but is unclear as to whom authorisation must be given. We assume that at least an element of authorisation is required to be given to an accredited requestor, in order for it to ascertain that it has adequate data to provide its service and initiate an action. Clause 33 is similarly unclear as to the entity to whom authorisation is given although the example provided at clause 33 appears to suggest that authorisation must be given to the bank as data holder. Amendments to clauses 30 and 33 are required to ensure that data holders and accredited requestors have clarity in respect of their respective roles in the authorisation process and that consent is duly obtained.

41. Similarly, the example given at clause 33 contemplates a situation whereby banks are able to rely on a customer's authorisation in respect of the provision of information to a specific accredited requestor until such time as the scope of that authorisation is modified or the authorisation ends. It is not clear whether it is intended that a bank may rely on a standing customer consent to the provision of specified data to multiple accredited requestors or whether MBIE expects that customer consent to the provision of data to each specific accredited requestor must be obtained on a case-by-case basis.

Part 4: Miscellaneous matters

42. In addition to the key themes discussed below, NZBA also notes the following:

(a) **Outsourced providers**: Clause 24 of the draft Bill requires a data holder or accredited requestor to take 'all reasonable steps' to ensure that an appointed outsourced service provider complies with any requirements or limitations applicable to the data holder or accredited requestor's performance or exercise of such duty or power under the Bill. NZBA would welcome further guidance as to what will constitute 'all reasonable steps' for the purposes of the Bill. For example, will it be adequate for this requirement to be addressed in contractual arrangements with any such service provider, or will additional requirements apply?

(b) **Government fees and levies**: We note that further and specific consultation will take place before the policies are set in relation to the Government's ability to impose levies and charge accreditation fees.[26] NZBA agrees with MBIE that significant investment will be required from banks in order to avail of the CDR and comply with the terms of the Bill and looks forward to further discussion on these matters, noting in particular that the cost of implementation for smaller banks may not necessarily be proportionate to their customer base or market share.

(c) **Accredited requestor insurance:** The Discussion Document seeks feedback on whether accredited requestors should be required to hold appropriate insurance and gives consideration to the imposition of

context of the Bill.

[26] Paragraphs 193 and 194 of the Discussion Document

insurance requirements on businesses involved in the CDR ecosystem more broadly. The insurance market for open banking is very limited both domestically and offshore and accordingly consideration should be given to ways in which the establishment of an appropriate insurance market can be supported by MBIE and the Government more broadly.

(d) **Record keeping**: Clauses 40(3)(a) and 41(2)(a) of the Bill require records to be kept for five years. We would welcome greater clarity on data holder obligations, particularly in respect of the point at which the five-year time period commences. We would also welcome clarity as to whether the requirement that data holders keep records of requests made for data under clause 41(2)(a) requires records to be kept for each individual data request, or the overarching authorisation provided in respect of each data request.

(e) **Notification of provision of data in cases of enduring consent:** Clause 38 requires data holders to notify a customer each time it provides a regulated data service to the customer, including requirements to notify the customer of certain rights under the Privacy Act where the customer's personal information has been provided. Clarity should be provided as to the application of this requirement to enduring consent cases where, for example, API calls may be made frequently to update information or where accredited requestors submit frequent requests to update customer transaction data. Is it intended to notify customers each time the data is provided or simply where the data provision is made in response to the initial customer authorisation? We note comments made in Australia's Statutory Review of the Consumer Data Right as to "consent fatigue" impact on customer experience[27] and, potentially, uptake of the CDR more broadly. We are equally concerned that constant notifications may drive fatigue and disinterest, potentially reducing customer engagement with more pivotal or fundamental CDR notifications. Alongside this, the effect of the proposed changes to Information Privacy Principle 3, requiring a party collecting personal information indirectly from another party to notify the individual concerned will need to be considered so that data holders and accredited requestors alike are not required to over-notify customers. Otherwise, the risk with over-notification is that customers will not read any of it and therefore potentially miss important notifications.

(f) **Required policies:** The Bill requires data holders to prepare and publish customer data, product data and action performance policies. Any requirement for such policies should be designed with reference to customer benefit, and only require information to be included that meets this purpose. For data holders, it is expected that the contents of these policies would therefore be very limited (given that data holders generally have obligations under the Bill, rather than powers with discretion as to how to exercise or manage those powers[28]) and consideration should be given to whether these policies are appropriate for data holders.

---

27 Page 43 to 44.

28 In particular, such policies should not be required to disclose 'back-end' service providers or basic function outsourced providers, as discussed above at paragraph 16(c)(iii).