



19 October 2020

Consumer Data Right Project Team  
Commerce, Consumers and Communications  
Ministry of Business, Innovation & Employment  
PO Box 1473  
Wellington 6140

By email: [consumerdataright@mbie.govt.nz](mailto:consumerdataright@mbie.govt.nz)

ASB Bank Limited  
PO Box 35, Shortland Street  
Auckland 1140, New Zealand  
Telephone +64 9 377 8930  
Freephone 0800 803 804  
CX10087 Auckland DX Sort  
**asb.co.nz**

A member of the  
Commonwealth Bank  
of Australia Group

### **ASB response - Consumer Data Right discussion document**

ASB Bank Limited (ASB) welcomes the opportunity to provide feedback to the Ministry of Business, Innovation & Employment (MBIE) on the Consumer Data Right (CDR) discussion document.

Our key submissions on the discussion document are set out in the enclosures to this letter.

We acknowledge that ASB's submission may be published on MBIE's website and may be released in response to a request under the Official Information Act. ASB does not seek confidentiality for any aspect of this submission, other than my direct contact details below.

We have also contributed to the New Zealand Bankers Association, Payments NZ and Data Economy Collective submissions on the discussion document and endorse the points made in those submissions.

If you require any further information in relation to this submission, please do not hesitate to contact me.

Yours faithfully,

**Sam Kelly**  
Head of Government Relations & Regulatory Affairs  
**ASB Bank Limited**



---

## ASB's perspective on a Consumer Data Right

---

### Introduction

1. ASB is supportive of the aims of a CDR, being improved consumer welfare through greater choice and control over their data, and economic development through growing the digital economy. From a banking perspective, we see this as an important extension to the data initiatives we have been supporting for some time - including on-going improvements to managing the privacy of our customer's data; sharing that data on request (as ASB has done with Xero and the bank switching initiative); and implementing digital identity practices to support Know Your Customer (KYC) and Anti Money Laundering (AML) regulation.
2. In relation to the introduction of a CDR in New Zealand, we advocate:
  - Greater collaboration between Government and key stakeholders to better define the problems and potential solutions to ensure a sound basis for policy decisions.
  - That the development of a CDR is considered in light of:
    - a clear consumer focus, alongside a consumer awareness program to encourage uptake
    - the specific features of New Zealand's regulatory settings and market developments
    - existing New Zealand data and privacy initiatives,
    - principles that will help foster competition and innovation, and
    - lessons that can be learned from overseas in relation to governance and implementation of data rights.
3. These points are further detailed below, and in our responses to the discussion document questions.

### Collaboration to identify problems and solutions

4. To ensure we achieve the best possible outcome for New Zealanders and New Zealand, ASB believes a detailed outcomes and cost/benefits analysis should be undertaken, prior to any formal policy decisions being taken on a CDR. We would welcome government and private sector collaboration on this.
5. We believe this work is critical, as similar data right initiatives overseas have required significant levels of industry investment and resource<sup>1</sup> and presented considerable implementation challenges, but as yet, perhaps unsurprisingly, given the relative immaturity of many CDR regimes, there is little evidence that promised benefits and outcomes have been delivered on a large scale.<sup>2</sup> In the current economic climate, it is especially important that such a potentially significant initiative is fully considered, before any wide-scale investment and effort is undertaken.
6. We recommend continuing with industry-led work already underway to maintain momentum while this foundational work on CDR is carried out. We would also welcome clarity on the next steps for the policy process, which we hope will include the opportunity to submit via a second discussion document, once further foundational work has been completed.

---

<sup>1</sup>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

<sup>2</sup> 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/>)

### **Key considerations for a consumer data right**

7. Should a CDR be introduced, international developments and the experience of other jurisdictions in implementing their open data agenda provide valuable insights for the design of data sharing regime for New Zealand, but we must also recognise New Zealand's unique regulatory and legal frameworks, and market-specific developments.
8. Key learnings from overseas include the need for clear consumer focus, alongside a consumer awareness program to encourage uptake; practical implementation timeframes; and a combination of regulatory and market driven approaches. Considering this and leaning on the recent experience of our Commonwealth Bank colleagues in implementing the Australian CDR, we set out below, the following elements as being crucial to support a successful regime.

