New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Economic Development, Science and Innovation Committee

on the

Customer and Product Data Bill

5 September 2024

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 (New Zealand) Limited
   - 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 Economic Development, Science and Innovation Committee (**the Select Committee**) on the Customer and Product Data Bill (**Bill**). NZBA commends the work that has gone into developing this Bill.

Contact details

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

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Associate Director, Policy & Legal Counsel
sam.schuyt@nzba.org.nz

Need for ongoing consultation and overview of submission

Initial Designation/Standards Consultation

4. NZBA notes that Ministry of Business, Innovation and Employment (**MBIE**) has recently released an initial discussion paper, *Open banking regulations and standards under the Customer and Product Data Bill*, on 2 September 2024 (**Initial Designation/Standards Consultation**)[1], which seeks feedback on proposals to implement open banking under the Bill. NZBA commends MBIE for such engagement.

5. Given the short timeframe between the release of this discussion paper and the due date for submission on the Bill, we have not considered the full potential impacts of the Initial Designation/Standards Consultation in this submission.

6. While we appreciate the opportunity to engage at each step of the development of a Consumer Data Right (**CDR**) in New Zealand, the sequencing of these consultations has created uncertainty and duplication of effort, to the extent that MBIE's discussion paper considers proposals under a Bill that is still going through the Select Committee process.

7. Given the overlap with the Select Committee process (and therefore, current lack of clarity on the final form of the Bill), NZBA further encourages officials to work transparently with industry to ensure the Designation Consultation reflects changes at Select Committee stage.

Engagement with industry

8. The Bill as introduced follows a 2023 consultation by the MBIE on an exposure draft of the Bill (**Previous Consultation**).

9. The Previous Consultation was undertaken on a short four week timeline, and in our submission (the **Previous Submission**) NZBA encouraged ongoing engagement to work through the complex matters included in the exposure draft (as well as the various matters that were left as placeholders in the exposure draft, such as for enforcement), with further industry workshops being considered an effective mechanism to share feedback on the implementation practicalities of the reforms. We noted that, 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.

10. While NZBA appreciates the work that has gone into development of the Bill, industry has not been engaged in the development of the Bill since the Previous Consultation. Therefore:

    (a) **NZBA reiterates that such engagement is vital**, both to creation of the CDR framework in the Bill and in further development of regulations and standards, which will involve substantially more complexity than the Bill itself.

---

[1] https://www.mbie.govt.nz/dmsdocument/29084-discussion-paper-open-banking-regulations-and-standards-under-the-customer-and-product-data-bill-pdf

(b) Where relevant, and for the Committee's benefit, **this submission canvasses points from the Previous Submission which we believe remain as outstanding concerns** (updated as applicable to refer to the Bill).

Learning from Australia

11. We would like to draw the Committee's attention to the recent strategic review of the Australian CDR regime prepared by Accenture and commissioned by the Australian Banking Association.[2] The Australian CDR regime has become known for its significant cost of implementation and compliance. The review found that only 0.31 per cent of bank customers were active CDR customers at the end of 2023, on the back of approximately A$1.5bn of banking industry investment since 2018 (with further significant investment still needed for switching and other action initiation).

12. A review of the Australian CDR regime commissioned by the Department of Treasury[3] found that changing regulatory obligations were a key contributor to costs, as policy, frameworks and (in particular) data standards have evolved over time, and that such ongoing compliance costs "may be contributing to slow adoption of CDR-enabled products and services".

13. NZBA encourages officials to take account of the solutions and improvements proposed for Australia when developing New Zealand's CDR, including:

(a) "**Industry participants would benefit from clearer strategic and tactical planning for the CDR**. This would allow them to plan and budget for future investment, including developing customer use cases. For example, the CDR agencies could publish a medium-term plan, with strategic priorities and explicit tactical objectives for improving the CDR experience and reducing costs in each industry over the next 1-2 years. This could also serve as a guide in prioritising future rules and standards changes."

(b) "**Formalise a forum for industry** to raise business implementation considerations across the Government agencies and discuss possible solutions."

(c) In relation to other implementation considerations, **adopting a more collaborative and iterative consultation approach between participants** and the relevant Government department.

Early clarity and direction is vital to a successful regime

14. As discussed further in paragraph 22, **additional clarity on boundary setting and guidance needs to be a priority concern** while the CDR framework moves closer to completion. Industry will require time to develop systems (with competing

---

2 "Consumer Data Right Strategic Review", July 2024, available here: https://www.ausbanking.org.au/release-of-strategic-review-into-roll-out-of-the-consumer-data-right/

3 Better Regulation Advisory "Consumer Data Right Compliance Costs Review: Report for the Deportment of the Treasury", December 2023. Available at https://treasury.gov.au/sites/default/files/2024-08/p2024-512569-report.pdf

resources from the Deposit Takers Act overhaul and other regulatory developments), which will require certainty of the potential scope and direction of the framework.

15. We highlight the **urgent need for clear direction ahead of deadlines** to ensure successful implementation. The intended timeframes set out in the Initial Designation/Standards Consultation is a very short timeframe to develop regulations and standards in, as well as for industry to build solutions off the back of unknown requirements in order meet the deadline. For instance, as discussed above, care and ongoing engagement will be needed to ensure the Initial Designation/Standards Consultation to ensure it links in with the final form of the Bill, and provide industry with certainty on the direction.

16. In the absence of clear guidance and proposed use cases, the truncated timeframe risks unintended consequences occurring and potential gaps in the system or weak points in the design, which may subsequently end up affecting customers and may have a detrimental effect on the uptake of the CDR regime.

