NEW ZEALAND BANKERS ASSOCIATION

Submission

to the

Ministry of Business, Innovation and Employment

on the

Discussion document: Options for establishing a consumer data right in New Zealand

19 October 2020

NEW ZEALAND BANKERS ASSOCIATION
Level 15, 80 The Terrace, PO Box 3043, Wellington 6140, New Zealand
TELEPHONE +64 4 802 3358 EMAIL nzba@nzba.org.nz WEB www.nzba.org.nz

About NZBA

1. The New Zealand Bankers' Association (**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 seventeen registered banks in New Zealand are members of NZBA:
   - ANZ Bank New Zealand Limited
   - ASB Bank Limited
   - Bank of China (NZ) Limited
   - Bank of New Zealand
   - China Construction Bank
   - Citibank N.A.
   - The Co-operative Bank Limited
   - Heartland Bank Limited
   - The Hongkong and Shanghai Banking Corporation Limited
   - Industrial and Commercial Bank of China (New Zealand) Limited
   - JPMorgan Chase Bank N.A.
   - Kiwibank Limited
   - MUFG Bank Ltd
   - Rabobank New Zealand Limited
   - SBS Bank
   - TSB Bank Limited
   - Westpac New Zealand Limited

Introduction

3. NZBA welcomes the opportunity to provide feedback to the Ministry of Business, Innovation and Employment (**MBIE**) on the discussion document: *Options for establishing a consumer data right in New Zealand* (**Discussion Document**). NZBA commends the work that has gone into developing the Discussion Document.

Summary

4. NZBA agrees that an ecosystem which promotes and facilitates data sharing will drive benefits for consumers, businesses, the economy, and NZ Inc.

5. In the context of the banking industry, we believe that open data has the potential to provide customers with new and innovative ways to make use of their banking data. We are supportive of the development of a CDR regime in New Zealand which is right-sized, empowers customers with control and choice over their data, and ensures consumer confidence through appropriate safeguards.

6. The priority should be to ensure that we build a regime that is consumer-centric, furthers an innovative, digital economy and is appropriate for the New Zealand market. It should:

   (a) Be fit for purpose and meet clearly defined, understood and measurable objectives.

   (b) Be designed for local market conditions. It should:

      (i) be built on consumer trust;

      (ii) guarantee privacy and data security;

      (iii) have a strong governance framework;

      (iv) prioritise read access before write access;

      (v) dovetail with a Digital Identity Trust Framework; and

      (vi) ensure that there is reciprocity between data holders and data recipients.

   (c) Utilise and build on existing sector-led initiatives.

   (d) Be compatible with existing legal and regulatory regimes.

7. NZBA's approach in this submission is to comment on those key themes, rather than providing detailed answers to the questions posed.

8. We note also that many of NZBA's members have prepared their own detailed submissions on the Discussion Document, and have met with MBIE bilaterally to discuss their views. Some of our members have also contributed to Payments NZ's submission, Business New Zealand's submission and to the Data Economy Collective's submission.

Objectives and benefits of a CDR

9. We understand and agree with the potential benefits of CDR regimes generally, as outlined in the Discussion Document, being:

   (a) enabling innovation;

   (b) facilitating competition;

   (c) increasing productivity;

   (d) strengthening privacy and data protection; and

   (e) consumer welfare.

10. However, the case for introducing a CDR in New Zealand has not been well articulated in the Discussion Document in terms of its objectives and benefits. We are concerned that the analysis of a CDR's benefits is very high-level and lacking detail. Additionally, little consideration has been given to how the benefits of CDR regimes generally would apply in the New Zealand context specifically. Similarly, the costs/risks of introducing a CDR are described very briefly without any real context or analysis.

11. For that reason, we believe it is essential that MBIE undertakes a more in-depth analysis around the perceived benefits and objectives of a CDR. In particular, we think that it is necessary to:

    (a) Clarify the problem(s) we are looking to solve, taking a consumer-focussed approach.