#### Consumer benefits, safeguards, and awareness

9. The benefits and potential detriment to consumers alongside safeguards should be well considered. In short, a CDR should be consumer focused. Introducing a CDR has the potential to improve privacy outcomes for New Zealanders by providing individuals with new ways in which they can use their personal information to their benefit. However, there are also privacy risks associated with the proposed change. Data portability will inevitably lead to more third parties having access to individuals' personal information. This increases the risk of data breaches which can cause serious harm, especially when sensitive financial information is involved. It will be crucial that Privacy by Design and Security by Design practices are adopted when designing and implementing any proposed mechanism for sharing.
10. One addition to the proposal that would improve the potential consumer benefit associated with the introduction of a data portability right would be an accompanying ban on screen-scraping and other unsafe technologies that are currently being used to facilitate third party access to customer data.
11. The introduction of any new consumer rights in respect of their data, should be accompanied by an awareness raising campaign about the rights and the benefits it provides consumers, as well as some of the risks that it could introduce. Without raising consumer awareness, adoption and uptake of the new right is likely to be weak and many of the heralded benefits will go unrealised.
12. ASB supports collaborative efforts between the industry (either through a combination of industry bodies like NZBA, Payments NZ or the recently formed Data Economy Collective), government and the Privacy Commissioner to inform and educate customers and businesses on data sharing e.g. how consents work, to build up trust through practice and experience.

#### A regime fit for New Zealand

13. While ultimately, interoperability and alignment with overseas data rights is likely to be desirable to ensure a free flow of data between countries and reduced compliance burdens, the priority in the development of a CDR regime should be to ensure that we build the regime that is right for NZ; i.e. is compatible with existing legal and regulatory obligations; appropriate in the context of local market conditions in NZ and which most effectively achieves the Government's unique CDR objectives.

#### Alignment with existing initiatives

14. There is already significant investment and innovation occurring in NZ to support data portability, without a formal CDR framework. Since first conceived around two years ago, the API Centre has been designed, established, and has delivered foundational API standards together with a roadmap of next priority features. While progress has been slower than hoped

for, we are of the view that where industry frameworks such as these are currently being developed these should be given leeway to develop alongside CDR proposals.

15. As we note in our response to question 1 below, trust in the participants (both data holders and accredited third parties) is key and the government's Digital Identity Trust Framework is likely to play a vital role in building this trust. ASB considers it crucial that any CDR is coordinated and aligned closely with the Digital Identity Trust Framework to enable greater data portability.

Fostering competition and innovation

16. To optimise the competition and innovation benefits of any new regime, there should be clear incentives for existing market players as well as new entrants to participate. ASB is firmly of the view that any CDR's data sharing framework should be based on principles of safety, security and reciprocity.

Governance and implementation

17. In terms of governance and regulation, we are open-minded as to the best approach, noting that the CDR framework is likely to sit across NZ's competition, consumer and privacy laws, and potentially beyond them; but it is important that governance of the CDR is clearly established in the early stages of its development. We have seen from Australia's experience that having multiple regulators involved in the governance and regulation of the Australian Consumer Data Right (ACDR) has caused uncertainty regarding responsibilities for implementation and/or regulation of particular aspects of the ACDR regime.
18. Experience has shown that many jurisdictions have underestimated the complexity and scale of consumer data portability initiatives, leading to sub-optimal outcomes. We therefore recommend that MBIE considers a staged approach and practical timelines for any potential CDR given the significant lead times for implementing technology reforms of this kind.

## Responses to discussion document questions

### Does New Zealand need a consumer data right?

1

*Are there any additional problems that are preventing greater data portability in New Zealand that have not been identified in this discussion document?*

We have made some observations below in relation to enabling greater data portability.

There is already significant investment and innovation occurring in NZ to support data portability, without a formal CDR framework. Since first conceived some two years ago, the API Centre has been designed, established, and has delivered foundational API standards together with a roadmap of next priority features, with API Providers on track to deliver APIs for commercial use over the next year. With that in mind, New Zealand's progress to date compares favourably with the UK and Australian Open Banking implementation timeframes.

Notwithstanding this, the current environment for developing an open data ecosystem is challenging. API providers are operating within unprecedented regulatory compliance programmes that draw heavily on the same scarce internal specialists required for their API delivery projects. Furthermore, progress on delivery of open APIs and associated commercial framework has been muted since the advent of the COVID-19 pandemic in March. ASB priorities, for example, have necessarily shifted to supporting customers in this crisis.