An equitable and clear liability regime is required

17. As discussed further in paragraphs 95 and 96, an **equitable and clear liability regime** is needed in the Bill to address the limitations and risks associated with customer and product data, especially given the speed and volume of data requests. As discussed below, clear rules are required to ensure customers know who is accountable for complaints, and to distribute risk equitably within the CDR ecosystem. Despite MBIE's comments, NZBA considers that a "safe harbour provision" is required to protect compliant participants, highlighting the risks of immediate, automated disclosures without traditional oversight. This provision is vital to the proper functioning of a CDR.

18. We also note that, further to our comments in paragraph 15 above and contrary to comments from the Ministry of Justice,[4] MBIE has specifically excluded the accessory defences in clause 91 from applying to development of electronic systems, on the basis of a strong desire to ensure that data holders do not "escape deadlines for implementation by asserting they were missed due to difficulties with third party IT providers, IT skill shortages, etc" to ensure a successful regime. However, NZBA believes that to ensure deadlines are met the focus should be on providing clear direction sufficiently in advance of those deadlines to allow them to be met, rather than just imposing penalties for a failure to meet requirements on an unnecessarily short timeline.

Other headline matters

19. As was generally described in the Previous Submission:

    (a) A successful, well-used and secure CDR requires careful design, with ongoing input from data holders, potential accredited requestors and customers into implementation, including in relation to the drafting of the regulations. Further, it should also consider and, where appropriate and tested, link with the Digital Identity Services Trust Framework Act 2023 as

[4] MBIE's Departmental Disclosure Statement dated 13 May 2024, in response to question 3.4.1.

a potential enabler of its benefits (noting that this is contemplated at paragraph 9 of the Initial Designation/Standards Consultation).

(b) NZBA supports the development of a CDR using the Bill as the overarching regime to deliver open banking. **The NZBA advocates that the Bill should be the sole way forward for delivering open banking**.

As such, the NZBA does not support the Commerce Commission's recommendations to separately designate the interbank payment network under the Retail Payment System Act. We understand from the Commerce Commission's Market Study recommendations, that the Commission is proposing a dual regulator model for open banking whereby the Commission is responsible for payments and MBIE is responsible for other aspects of the CDR. In the NZBA's view, having both the Bill and the designation is unnecessary, duplicative and inefficient. Taking such a split approach will undermine the need for cohesion in the roll out of open banking, and increase risk of non-compliance. **NZBA supports a single regulator approach to open banking (including for payments), to be addressed under the Bill.**

(c) 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 include a strong customer education component and be:

(i) designed for **certainty**, **efficiency**, **ease of use**, and – above all – **security.** Access to data in the CDR regime, including product data (which the Bill provides must be made available to any person) and customer data (which the Bill provides must be made available to any customer which includes any person seeking to acquire goods and services) should be limited to only accredited requestors to mitigate inherent security risks in the CDR. CDRs must allow for standardised, robust and efficient deployment, while also providing customers with utmost confidence to use the system; and

(ii) respectful of customer data and its value to customers, to foster the trust and confidence of customers in using the CDR. A CDR needs to strike the right balance between making data available for appropriate usage, and enabling the protection of such customer data.

(d) 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.

(e) It is important to **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.

Submission outline

20. 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 further 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**.

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

21. 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.

22. We also support the Bill's inclusion of some safeguards for the setting such future regulation. However, as discussed further below we consider that more work needs to be done to bolster and refine such safeguards.

Protecting CDR data obtained by accredited requestors

23. Ensuring that the CDR requirements cannot be avoided by using an intermediary, and ensuring customers know that they are in the CDR ecosystem, will be very important considerations for regulations.

24. An accredited requestor should only be permitted to share CDR data in circumstances expressly permitted by regulation.

25. This is vital to build customer trust and confidence in the CDR and to ensure its proper use and growth – without strong protections around sharing of CDR data, there are incentives on data recipients to remain unaccredited and access CDR data through a small number of accredited intermediaries. As it stands, the Bill is currently silent on this issue which means that by default the Privacy Act would apply if personal information were being disclosed, or no specific regime would apply to business customer information.

26. 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 (and only to personal information. For non-personal information, no statutory provisions would apply, unless those protections are to be specified in the Bill).

27. NZBA is concerned that general reliance on the Privacy Act risks customer data being shared more widely than expected, in uncontrolled environments (see also further discussion at paragraph 75 below). We consider that this needs to be considered in more detail at regulation stage, in relation to the information being made available and the relevant sector (i.e., in this case open banking).

Electronic system access should be limited to accredited requestors

28. As discussed in the Previous Submission, the Bill requires data holders to operate 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:

    (a) product data must be made available to any person (clause 22), and this may potentially include an extremely wide range of data because the details of what is designated product data is to be left to the regulations; and

(b) customer data must be made available using the electronic system to any "customer" (clause 14),[5] which is defined in clause 8 to include any person "seeking to acquire" goods or services from a data holder.

29. NZBA notes that the Initial Designation/Standards Consultation states that MBIE is still considering whether to designate product data (paragraphs 62 to 68).

30. In any event, NZBA is concerned about any potential requirement in the Bill to provide information to, and open systems to, parties beyond accredited requestors at any stage. 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 of the proper use of such data). This is an important consideration given scam and fraud risks in particular.

31. 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.

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

(a) 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

(b) providing product data to accredited requestors would be sufficient to allow those accredited requestors to analyse customer data and give effect to the CDR.

33. There are risks if the Bill continues to allow data to flow to parties beyond accredited requestors because these parties are not subject to MBIE's accreditation process. Protections and liability for information flowing to parties beyond accredited requestors (called 'fourth parties' by some) need to be set out in the Bill. Information being disclosed by accredited requestors risks negative potential outcomes, including mass data leakage, state actor profiling which would be hard to detect and stop potentially causing irreversible damage to people, property and these outcomes would erode trust in the CDR regime. For this reason it is vital that adequate protections and robust liability settings are included in the Bill to deal with the downstream effects of data flowing to fourth parties.

34. NZBA submits that data holders should be able to reject access requests where they reasonably believe the accredited requestor is not fulfilling their requirements or performing their duties under the Bill.