    (b) Evaluate the current situation and the target state.

    (c) Identify whether any existing legislation, regulation and sector-led initiatives could be used or altered to close the gap between the current situation and the desired target state.

    (d) Consider what else is needed to promote open data, as well as measures of what success will look like in the New Zealand context.

12. We believe this foundational analysis is critical to a successful CDR regime. It would help to answer the question of whether New Zealand needs a CDR, and if so, what form it should take. This may also help to ensure New Zealand does not make the same mistakes as have occurred in comparable jurisdictions. For example, in the UK there has been little evidence that the promised benefits and objectives of a CDR have been delivered on a large scale,[1] despite significant levels of industry investment and resource,[2] and in the context of considerable implementation challenges.

13. We consider that this work should be undertaken with input from a cross-sector advisory group. An advisory group would provide valuable input into the policy making process. It would:

    (a) Allow MBIE to utilise private sector resources, experience, insights and analytics.

    (b) Ensure there is buy-in from those who would be most affected by the regime during its implementation.

    (c) Ensure the benefits and objectives of a CDR are appropriate for local market conditions and would generate advantages for NZ Inc.

[1] In the UK, which is the most advanced in terms of a data portability right, the uptake of Open Banking has steadily grown, but from a slow start, as illustrated by the number of successful API calls made by third party providers (see https://www.openbanking.org.uk/providers/account-providers/api-performance/)

[2] The banking and finance industry has invested an estimated £1.5 billion in infrastructure since the launch of the Open Banking Implementation Entity (OBIE) in 2016, according to UK Finance – see UK Finance proposes next steps for Open Banking, 17 June 2020.

14. NZBA and our member banks would welcome the opportunity to participate in an advisory group set up for this purpose.

Design features of a CDR

15. As discussed above, NZBA strongly believes that more work needs to be undertaken before we can assess whether a CDR is appropriate for New Zealand and, if so, what form it should take. For that reason, we believe it is premature to comment on whether the options presented in the Discussion Document (if any) would be suited to New Zealand.

16. We do, however, have some general comments regarding features of a CDR, which we have set out below. Those comments relate to:

    (a) Consumer awareness and trust.

    (b) Privacy and data security.

    (c) Governance.

    (d) Read/write access.

    (e) Digital Identity Trust Framework.

    (f) Reciprocity.

17. If a CDR is to proceed, we ask that MBIE provides a revised set of options including a rigorous cost/benefit analysis of each. We believe that this too would benefit from the input from a cross-sector advisory group.

Consumer awareness and trust

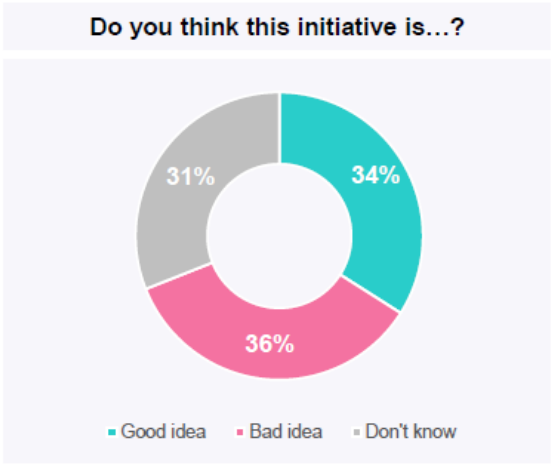
18. Consumer awareness and trust are vital to the success of a CDR. Awareness of, and trust in, the regime will be the foundation of consumer demand. At this stage, we don't think that there is enough awareness of, trust in, or demand for, a CDR in New Zealand.

