New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Ministry of Business, Innovation and Employment

on the

Discussion paper: *Open banking regulations and standards under the Customer and Product Data Bill*

10 October 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

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

Introduction

4. NZBA welcomes the opportunity to provide feedback to the Ministry of Business, Innovation and Employment (**MBIE**) on the Discussion paper: *Open banking regulations and standards under the Customer and Product Data Bill* (**Discussion Paper**).

5. NZBA commends the work that has gone into developing the Discussion Paper, and agrees that further development of open banking in New Zealand could provide benefit to customers. Open banking will empower customers by giving them more control over their banking data, including greater accessibility and the ability to enable sharing of their data between their banks and other organisations.

6. As a general comment, we note that there are three separate, public workstreams currently providing input into the development of a Customer Data Right (**CDR**) regime applying to banks at present, namely:

    6.1. The development of the draft Customer and Product Data Bill (**Bill**) through Select Committee.

    6.2. The Commerce Commission's ongoing investigation into designating the interbank payment network under the Retail Payment System Act.

    6.3. MBIE's ongoing work as captured in this Discussion Paper.

7. NZBA is concerned about the inconsistencies between these various pieces of work – in particular, between the Commerce Commission's recommendation to the Minister and this Discussion Paper.

    7.1. For example, the Commerce Commission notes in its recommendation paper that payments initiation will not be addressed by the open banking regulations and standards, and so will be covered by a possible Commerce Commission designation.[1] Meanwhile, the Discussion Paper expressly notes that payments initiation will be a designated action.[2]

8. This is creating uncertainty and nervousness for industry, given the complexity of the proposed changes that open banking will require. This will likely, in turn, lead to confusion around the roles and responsibilities of relevant entities, regulatory uncertainty and an overly complex compliance burden.

9. We recommend consideration is given to the establishment of a single digital agency (such as the Singapore example) or at least absolute clarity on each agency's

[1] At page six of the Retail Payment System: Recommendation to the Minister to designate the interbank payment network (August 2024)
[2] At paragraph 69.

responsibilities is provided. Further clarity could also be provided by way of roadmaps across the broader, interlinked projects on (for example) payments.

10. The balance of our submission works through the following sections of the Discussion Paper:

    10.1. Status quo and problem definition

    10.2. Objectives

    10.3. The scope of an open banking designation

    10.4. The benefits, costs, and risks of an open banking designation

    10.5. Accreditation criteria

    10.6. Fees

    10.7. The detailed rules for open banking

    10.8. Standards for open banking

    10.9. Further comments

Status quo and problem definition

11. NZBA agrees that the customer data held by banks could be of value to customers, and that open banking is the preferred global solution for bank data sharing.

12. We contest the statement made by MBIE at paragraph 20 of the Discussion Paper, however – this understates the effort that the industry has undertaken in the absence of a government-led framework to govern the rules and regulations surrounding the sharing of customer data. There have already been comprehensive standards developed by banks and third parties due to market demand, opportunity and feasibility. Trust in security and availability/useability is key and that has been a focus of work to date. Without clear criteria for accreditation, use of data and a clear liability framework, conditions for access under the current API Centre scheme are inevitably risk-based decisions.

Objectives

13. NZBA queries exactly how MBIE intends to measure the criteria set out at paragraph 35 of the Discussion Paper and submits that further detail is required. In particular:

    13.1. How is uptake and the value of use cases to be measured prior to implementation of a CDR regime? In our view:

13.1.1. It should be customer uptake and not third-party user uptake that is measured.

13.1.2. A cross functional steering group is crucial to help ensure use cases are properly vetted and prioritised.

13.1.3. The need for meaningful use cases driven by customer demand is key, with appropriate cost/benefit analysis undertaken for each. For example, the recent Natwest and National Australia Bank white paper revealed that two-thirds of use cases in the UK and Australia are payments-related.

13.2. We submit that the API Centre would be an appropriate assessor of efficient investment.

13.3. Other areas for focus should include promoting economic value and minimising barriers to a well-functioning system.

The scope of an open banking designation

Requestor designation

14. NZBA supports the proposal that, in the first instance, only requests by accredited requestors be designated.

15. As captured in our previous submission to the Economic Development, Science and Innovation Committee on the Customer and Product Data Bill (**Previous CDR Submission**), NZBA is concerned about any potential requirement to provide information to, and open systems to, parties beyond accredited requestors at any stage. Any such requesters 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.