---

5 See further comments on this clause below.

Direct-to-customer data access and action initiation is not appropriate for CDR and increases risk

35. The Bill contemplates customers[6] accessing data (clause 14) and initiating actions (clause 18) directly, as well as through accredited requestors. As drafted, it appears to be intended that data holders build such access into their electronic system design (clause 27) when designated customer data is specified for a sector.

36. In this regard, NZBA supports the position in the Initial Designation/Standards Consultation, which proposes that (at least initially) access be limited to accredited requestors only, without extending to direct-to-customer data access and action initiation (see paragraphs 52 to 54). However, NZBA considers that direct-to-customer access/initiation should be removed at statute level as well.

37. 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.

38. 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'.[7] 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. The Australian Government's statement in response to the Statutory Review of the Consumer Data Right (June 2023) stated that as the consumer data right regime matures, the risks associated with direct-to-consumer data share may decrease, at which point enabling data transfers should be reconsidered but any future changes would require amendments to the statutory framework particularly in relation to liability for loss.

39. Accordingly, we recommend reconsidering the introduction of a direct-to-customer data right at a later point when the CDR has matured.[8] 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

---

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

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

8 See page 27.

possibly be given to its inclusion in future if a strong customer benefit is established which outweighs associated risks.

The Bill should provide a clear roadmap for action initiation including a bedding-in period for certain action initiation after data access has commenced

40. Clauses 18 and 19 of the Bill require data holders to carry out actions (action initiation) where the request meets the relevant criteria (and clause 20 provides certain circumstances in which a data holder may or must refuse to perform actions). 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.[9]

41. NZBA supports the general position in the Initial Designation/Standards Consultation, to initially focus on matters addressed in the API Centre Minimum Open Banking Implementation Plan (see paragraph 39). The industry is supportive of the move to accelerate open banking. However, there are reasonable practical limitations to how quickly the regime can be fully implemented. A staged approach to implementing the action initiation part of the regime would recognise these practical limitations. 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 and downstream non-accredited requestors to operate customer accounts.

42. NZBA submits that 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. This is not currently listed in clause 100 as one of the factors that may be set out in the designation regulations.

Clear limits should be included on ability to designate product data

43. NZBA notes that the Initial Designation/Standards Consultation states that MBIE is still considering whether to designate product data for open banking (paragraphs 62 to 68). However, the Bill generally allows for any data "that is about, or relates to, 1 or more of the data holder's products" to become designated product data (clause 9). Clause 100 further defines various categories of data that may become designated product data, providing some limits and guardrails to this potentially extremely broad category.

44. Guidance from MBIE further suggests that the intention of clause 100 is to (among other things) limit designated product data to information that is otherwise publicly available, stating that "it was not the policy intent for the Bill to generally require data holders to produce and disclose new, non-public information".[10]

---

9 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.

45. While cause 100(2)(e) does provide that the general category of designated product data is limited to "data about [a] product that is of a kind that is ordinarily publicly available", this may be read as referring to data that, in a general sense across the sector, is ordinarily made publicly available for various products (rather than data that the specific data holder ordinarily makes publicly available about its own specific products).[11]

46. Further the types of data described in clauses 100(2)(a) to (d) are not subject to this "publicly available" limitation at all.

47. The provisions therefore remain potentially exceptionally broad, and:

    (a) 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 be interpreted as requiring disclosure of internal credit metrics and analysis. As discussed above, the "ordinarily publicly available" limit does not apply to such information (as it relates to the price of the product, clause 100(2)(d))), but even if it did that limitation would still be insufficient – e.g. although carded rates may be considered "ordinarily publicly available", but more specifically they may not be made available for non-consumer lending. 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

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

48. 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.

49. 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. This could be achieved by:

    (a) amending clause 100(2) to provide that paragraph (e) applies to all data or classes of data that may be designated as designated product data;

---

11 This contrasts with clause 18(1)(c), which only requires a data holder to perform actions if "the data holder would ordinarily perform the action to which the request relates in the course of the data holder's business", and is clearly directed at the specific data holder rather than what may constitute ordinary course for the broader industry.

(b) providing in the definition of "product data" that such information extends only to such information that the relevant data holder ordinarily makes publicly available; and

(c) in addition, if anything beyond basic publicly available information is to be 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).

Limits on granting access and processing requests

50. The Bill allows a data holder to refuse a request for data or to initiate actions in certain limited grounds, including where the data holder reasonably believes that disclosure or action would be likely to have a materially adverse effect on the security, integrity or stability of the data holder's systems. However:

(a) the grounds still require data holders to provide general *access* to the relevant systems (i.e. it only permits or requires refusal to process instructions after access, in certain circumstances);

(b) data holders are allowed to refuse action initiation on the basis of "significant likelihood of serious financial harm" or if the request was made as a "consequence of deception" (clauses 20(1)(b) and 20(1)(c)), but no similar provision is included to allow data holders to refuse data access; and

(c) the data holder would be restricted from agreeing contractual terms to manage these risks.

51. NZBA submits that data holders should have the right to refuse access to their relevant systems, and provide data or initiate actions, in relation to a relevant accredited requestor if the data holder believes that:

(a) shared data is subsequently being shared outside of the CDR regime; or

(b) the accredited requestor is not fulfilling its requirements/performing its duties.

52. As a more general point, it is not clear how the ability (and, in some cases, requirement) to refuse to process requests in clauses 16 and 20 are expected to function in practice, given the automated nature of electronic system responses. For instance:

(a) Data must not be disclosed if the data holder has reasonable grounds to believe that the request is made under the threat of physical or mental harm. However, by design data requests will be processed immediately without human involvement, based on machine interaction with an API. If this obligation is to be included in the Bill, then the NZBA submits that it should be restricted to situations where the data holder has actual

knowledge of a threat rather than simply "reasonable grounds to believe", particularly since there is an obligation in such situations for the data holder not to disclose the information. If (despite this submission) the "reasonable grounds" wording is retained, then guidance is required as to what such "reasonable grounds" are expected to include in such cases, and it should be clear that it is only satisfied where relevant necessary information is in fact provided in a manner that can be reasonably assessed in the timeframe.