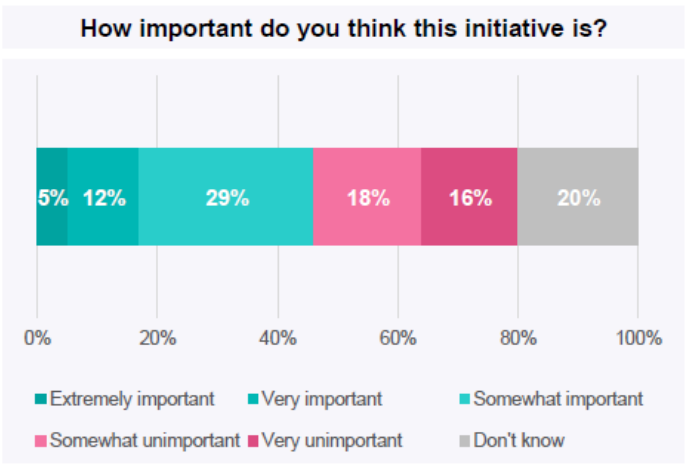
19. If a CDR is to be considered, we would support a consumer awareness campaign to test whether the objectives, benefits, and safeguards resonate with consumers. This could also involve consumer testing, such as focus groups, to ensure that the CDR has the customer at its heart.

20. In March 2020 NZBA commissioned a survey on attitudes to the banking industry in New Zealand.[3] Survey respondents were asked about open banking:

> Open banking will mean that bank customers can choose to share their personal banking data with third parties like payment services or money management services. Personal banking data includes things like account access, balances, transaction history and loan details. Being able to share that information safely with third parties will make it easier for customers to find products or services that suit them as individuals, and make switching simpler.
>
> Do you think the initiative is: good idea / bad idea / don't know
>
> How important do you think the initiative is: extremely important / very important / somewhat important / somewhat unimportant / very unimportant / don't know

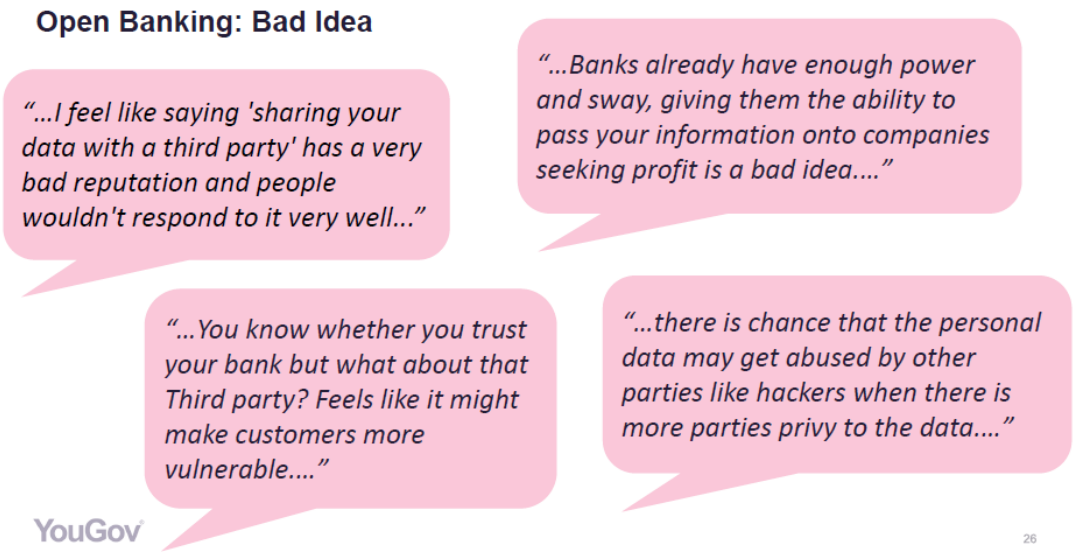
21. Respondents were divided over open banking, with a third saying it is a bad idea and less than half believing it is important to implement:



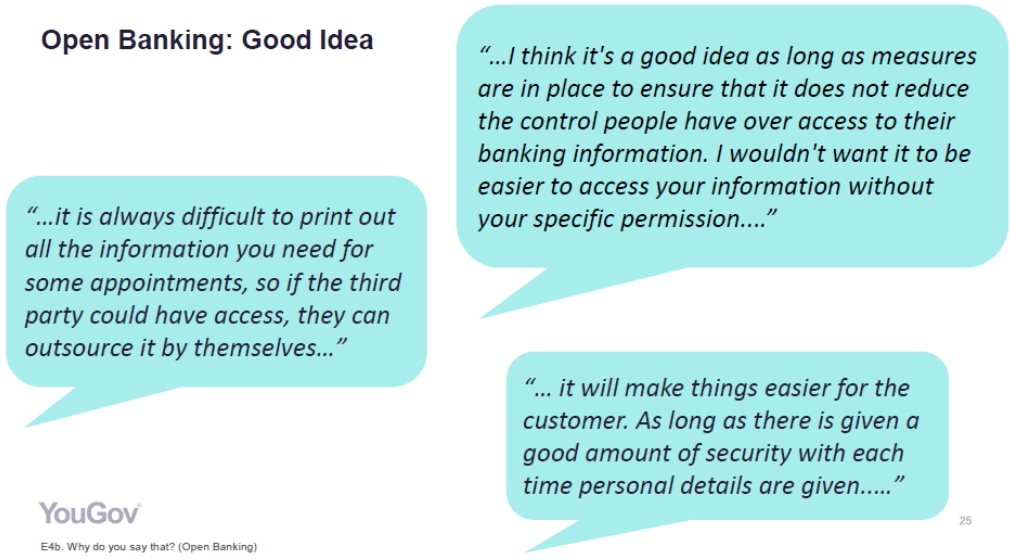


[3] Sample n=1012. Fieldwork conducted online 19-26 February 2020. Quotas were put in place to ensure representativeness and post survey weighting was applied according to latest official population estimates.

22. Qualitative analysis of those who thought it was a bad idea revealed that concerns over privacy and security of personal data are the primary reasons why the initiative is not widely supported at this stage.



23. Those who thought it was a good idea cited ease of transferring information as the key benefit:



24. Research undertaken in Australia shows a similar sentiment:[4]

(a) 48 per cent of consumers surveyed would be willing to share their banking transaction information with a major bank.

[4] Deloitte: Open banking: switch or stick? Insights into customer switching behaviour and trust, October 2019.

(b) Less than 20 per cent would be willing to share that information with a digital bank.

(c) Less than 10 per cent with a technology company.

25. In the UK, which is the most advanced jurisdiction in terms of data portability, the uptake of open banking has steadily grown, but from a slow start, as illustrated by the number of successful API calls made by third party providers.

26. For that reason, we consider that the development of a CDR should be preceded by an awareness raising campaign which tests with consumers:

(a) the benefits it could provide;

(b) the risks it could introduce; and

(c) the safeguards that could mitigate those risks.

27. The outcomes of that consumer testing will be key to understanding whether New Zealand needs a CDR, and if so, what form it should take. Without raising consumer awareness and trust, uptake of a CDR is likely to be low and its objectives will not be met.

Privacy and data security

28. As illustrated by the survey feedback above, privacy and data security need to be at the forefront of a CDR – it is of critical importance to both consumers and industry participants. A CDR regime risks failing if consumers lack trust and confidence that there are appropriate safeguards in place to protect their data. A breach could undermine the legitimacy of the whole CDR regime. It is therefore important that government and the sector take the time to get this aspect right.

29. Accreditation requirements should be proportionate to the level of risk. Different types of data carry different levels of risk. Different risk profiles also apply to different activities – for example, payments initiation vs. read access to transactional data only.

30. As discussed below, Payments NZ and some banks have already done a significant amount of work on the non-technical aspects of API standards, including customer data protection. That work should be leveraged in the development of a CDR's data security development.

31. Finally, the liability framework must be established early on, including its participant scope, and then clearly communicated to all participants. NZBA's view is that accountability for breaches is an important way to incentivise participants to treat customer data with care, diligence, and skill. The liability framework should reflect the harm that could be caused to the customer in the event of a breach, as well as the fact that the reputational impact on the data provider and the CDR regime more generally may be significant and long lasting.