16. Such broad 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.

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

17.1. 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 (for example, data obtained during the course of looking to establish a banking relationship where this ultimately did not eventuate) (and, as

discussed below, direct-to-customer data access should not be within scope of the CDR); and

17.2. providing customer data to accredited requestors would be sufficient to allow those accredited requestors to analyse customer data and give effect to the CDR.

18. The Bill contemplates customers 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.

19. In this regard, NZBA supports the position in the Discussion Paper, which proposes that (at least initially) access be limited to accredited requestors only, without extending to direct-to-customer data access and action initiation. However, NZBA considers that direct-to-customer access/initiation should be removed at statute level as well.

20. 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.

21. 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'.[3] 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

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

would require amendments to the statutory framework particularly in relation to liability for loss.

22. Accordingly, we recommend reconsidering the introduction of a direct-to-customer data right at a later point when the CDR has matured. 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. This relates to our broader point that for the relatively small size of the Aotearoa New Zealand jurisdiction we must leverage the lessons from overseas and be measured in right sizing our regime.

Data designation: customer data

23. In respect of customer data, NZBA submits that there should be a 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 and (2) what can be reasonably synthesised into a standardised form for sharing through electronic systems.

24. 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 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.

25. We also submit that offline or closed accounts should be treated as out of scope. Designating offline or closed accounts as in-scope customer data would be significantly costly to enable and implement without providing commensurate benefit.

26. 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).[4] 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.

27. NZBA notes the proposal in paragraph 61 of the Discussion Paper that customer data can be requested for up to seven years. We submit that the existing standard of two years is appropriate for the New Zealand jurisdiction, otherwise compliance costs and

[4] 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.

resulting impacts on system performance to enable access to large data sets could be substantial.

28. NZBA does not support introducing new terms and instead prefers those developed in the existing API Centre Standards. We note MBIE's proposal in paragraph 39 of the Discussion Paper is to utilise the categories of customer data and actions in the Standards but paragraph 56 appears to go further. Our preference is for the initial requirements to align with the mandatory 2.3 Standards and for future standards to be developed with industry.

29. As a general comment on MBIE's designated customer data at Paragraph 56, we note that these extend beyond the current standard set out in the API Centre's Account Information API Standard.

30. NZBA also queries the following:

    30.1. we do not understand the rationale for 'customer number', and note it could for example facilitate fraudulent behaviour.

    30.2. what does 'eligibility' mean? We understand that "a customer's eligibility for services and offers provided by a data holder" means information about services and offers regarding the designated account types, rather than all services and offers. This would benefit from further clarification.

    30.3. in our view 'account name' and 'account type' are unnecessary.

    30.4. are 'payment obligations' referring to scheduled payments?

    30.5. direct debit authorities will likely pose implementation challenges as the authority to debit is between the acceptor and the initiator and involves their respective banks. This means a bank, as a data holder, may not have all of the information required to respond to a requestor.

Data designation: product data

31. NZBA supports the proposition in paragraph 68 of the Discussion Paper that standards need to be developed before any designation for product data comes into force.

32. We note that the Discussion Paper 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.

33. 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".[5]

34. 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).[6]

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

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

    36.1. 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 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", 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

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

37. 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.

38. NZBA submits that MBIE should consider Australia's experience with the wide scope of product data regulation. This proved to be costly and resource intensive for participants to comply with, and the scope of product data regulation in Australia is now being reconsidered.

---

6 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.

39. 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. We further submit that any designation of product data should be consistent with customer data designation – i.e., in-scope products will need to align with customer data regulation.

Action designation

40. NZBA supports the general position in the Discussion Paper to initially focus on matters addressed in the API Centre Minimum Open Banking Implementation Plan. 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.

The benefits, costs and risks of an open banking designation

41. In response to Question 14, NZBA agrees with the benefits listed by MBIE at paragraph 82 of the Discussion Paper (in particular, paragraph 82(c)). Open banking will reduce the need for customers to conduct data sharing activities through insecure methods, such as screen scraping, which should significantly reduce the risk of misuse of banking credentials.