(b) The limits are generally expressed as applying on a 'per request' basis, so that (for example) if a data holder discovers an issue with a process rather than a request, the data holder is not able to refuse to provide data as a result of that discovery. NZBA considers that the ability to refuse requests in clauses 16(1) and 20(1) should also allow a process approach, where data holders may refuse to provide data etc if **a process they maintain** (in accordance with relevant guidance) has identified that one of the concerns in that clause may apply. It should also be acknowledged that the actioning of some requests may be delayed if such processes identify a concern requiring human intervention to review.

(c) Clauses 16(1)(d) and 20(1)(e) allow an action to be refused "if the customer owes a debt to the data holder in relation to charges imposed in connection with the request". Similar provisions are also included for accredited requestors. These should be amended to:

(i) expressly confirm that data holders may charge for requests, and require payment before actioning (noting that this is currently left for regulation in clause 32(1)(a)). The Initial Designation/Standards Consultation indicates that the intention is that regulations may be made for this purpose, so this should be clearly reflected in the Bill as well; and

(ii) in the case of a customer, refuse to action a request if the customer owes a debt in relation to charges imposed in connection with any previous request (similar to the provisions included for accredited requestors).

53. The NZBA submits that the current grounds in the Bill for refusal to process a request are insufficient, or, in some cases, the grounds in the Bill set too high a bar for refusal (for example, the applicable standard in clause 16(1)(a) and 20(1)(a) should be "reasonably believes" rather than "would be likely to" to align with the rest of the clause). It is important that banks are able to take steps where there is a risk of fraud or scams or where there are concerns a vulnerable customer may be being taken advantage of. There should be additional grounds added as follows:

(a) the data holder has reasonable grounds to believe that providing the data (clause 16) or performing the action (clause 20) would cause it to be in breach of any laws in New Zealand or relevant other countries;

(b) clause 20 – for payments, the data holder may refuse to perform the action if the customer has insufficient funds;

(c) the data holder may refuse a request when the account to which the request relates has been suspended or closed for any reason;

(d) data holder may refuse a request when the data holder has reasonable grounds to believe that a customer may not have authorised the instruction, for example, a bank picks up unusual behaviour through biometrics;

(e) the data holder may refuse a request when the data holder has reasonable grounds to believe that the instruction is for an illegal purpose;

(f) to mirror a data holder's current rights to refuse requests through banking terms and conditions;

(g) processing the request would otherwise conflict with applicable law. See further paragraph 70.

54. The Bill should make it clear that a data holder has the ability to impose limits of instructions through a particular accredited requestor (such as transaction size limits) if it is concerned about particular fraud risks or if an individual or cumulative transaction limit for that customer would be breached. A provider should be able to still restrict actions based on the underlying product/service or channel design – for example, payment limits. The electronic access method that the CDR introduces should not be able to bypass protections such as confirmation of payee.

55. The NZBA also submits that there should be "reasonable access" rights. For example, the UK has limits of three requests per customer per day. The details of the reasonable access rights should be included as part of the regulations, but reference should be made to reasonable access rights as part of the definition of a valid request.

56. Consideration should be given to the data required in order for a data holder to make an informed risk-based decision. This should include the necessary information that is required in a request to enable an informed risk-based decision. These considerations should form part of the regulations, but should be signalled in the Bill as a topic for the regulations (along the lines of the indications provided by MBIE as part of its discussion paper).

General guidance on matters to be considered and timing when making a regulation, standard or designation

57. 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 the following points.

Alignment with relevant industry-led standards is imperative

58. Existing industry standards must be the basis that CDR builds on, and NZBA supports the general approach shown in the Initial Designation/Standards Consultation in this regard. The API Centre standards have been developed with considered industry feedback over a number of years. It is beneficial for both data holders and accredited requestors to have certainty that the prior investments they have made into the development of the industry-led standards is not wasted. Otherwise the wrong signal could be sent for future participation in industry-led standards as there will be little incentive for entities to participate if the agreed standards are unwound in the future.

59. 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 in the Bill 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. While the general policy statement in the Explanatory Note to the Bill states that the Bill should not prevent industry-led options from being progressed in parallel to regulatory intervention and where possible, should seek to leverage that work, for example by making use of existing industry standards, technologies and expertise, this requirement is not contained in the provisions of the Bill.

Proportionality of obligations

60. NZBA supports the inclusion of matters in clause 98 that the Minister is required to take into account when making designation regulations, including likely costs and benefits. However, NZBA submits that this should:

(a) apply more broadly in relation to the design of other regulations and standards for each sector; and

(b) be expressly required to considered 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. 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 burdens on industry participants.

Recency of required information

61. For instance, supply of transaction records should be required to be time-limited (consistent with proposals in the Initial Designation/Standards Consultation, to limit data to 7 years of transactions – see paragraph 61) and also limited to open accounts only (both on the basis that historical information is of less relevance, and for practical data availability reasons).

Targeting of required information

62. NZBA notes that the Initial Designation/Standards Consultation proposes a targeted set of designated customer data (paragraph 56).

---

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

63. However, NZBA submits that the Bill itself should be more targeted in what can designated. Rather than potentially requiring "all data" relating to a customer, there should be a legislated focus on (1) what is relevant to the proper functioning of a CDR, including what the customer would benefit from receiving in the context of a CDR and what data could alleviate a particular pain point for customers, and respect for data as discussed in paragraph 19(c)(ii);[13] 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 difficult and potentially costly[14] 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.