32. The need for an appropriate liability framework will have to be balanced to ensure that it is not so punitive that it has a chilling effect on participation. We think this is another design aspect that would benefit from sector input via an advisory group.

Governance framework

33. A strong governance framework is an essential feature of a CDR regime, and should be an early priority. The governance design of the regime will create the accreditation and liability frameworks, which are also both fundamental to the success of the regime, as discussed above.

34. Governance design will make a material difference to the success of a CDR in New Zealand. It should:

    (a) Encourage positive and balanced interactions between regulators and market participants.

    (b) Avoid creating an interventionist or overly complex framework.

    (c) Ensure legislative clarity, while leaving flexibility to innovate.

    (d) Set clear expectations, especially with respect to accountability and liability.

    (e) Have realistic expectations around implementation timeframes. It will take time to design and establish a CDR regime, create an accreditation and liability framework, build systems and test their functionality.

35. The sectors that a CDR will be applied to are already highly regulated. Care needs to be taken to avoid creating overlaps, inconsistencies, or gaps. For that reason, we think that a cross-sector advisory group, including sector representatives, could provide valuable input into governance design.

36. Our current thinking is that there should be one regulator responsible for the implementation and enforcement of the CDR to ensure clarity and consistency for all stakeholders involved in the process. We have seen from Australia's experience that having multiple regulators involved in the implementation and regulation of the Australian Consumer Data Right – the Office of the Australian Information Commissioner, the Australian Competition and Consumer Commission and the Data Standards Body – has caused considerable uncertainty regarding responsibilities for implementation and/or regulation of particular aspects of the regime. However, given the interplay between privacy, competition, and consumer law, it may be that a single regulator may also pose a different set of challenges.

37. Whichever model is ultimately selected, the key will be to ensure that it is properly resourced to achieve the overall goals (including education, furthering innovation, and enforcement). We welcome the opportunity to work with MBIE on this important point.

Read/write access

38. The Discussion Document proposes that a CDR should provide for both read and write access in order to fully realise the benefits of a CDR.

39. While there is potentially value in write access, this is a significant step-up in complexity, risk, and cost. The accreditation and liability framework, among other things, would need to appropriately reflect these higher risks.

40. We do not think the Discussion Document makes the case for write access. We are concerned that pursuing write access from the beginning is a significant overreach and would be more likely to lead to negative outcomes. A more rigorous cost-benefit analysis is required before this can be considered.

41. It is also important not to underestimate the complexity of implementing a CDR regime with read access only. In Australia, for example, read access was implemented first and write access is currently being considered. Despite that, implementation has been delayed in order to complete testing of systems and security and costs have also been considerably higher than anticipated.

42. We therefore submit that MBIE should follow a phased approach which first focuses on consumers accessing and sharing their readable data, and appropriately reflecting the related risks in the accreditation and liability framework.

Digital Identity Trust Framework

43. The Discussion Document briefly mentions the Digital Identity Trust Framework that has recently been approved for development by Cabinet.

44. A Digital Identity Trust Framework will benefit consumers by enabling user-initiated digital identity information sharing. It will streamline banks' obligations under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (**AML/CFT Act**) and simplify their Know Your Customer processes. It will facilitate more efficient onboarding and switching.

45. The inclusion of identity data within the scope of a CDR regime is likely to support the development of numerous CDR use cases. These two government initiatives should dovetail to ensure the Digital Identity Trust Framework can meet the needs of a CDR, if developed.

Reciprocity

46. Reciprocity of data sharing is critical to avoid an asymmetry between the obligations on data holders and data recipients.

47. If big tech data holders (eg Google, Facebook) are able to obtain large volumes of additional data they will be at a significant competitive advantage.

48. Other companies (eg smaller fintechs, banks) should also be able to receive consumer data from these companies, if directed to do so by the consumer. That will allow all players in the data economy to harness all available data and compete based on their product and service offering.