42. In relation to risks from the designation to intellectual property rights in relation to customer or product data (Question 15), we consider there are some risks relating to how derived data is to be classified or treated. If this is, for instance, a credit rating or a loan limit which would be available to the customer, it is probably in scope – but a risk or similar score which is based on a bank’s own specific policies, market strategies and risk tolerances should in our view be out of scope. The same should hold for any predictive measures like the probability of a default.

43. The same set of factors will apply to product data. For instance, in relation to some products, some of our members have “acceptance criteria” which drive an initial assessment of the acceptability or not of an applicant. This is based on a number of factors including risk measures (including the risk of regulatory / AML non-compliance) and things like the potential impact on a bank’s brand. Banks do not typically disclose these criteria and would not support their inclusion in the classification of product data.

44. NZBA notes that paragraph 83 of the Discussion Paper only addresses accredited requestors, but in our view a risk in relation to secondary users remains. Where will liability sit once a data holder has met the consent request from a third party?

45. NZBA again refers to its Previous CDR Submission, in particular to the potential risks raised by conflict with other legislation (see paragraphs 68 – 82). In particular:

    45.1. 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 CDR framework could be unworkable for data holders (see paragraph 70 of the Previous CDR Submission).

    45.2. NZBA proposes that provision is made for leniency in emergency or high stress scenarios or situations where data holders experience an increase in data requests at the same time as experience 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.

    45.3. Overlaps and conflicts with breach reporting, the Privacy Act and the Single Depositor View may also cause risks to the operation of a CDR in the banking sector (see paragraphs 74 – 82).

Accreditation criteria

46. NZBA agrees that there is a significant risk, in the absence of insurance or guarantee requirements, that banks or customers are not fully compensated for losses that might reasonably be expected to arise from an accredited requestors breaching its obligations. In our view, professional indemnity insurance and/or cyber insurance should be required and a part of the cost of doing business for an accredited intermediary.

47. Further, adherence to and compliance with a set of information security standards should form a part of accreditation (as is the case in the cards space with PCI DSS) to ensure a level playing field and consistent application of basic security measures to keep data safe. Additionally, an accredited requestor should be required to notify a data holder when there has been an incident and customer data could be at risk.

48. NZBA agrees with the proposal at Question 25 of the Discussion Paper that an applicant for accreditation demonstrate compliance with its policies around customer data, product data and action initiation as well as with the Act.

49. In response to Question 26, NZBA submits that there should be additional requirements:

49.1. To periodically confirm compliance for entities that do not already have appropriate information security requirements. This could be achieved through an external audit (as is the case with PCI DSS in the cards space).

49.2. To consider the nature of business carried out, or to be carried out, by the applicant.

The detailed rules for open banking

Express and informed consent

50. NZBA supports the proposal at Question 30. Customers should be able to specify what their data will be used for. This will prevent customer data being used for purposes that may not benefit the customer, and encourage customer uptake of CDR; customers will be more likely to use the service if they understand the exact use of their data.

51. Further, and as previously captured at paragraphs 103 – 115 of our Previous CDR Submission:

51.1. 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. 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 or prescriptive as to stifle innovation), may be as important in ensuring the success of the CDR as technical API standards.

51.2. 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. 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.

Customer dashboards

52. We agree with MBIE's proposals to establish customer dashboards for viewing or receiving consent. Customers should be able to efficiently see who and where their data and consent is connected to, and be able to withdraw this at any time.

Joint customers

53. NZBA submits where a joint account requires only one signatory, then either account holder should be able to provide consent to access account information. Likewise,

either account holder should also be able to revoke consent, regardless of which account holder originally gave consent. However, we do not think an account holder should be able to share personal information about the other account holder (such as name, address, or date of birth) without that other account holder's consent.

Payment limits

54. In our view, payment limits should be set individually on a bank-by-bank basis, with no minimum limit imposed. Banks take many data points into consideration when making a risk-based decision about payments. If a minimum limit were to be imposed, this could allow payments to go through that would have otherwise been blocked by a bank's security measures.

Remediation of unauthorised payment

55. NZBA agrees that accredited requestors should remediate banks for unauthorised payments they request. Further, normal customer limits (for instance, individual or cumulative transaction limits) should still apply regardless of how the payments are generated. Normal funds checking and offline limits (if any) should also still apply where online fund authorisation is not available.