64. Customer data files may also include information held by a bank when providing ancillary services (such as a discretionary investment management service or DIMS) or held in relation to products offered by third parties (such as KiwiSaver or insurance products).[15] 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.

Requests to withdraw consent to be given "immediate effect"

65. Clause 39(3) of the Bill requires requests to withdraw consent be given "immediate effect". This should be amended to allow some level of flexibility for participants where their systems may not yet be developed in a way that allows for immediate revocation. In Australia, if the customer withdraws authorisation, the data holder must action that request as soon as possible, within two business days at the most. A similar timeframe for actioning withdrawal requests should be included in the draft Bill. This would align with a similar construct in the Unsolicited Electronic Messages Act 2017 which requires a business to unsubscribe a customer from marketing material within 5 business days of their request.

Timing requirements for consultation

66. 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

---

13 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).

14 See paragraph 102(b) below.

15 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.

Consumer Data Right[16] 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.

67. 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.[17] 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.

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

17 For example, see provision made for regulation and standards at clauses 26(b) and (c), 28(2), 31, 32, 33 and 34 of the Bill.

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

Conflict with other legislation

68. 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 18 and 19,[18] which generally require data holders to perform certain actions on request.

69. Although some limits on requirements to provide data or initiate actions has been added in the Bill (as discussed above), these limits do not expressly address situations where compliance would breach applicable law. [19] Clause 20(g) acknowledges that there may be other circumstances prescribed in the regulations or standards, but there is a lack of certainty as to whether this factor would be included.

70. As generally discussed in the Previous Submission, 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 and points of friction, the Bill could be unworkable for data holders, including the banks as the first designated data holders.[20] 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 assessments;

---

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

19 Although clauses 18(1)(c) and 18(1)(d) limit the requirement to comply to situations where "the data holder would ordinarily perform actions to which the request relates in the course of the data holder's business". However, this appears to have been drafted to exclude situations where a data holder would not perform such actions due to specific laws applying in the relevant circumstances.

We also note that MBIE's Response to submissions on the exposure draft Customer and Product Data Bill states that data holders may or must decline requests "including where this may result in breaches to other laws", but this does not seem to be reflected in the Bill.

20 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 that accompanied the Exposure Draft version of the Customer and Product Data Bill provides protection from liability where an entity complied with the CDR requirements). The omission of this safe harbour in the New Zealand regime could conflict with other obligations if an entity complies with a data request without regard to those other obligations. See our points in this submission at paragraphs 66 and 68.

(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 18 or 19; and

(d) the need to consider sanctions legislation before giving effect to a transaction under clauses 18 or 19.

71. 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. If no safe harbour is provided for data holders providing the relevant data or performing the requested action, then the data holder could be liable for customer harm.

72. 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 increase in data requests at the same time as experiencing a reduced ability to respond to these. For example, if there was an unexplained/unwarranted bank run which would impact on the bank's ability to immediately action outgoing payments, or the early stages of the COVID-19 pandemic which 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. Additionally, reasonable access rights could assist in this situation (see our comments at paragraph 39 on this point).

73. 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 (i.e. extending the factors listed in clause 20 to cover such situations). 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. See our comments at paragraph 39 on this point.

Overlap with other legislation

Breach reporting

74. As generally discussed in the Previous Submission, the Reserve Bank's 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.

Privacy Act

75. NZBA also notes that the proposed reliance on the Privacy Act and the incorporation of the Information Privacy Principles into the Bill in certain clauses.[21] 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. The Privacy Act requires agencies to only take steps that are reasonable to ensure individuals are aware of the collection, use and sharing of their data. It does not mandate explicit 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, being principle-based it 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.

76. By way of comparison, the CDR regime in Australia has introduced 13 privacy safeguards, which apply to "accredited persons" or "accredited data recipients" instead of the Australian Privacy Principles (APPs) and other prescriptive participation requirements to ensure customers have trust in the CDR regime and control over their data.

77. The privacy safeguards in the Bill are intended to complement existing protections in the Privacy Act. A request for data under the Bill (that involves personal information) is deemed to not be a request under Information Privacy Principle 6. Otherwise the Privacy Act provisions exist alongside the provisions in the Bill. The current Privacy Act and its IPPs do not provide full coverage in the CDR context. We note potential tensions between the IPPs and the concept of the CDR framework. For example:

(a) **IPP 1: Purpose of collection of personal information**

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. This is different to the CDR framework which relies on "customer authorisation" for data collection.

(b) **IPP 3: Collection of personal information from subject**

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

There is no “authorisation” requirement under IPP 3. IPP 3 requires agencies only to ensure individuals are aware of certain information stipulated under IPP 3(1). The Bill requires customers to be “reasonably informed” and to provide “express” authorisation to data holders and accredited requestors to enable data access. This implies if data is on shared beyond the CDR ecosystem, “authorisation” may not be required and customers only have to be made aware of the data collection under IPP 3(1).

NZBA submits that the wording of the Bill in this regard aligns with the Privacy Act wording, i.e. that the customer is “aware” of certain information rather than requiring customers to be “reasonably informed”. If the current standard in the Bill is to be kept, the Bill should clearly define what is meant by “reasonably informed”. It should include making customers aware of exactly what data is being collected and shared, how it will be used, who will have access to it, how long they will have access to the data and how the customer can manage and withdraw “authorisations”.

The approach taken by the Privacy Act is a principles-based approach and the NZBA advocates for a similar approach to be taken in relation to privacy matters under the Bill.

(c) **IPP 5: Storage and security of personal information**

The purpose of IPP 5 is to ensure agencies have appropriate security safeguards in place to protect personal information they hold, which generally refers to having appropriate information security safeguards. For example, being ISO27001 certified.

Clause 53 of the Bill provides that a data holder contravenes a CPD storage and security requirement, if they fail to confirm an authorisation received from an accredited requestor (clause 38(3)) or if they fail to verify the identity of the customer (clause 44(2)). This requirement does not fall within the general concept of IPP 5. We consider it is important to have CDR specific privacy-related safeguards.