49. A lack of reciprocity undermines consumer choice and creates an environment where competitive constraints are placed unequally on providers competing in the same data economy. A lack of reciprocity reduces the ability of all providers to harness the same data sets and compete, via their insights and analytics to make innovative products and services, thereby maximising benefits to consumers.

50. Reciprocity should not create a barrier to entry for smaller players, so consideration could be given to a phased approach, or an exemption process for small business, fintech, and start-ups.

Utilisation of existing sector-led initiatives

51. The Discussion Document refers to a number of sector-led initiatives and notes that they "do not appear to be delivering the full range of positive outcomes for consumers as yet". By way of example, the Discussion Document refers to bank switching in New Zealand as still having high search and switch costs.

52. In our view, banks have been leaders in the field of data portability – both at industry level and at brand level. There has been significant investment and innovation occurring notwithstanding the absence of a CDR framework. We believe that a CDR should build on and complement those existing sector-led initiatives rather than replacing them.

53. In particular, the banking industry has led on:

    (a) an initiative that supports customers to switch banks easily; and

    (b) payments-related innovations via standardised APIs.

Bank switching initiative

54. In New Zealand, switching banks is safe, easy, and among the fastest in the world. A customer's new bank can take care of everything in five working days – they will manage the entire switching process and the account will move from the old bank to the new bank along with all payment instructions. That is facilitated by Payments NZ's account switching rules.

55. We would like to understand MBIE's concerns regarding bank switching. Particularly, whether there are aspects of the process that are not working as they should from a customer perspective. If that is the case, NZBA, Payments NZ, and member banks can work together to address those issues.

Payments-related innovations

56. A number of NZBA's members have been involved in the development of payment-related API standards via the Payments NZ API Centre.

57. Payments NZ recently launched v2.0 of the two API standards which relate to payment initiation and account information. The v2.0 standards continue to promote ecosystem efficiency, safety, security, and innovation. They leverage the latest UK open banking standards which enables Payments NZ to streamline development, incorporate best practice and international methodologies, and ensure the standards are tailored to fit local market and conditions.

58. In addition to their work implementing the technical API standards, API providers have been working on the non-technical aspects which are needed to enable innovation and make open banking safe for consumers. That includes the bilateral agreement model, development of a common process for on-boarding of third parties, digital identity, security, customer data protections, customer consent and data management requirements.

59. We note the concerns raised by Minister Faafoi in his December 2019 open letter to API providers regarding the scope and pace of progress implementing Payments NZ's API standards. API providers have taken that feedback on board and, prior to the disruption caused by Covid-19, many were on track to deliver v2.0 within the timeframes set by the API Council. Unfortunately, implementation is now expected to be impacted as a result of Covid-19.

Existing legal obligations

60. The implementation of a CDR in New Zealand is an important development. It will be crucial to try to avoid or manage regulatory overlap. There is a risk that a CDR might create tensions with banks existing legislative obligations, for example under the:

    (a) Credit Contracts and Consumer Finance Act 2003 (**CCCFA**);

    (b) Financial Services Legislation Amendment Act 2019 (**FSLAA**);

    (c) AML/CFT Act.

    (d) Privacy Act 2020.

61. By way of example:

    (a) The CCCFA requires lenders to act responsibly when offering credit products. Having third parties digitally intermediating the product opening process could complicate the bank's obligations under that legislation.

    (b) Similarly, the regulation of financial advice has recently been reviewed and updated by way of FSLAA. Having third parties digitally intermediating the provision of financial advice about banking products and services would

also be likely to complicate the bank's obligations. For example, advice about what type of bank account to open, which KiwiSaver provider to use, etc.

Next steps

62. We are happy to discuss this submission or provide any further information. We reiterate our support for a cross-sector advisory group to input into the development of a CDR in New Zealand.

Contact details

63. 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

Olivia Bouchier
Policy Director & Legal Counsel
olivia.bouchier@nzba.org.nz