Content of the register and on-boarding of accredited requestors

56. We submit that information held by the register should be publicly available. This information is relevant not only to data holders, but customers, as it may play a part in who those customers give consent to.

57. NZBA also submits that express obligations for the on-boarding of accredited requestors is necessary. For example, such obligations should include suitable due diligence on the individuals involved; confirmation of acceptable security / data protection requirements (including policies); notification of cyber breaches; and some requirements to monitor additional requestors to ensure they maintain the same standards.

58. It would be beneficial, in our view, to have a single regulator model for payments and open banking. At present, there are three regulators involved in this work: The Commerce Commission, MBIE and RBNZ (through the designation of payments under the Financial Infrastructure Markets Act). The designation of this area may bring further complexities. It would be beneficial to have one regulator for this area to provide consistency and clarity to regulated entities.

Content of policies relating to customer data and action initiation

59. In addition to the requirements specified in paragraph 180 of the Discussion Paper, we submit that, in developing the open banking regulations and standards, MBIE should

consider the following points for inclusion in the customer data policies of accredited requestors:

59.1. Paragraph 180(b): Whether the storage provider (e.g. cloud provider) is required to protect the data in a way that, overall, provides comparable safeguards to those in the CDR Bill.

59.2. Paragraph 180(c) and (d): The wording “who benefits from each purpose for which customer data is used” is quite broad, as there may be indirect beneficiaries who are not involved in the collection, use or disclosure of the data. NZBA submits that MBIE should consider narrowing this to only specifying who will be directly using or benefiting from the data.

59.3. The process for obtaining express and informed consent from customers, and how the consent can be withdrawn.

59.4. Specify how customers will be informed about changes to the policies, and how they can contact the requestor should they have questions or concerns on how to exercise their rights under the CDR Bill.

59.5. Outline procedures on how data breaches and other security incidents will be handled, and how the notification process will work.

Performance

60. In response to Question 47, we submit that performance standards will likely need to evolve over time, and should therefore be light touch until the regime has matured.

61. Standards should also, in our view, be set at a high level to avoid placing restrictions on participants and stifling innovation. Standards should assess all parties to ensure good customer outcomes and services across the regime.

62. We note the Discussion paper references the Australian CDR traffic thresholds and tiering. We do not believe these were developed with a strong evidence base, and therefore there is risk involved on relying on this approach. It takes time and resource to expand infrastructure and performance capacity. A sudden shift in tiers could be due to a number of reasons such as industry migration from screen scraping, and may not be a realistic reflection of the activity in the regime.

63. On this basis, we submit that performance requirements need to cater for the appropriate transition periods.

Standards for open banking

64. Existing industry standards must be the basis that CDR builds on, and NZBA supports the general approach shown in the Discussion Paper in this regard.

65. 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.

66. In our view, the following additional standards would be beneficial:

    66.1. Prescribed clarity on MBIE's position relating to screen scraping and when it should not be permitted.

    66.2. Enforced ramifications relating to use cases that target vulnerable customers, to avoid any issues in future.

    66.3. Enforced ramifications for misuse of consent or insufficient third party protocols relating to the protection of customer data.

Further comments

Liability and dispute resolution

67. 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.

68. We note MBIE's previous 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.[7]

69. 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.

70. The CDR framework removes these traditional elements and may involve extremely large numbers of varying requests, particularly given the flexibility built into the Bill. In such cases, it is appropriate for relevant safe harbours to be provided to data holders,

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

to ensure that services can be efficiently provided and prevent an overly conservative approach discouraging innovation.

71. NZBA is concerned that third party liability has not been explored enough as part of the Bill. If poor conduct arises from third parties then 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.

72. 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.

73. Please refer to: paragraph 102 of our Previous CDR Submission for further considerations in respect of the apportionment of liability under the CDR regime; and paragraphs 92-94 of that Submission for considerations in respect of dispute resolution and dispute resolution schemes.

74. Some parties, such as fintechs, may not neatly fit within the mandate of the current dispute resolution schemes. An alternative approach could be to set up a single disputes organisation, which has been adopted in Australia with AFCA.

Reciprocity Obligations

75. NZBA submits that it would be worthwhile considering if there should be some reciprocity obligations introduced into the regime in future. 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 enhancements that were made to that data by third parties once the third parties had received the data.