(d) **IPP 6: Access to personal information**

We note the Bill now provides that access requests made under the Bill will not be considered IPP 6 requests; however contravention of clauses 14, 15 and 16(2) of the Bill will be treated as an ‘interference with privacy’.

In practice, it would be difficult for data holders to comply with clause 16(2) of the Bill, where a data holder must refuse to provide any data requested if the data holder has reasonable grounds to believe the request is made under the threat of physical or mental harm. Given the CDR framework operates on a near real-time basis, data holders will not have sufficient time to evaluate how the request was made.

We also query the intention of clauses 16(1)(d) and 16(1)(e), as we cannot identify in the Bill when data holders may impose a charge on data requests.

(e) **IPP 8: Accuracy of data**

IPP 8, which requires a data holder to hold accurate information, to check the accuracy of personal information before disclosing that information and to ensure that information is up to date. In the context of the CDR, IPP8 would require a data holder to check the accuracy of personal information before disclosing that information. Given the speed with which a data holder must comply with a request and given the likely volume of requests. NZBA submits that IPP 8 should be disapplied in the context of the CDR regime because compliance with this principle would be neither possible nor practicable.

(f) **IPP 9 – Data retention**

IPP9 requires that personal information not be kept longer than is necessary. This should be considered for all CDR data (and not just personal information). It should be clarified how this interacts with the record-keeping requirements in clauses 45 and 46 of the Bill.

The Bill should expressly provide that:

- 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 immediately deleted, unless a law or court order requires it to be retained.

(g) **IPP 10 and 11**

IPPs 10 and 11 set out the uses and disclosures of personal information.

The Bill should 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 126, for example.

As mentioned above, the Australia CDR regime has expressly set out 13 privacy safeguards that are specific to the CDR framework, instead of relying on their Australia Privacy Principles (APPs). Similarly, the European Union General Data Protection Regulation (EU GDPR) also introduced a stricter privacy standard specific for the operation of Open Banking.

We suggest consideration of a CDR/Open Banking Privacy Code of Practice issued by the Office of the Privacy Commissioner under section

32 of the Privacy Act. This would be similar to Codes of Practice applying to Health Information, Credit Reporting and the proposed Biometrics Code of Practice, and would provide a bespoke set of privacy and data ethics safeguards for the CDR framework, based on the IPPs, drafted for easy application in a CDR context.

While we note the potential tensions between the IPPs and the Privacy Act processes, and the concept of the CDR framework, we do not advocate for an entirely separate set of privacy principles for the CDR as is the case in Australia. Having two distinct privacy regimes has led to significant complexities under the Australian regime and this is something that should be avoided in New Zealand. Instead, NZBA recommends that further thought is given to this interaction in the regulations for each sector including by way of issuing a new Privacy Code of Practice (as discussed above in paragraph 24).

78. In addition, clause 52 of the Bill provides that a contravention of an access request will be regarded as interference with privacy, as per section 69 of the Privacy Act. Under section 103(1) of the Privacy Act, the Tribunal may award damages against a defendant for an interference with the privacy of an individual. We note, under section 69(3), the element of harm is not required when an agency breaches IPP 6 and that this aligns with clause 52 of the Bill. The Privacy Act has an open cap on the amount of damages that can be awarded, data holders may be subject to extensive damages. Given that the Bill already contains clauses for fines and damages, for example clause 45 where data holders may be fined if they do not keep records about regulated data service, we therefore suggest the Bill expressly state a damage cap for contraventions of clause 52.

79. Similarly, clause 53 of the Bill provides that a contravention of storage and security requirement will be treated as breaching IPP 5 of the Privacy Act. Breaching IPP 5 will trigger section 69(1) of the Privacy Act, where it is necessary to assess whether the breach has also caused, or may cause harm. Under the Privacy Act, the Office of the Privacy Commissioner (OPC) has the power to investigate and assess the harm caused. Is the intention of the Bill to get the OPC to assess IPP 5 breaches triggered under the Bill? As noted above, the Privacy Act has an open cap on the amount of damages, we therefore suggest the Bill expressly state a damage cap for contraventions of clause 53.

80. We note the complaints process under the Bill is not clear. It does not specify which regulator customers should be complaining to, whether it is MBIE or the Office of the Privacy Commissioner (OPC)? There should be a clear complaints procedure to reduce duplicated efforts (from both the customer and the data holder).

Single Depositor View

81. NZBA recommends 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 the Single Depositor View requirements for the depositor compensation scheme under the Deposit Takers Act and CDR can be made, which MBIE had signalled was its intention in the consultation paper accompanying the Exposure Draft of the Customer and Product Data Bill.

82. 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

Role and powers

83. NZBA notes the proposed role of MBIE as regulator under the Bill, and the Chief Executive's functions in clause 96.

84. NZBA submits that the Bill should go further to provide appropriate direction to the chief executive when undertaking its functions, rights and obligations (including issuing standards and taking enforcement action).

85. In particular, the Chief Executive should be required to act consistently with clear set objectives that include a purpose element. Similar guidance is provided to relevant regulators in (for example) section of the Financial Markets Authority Act 2011, section 4 of the Banking (Prudential Supervision) Act 29189 sections 9 and 10 of the Reserve Bank of New Zealand Act 2021, and section 21 of the Privacy Act 2020). The current functions described in clause 96 of the Bill are extremely broad and do not provide any guidance to the Chief Executive.

86. This could be achieved by requiring the Chief Executive to have regard to certain matters (similar to section 21 of the Privacy Act 2020), such as:

(a) promoting confident and informed participation of data holders and customers in the CDR regime;

(b) having regard to the rights of customers to protection of their data, including Māori customers; and

(c) avoiding unnecessary compliance costs.

87. The Bill should also expressly ringfence MBIE's powers and 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 banking sector frequently engages with MBIE and care should be taken not to adversely affect the level of open, independent engagement as a result of overlap with regulatory roles.

Ability to regulate screen scraping is needed

88. The NZBA also strongly submits that the Chief Executive is given specific powers to deal with screen-scraping. Currently there are no provisions in the Bill that would allow MBIE to regulate screen-scraping. It is important for the proper function of the CDR that screen scraping practices are regulated because it involves the data seeker impersonating the customer, using the customer's access ID and password and knowingly breaching many customer agreements and terms and conditions.

Information-gathering powers represent significant overreach

89. The Bill proposes to provide the Chief Executive with extremely broad information-gathering powers under clause 54, with failure to provide such information constituting an offence under clause 58. This appears to be modelled on similar powers provided to the RBNZ under section 99 of the Deposit Takers Act 2023.

90. However, NZBA submits that such powers would significantly overreach in the context of a CDR. They have been included in the Deposit Takers Act given the RBNZ's need to be able to act quickly and closely monitor deposit takers to support New Zealand's financial stability. Those drivers do not apply to management of the CDR.

91. In addition, we also note the proposal that captured data holders must provide information to the Chief Executive *before* a designation comes into force, if they know "or ought reasonably to know" that such designation would apply to them. Such a deemed knowledge provision is unnecessary and inappropriate, particularly as it relates to knowledge of regulations that are not yet in force.

Dispute resolution

92. The Bill sets out that dispute resolution schemes will play a primary role in managing disputes involving customers, by requiring that data holders and accredited requestors be a member of a dispute resolution scheme (if required by regulation – noting this has been signalled in the Initial Designation/Standards Consultation).

93. NZBA does not consider it appropriate to solely rely on the OPC or dispute resolution schemes for resolving disputes arising in relation to this regime. Both the OPC and the dispute resolution schemes could be overwhelmed with the introduction of the CDR regime and the scope of their operations may need to be reconsidered as a result. NZBA is also concerned that OPC and the dispute resolution schemes may not be equipped to address the unique issues that may arise within the regime.

94. NZBA submits that specific regulator involvement by MBIE will be key in disputes between data holders and accredited requestors, as well as in ongoing testing, monitoring and re-confirming accreditation.[22] NZBA acknowledges that there may be practical limitations to MBIE performing this role without increasing its current resources and would require a separate division in MBIE given the need to separate functions.

Liability regime - general

95. As discussed in the Previous Submission, the Bill needs to have a robust liability regime 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

[22] 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.

provide from time to time. Further detail will then need to be set by regulation for relevant sectors, with the Bill providing guidance on how to achieve this.

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

Liability regime – inclusion of safe harbour

97. We note MBIE's view that it was not necessary to include a "safe harbour provision … to protect participants from liability insofar as they comply with their obligations under the Bill", on the basis that data holders only need to perform actions where they would ordinarily do so in the course of business, and have the ability (or requirement) to decline requests in certain cases.[23] However, this does not acknowledge the inherent risks created by requiring immediate, automated disclosure and action initiation. For instance, while a data holder may perform various actions in their ordinary course of business, this would often involve human initiation, oversight, escalation and training where appropriate. The CDR framework removes these traditional elements and may involve extremely large numbers of varying requests, particularly given the flexibility built into the Bill (as discussed above). In such cases, it is appropriate for relevant safe harbours to be provided to data holders, to ensure that services can be efficiently provided and prevent an overly conservative approach discouraging innovation.

98. By contrast, clause 63 appears to prohibit a data holder from taking action against a customer to recover amounts that may have been paid out to that customer as a result of a contravention of the Bill. This appears to provide customers with a potential windfall gain in such cases, and does not appear to have a strong basis for inclusion.

99. Clause 63 needs to be very closely thought through, where a breach by an accredited requestor creates flow-on effects (for example, where the accredited requestor directs a loan repayment to the wrong account, in circumstances where it cannot then be recovered). An inability to follow up the customer for payment would effectively require banks to consider the credit risk of the accredited requestor (and its insurer) as well as the customer. NZBA submits that clause 63 should be removed.

100. The NZBA is concerned that third party liability has not been explored enough as part of the Bill. If poor conduct arises from third parties than data holders should not be accountable for the third parties' behaviour. For example, there could be fraudulent activity with payment wallets. In such a case, the data holder should not be liable for the third party's actions.

---

[23] Refer MBIE's Response to submissions on the exposure draft Customer and Product Data Bill.

101. We suggest that the Australian legislation provides a suitable approach here. In Australia, if all parties are following the rules, then the Government is responsible for customer redress.

Liability regime – further points

102. Further, as generally discussed in the Previous Submission:

(a) **Proper authorisation**: The Bill should clearly establish that data holders will in no case be liable to customers where they have met and followed CDR standards and rules. This would include where data holders have properly verified the customer and the accredited requestor, where relevant,[24] confirmed the customer's authorisation[25] 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. In the case of banks, much of this data will be historic data stored by the 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 (which details are still to come as part of the regulations and standards), then data holders should not be liable provided they have acted in good faith and have proper processes and systems in place in accordance with the requirements in the Bill and the regulations and standards. In the absence of such a provision, the compliance costs of the regime and the cost for banks (and other data holders) to review all customer data on their systems and ensure it is correctly formatted (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 once the designation regulations are passed[26]) will outweigh the benefits of the regime and slow provision of data. This would align the New Zealand regime with the Australian regime (as described above) where there is general immunity from liability if a data holder performs an action in response to a request in good faith. This is an important safe harbour to include in the Bill to ensure the efficient running of the regime, particular in this area were there are potentially inconsistent duties in place.

---

[24] Pursuant to clause 44.

[25] Pursuant to clause 38.

[26] This, like other details, is to be made by regulations and standards and is not part of the Bill. The NZBA submits that free form text notes on a customer's file should not be within the scope of the Bill when regulations are enacted because some of this information would cross-over to being bank data and potential not formal data at all. It is not appropriate for such information to be included as customer data in the CDR regime.

(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. (While we note this is effectively proposed at paragraph 170 of the Initial Designation/Standards Consultation, this should be reflected within the Bill itself.)

In this regard, we note that paragraph 223 of the Discussion Document accompanying the Exposure Draft 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.

(d) **Steps to avoid loss or damage**: Clause 59 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 126(2)). In its current drafting, clause 59 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.

(e) **Loss of accreditation for poor conduct**: there should be some type of conduct obligation or standard of care applied to the accredited requestor that is expressly set out in the Bill. NZBA submits that there should be a mechanism for an accredited requester to lose their accreditation if they engage in poor conduct, for example misuse of customer data or similar. This could be similar to the duty to treat customers fairly (see the duty in the Conduct of Financial Institutions (COFI) regime for a comparator), act in good faith or a general duty to act in the customer's best interests.

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

Provision of consent

103. 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) and that they clearly appreciate the implications of doing so.

104. 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 38 (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. And yet data holders have the obligation to confirm the authorisation in clause 38 and verify the identity of the person making the request in clause 44. This could be because it is not possible to modify customer consent, and, instead, the customer must replace the earlier consent with a new consent that contains the terms the customer now wishes to be in effect.

105. While these matters are likely to be dealt with in regulations or standards (the Discussion Paper accompanying the Exposure Draft talked 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.

Withdrawal of consent

106. Clause 37 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**.

107. We comment on these approaches below, but in any event the Bill itself should require consideration of the appropriateness of these approaches when setting relevant regulation.

(a) **Time-limited authorisation**: NZBA considers that an enduring consent, coupled with a requirement to periodically remind customers of their authorisation (with the ability to opt-out after a certain time) will typically be more appropriate than time-limited authorisations. This strikes a balance

of ensuring customers remain aware of their authorisations, without adding unnecessary friction and resource requirements.

(b) Where a time-limited authorisation is considered appropriate, NZBA submits that an expiry date of up to twelve months will often be appropriate in New Zealand (similar to common approaches in both Australia and the UK[27]), 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).

(c) **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 accompanying the Exposure Draft. We acknowledge that this is a point for the regulations given clause 37(a) and (b) of the Bill. In this way events-based authorisation could be based on risk or a change in the underlying customer's relationship with the provider – for example, a relationship split may trigger revocation of consent if the construct with the provider changes (for example, joint to single account under a relationship split scenario).

(d) The **time specified by the customer.** NZBA supports inclusion of this limb as an option in relevant circumstances. However, this should be amended to be clear that such customer specification needs to be made in a manner provided in relevant regulation. It will not be practicable to monitor customer specifications unless they can be required to be made in a set manner (for example, within the original consent).

108. NZBA is also 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.

Joint account holders, secondary users and minors

109. Clauses 21 and 24 of the Bill provides 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. The operational considerations behind processes and systems for joint account holders and secondary users can

[27] The UK originally had rules automatically causing consents to expire after three months. NZBA understands that both customers and third parties complained about the short-lived nature of the consent and the hassle to have to extend the consent, and the UK has since changed its rules.

be complex, for example where multiple parties may be required to provide express and informed consent to an action.

110. 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, including in respect of the need for multiple authorisations to provide express and informed consent to an action. We note that this is 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.

111. NZBA notes that the Bill does not specifically propose an approach in respect of the designated data of customers under the age of 18, but that that is supposed to be one of the reasons for the concept of a secondary user. As set out at paragraph 110 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.

Clarity on nature of authorisation

112. Clause 36 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 38 is similarly unclear as to the entity to whom authorisation is given although the example provided at clause 38 appears to suggest that authorisation must be given to the bank as data holder.

113. Amendments to clauses 36 and 38 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.

114. Similarly, the example given at clause 38 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 an enduring customer consent to the provision of specified data to multiple accredited requestors or whether it is expected that customer consent to the provision of data to each specific accredited requestor must be obtained on a case-by-case basis.

115. NZBA considers that a specific customer consent should be required for each accredited requestor. A blanket consent relating to multiple accredited requestors may make it difficult for a customer to revoke consent in respect of a specific accredited requestor but would have the advantage of revoking all consents which could cause less hassle for the customer if that is what they would like to do. Both options could be made available to accredited requestors and consumers in the regulations.

Part 4: Miscellaneous matters

Government fees and levies

116. We expect 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. NZBA agrees that significant investment will be required from banks in order to implement 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.

Record keeping

117. Clauses 45(3)(a) and 46(2)(a) of the Bill require records to be kept for five years. Assuming that no maximum time limit is to apply to authorisations, an authorisation may be given until it is cancelled by the customer and requests based on that authorisation may continue for longer than 5 years. For this reason, 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 46(1)(a) requires records to be kept for each individual data request, or the overarching authorisation provided in respect of each data request.

Required policies

118. Clause 47 of 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) and consideration should be given to whether these policies are appropriate for data holders. Additionally, the Bill should be more prescriptive about what is required from a data policy perspective, to ensure both transparency for customers and to assist accreditation bodies in their assessment process.

Reciprocity obligations

119. NZBA submits that it would be worthwhile considering if there should be some reciprocity obligations introduced into the regime. While the reciprocity rules in the Australian CDR regime have been criticised as discouraging accreditation, we think that the idea is worth exploring further, while learning from the pitfalls of the Australian regime. If New Zealand wishes to create a data eco-system with the introduction of the CDR regime, then it would seem to make sense that data exchange is two way (and not solely one way). It would be a concern if data holders were required to transfer data out of their systems but were not able to take advantage of any enhancement that were made to that data by third parties once the third parties had received the data. The role of the government and whether it

should be required to provide data and be in the ecosystem should also be considered in this context.