However, we are strongly of the view that where industry frameworks are currently being developed these should be given leeway to develop without additional regulatory burden hampering them.

Consumer concerns about privacy should be well-understood, so that these can be addressed in the development of a CDR regime – otherwise mechanisms for data portability may have little take-up and use by consumers, which in turn would disincentivise innovation. Adoption of Open Banking in the United Kingdom was slow in part because consumer trust and awareness were low for the first 12 months. Last year, Deloitte released research showing a similar sentiment in Australia:

- 48 per cent of consumers surveyed would be willing to share their banking transaction information with a major bank;
- Less than 20 per cent would be willing to share that information with a digital bank; and
- Less than 10 per cent with a technology company.<sup>3</sup>

We believe that trust is crucial for the success of a CDR. The discussion document briefly mentions the Digital Identity Trust Framework that has recently been approved for development by Cabinet. Trust in the participants (both data holders and accredited third parties) is essential and the Digital Identity Trust Framework is likely to play a vital role in providing consumers with confidence that the participants with access to their data have appropriate processes and controls in place to keep their data safe. It is therefore important

---

<sup>3</sup> Deloitte: [Open banking: switch or stick?](#) October 2019

these two government initiatives are closely aligned and coordinated to enable greater data portability.

---

*Do you agree with the potential benefits, costs or risks associated with a consumer data right as outlined in this discussion document? Why/why not?*

---

The table provided in the discussion document provides a very high-level guide around the potential benefits and costs associated with establishing a CDR. We believe a rigorous investigation of the policy problems and solutions, and a robust cost-benefit assessment should take place if there is a decision to proceed with a CDR in New Zealand. Below, we have set out points for consideration under each of the benefits, costs and risks identified.

#### Competition and Innovation

ASB agrees that greater data portability can facilitate competition to enable innovation and the development of new products and services. However, to optimise the competition and innovation benefits of any new regime, there should be clear incentives for existing market players as well as new entrants to participate. To facilitate this, we firmly believe that any CDR's data sharing framework should be based on principles of safety, security and reciprocity. Participants seeking access to consumer data should be prepared to (i) meet high levels of operational integrity and (ii) be prepared to share data when requested by consumers.

Providing greater volumes of consumer data from across industries would provide greater incentives to consumers to participate in a CDR regime, resulting in greater business and consumer take-up. We believe the principle of reciprocity is key to creating a 'network effect' to quickly advance the successful implementation of any CDR. The principle of reciprocity should ensure that those receiving data and benefitting from the regime are also subject to its obligations to share data, if directed to do so by consumers. There would be significant benefits for consumers if they were able to choose to share their data from one company to another, however under MBIE's preferred sector-designation approach, there might be no incentive for companies in non-designated sectors to enable this consumer benefit.

Furthermore, reciprocity of data sharing is critical to ensure New Zealand businesses can remain competitive in the digital economy and to avoid an asymmetry between the obligations on data holders and data recipients. For example, a lack of reciprocity for non-designated sectors might adversely impact the ability of New Zealand businesses to compete with international tech giants who could access CDR data sets but are not required to share their own data sets. This would allow these businesses to consolidate their position and practices as data companies by overlaying their existing data insights and analytics while the lack of reciprocity would limit the ability for data holders in New Zealand to compete on a level playing field. We believe that all participants who are prepared to ingest consumer data through any New Zealand CDR regime should be required to reciprocate, irrespective of whether those entities are within a designated sector. The principle of reciprocity will enable greater competition and ensure all participants are incentivised to deliver the right outcome for consumers.

#### Increased Productivity

ASB agrees that data portability has the potential to enable some consumer productivity gains by reducing search and switching costs, although we note that the work to quantify the potential cost savings that a CDR could deliver to New Zealanders has yet to be undertaken. While regulation in the UK introducing Open Banking has led to pockets of innovative new third party services, it has not had the impact or delivered the level of benefits anticipated

by its advocates. That said, improved access to data can improve the visibility that consumers have of the various products available to meet their needs, and the relative costs and benefits of those competing products. A CDR will give consumers greater control of their data held by their existing service providers, enabling the delivery of new services, increasing transparency and delivering more choice and competition among products. For example, in banking, there are potential productivity benefits from making headline product information such as published interest rates and terms and conditions available in a standardised, easily accessible form. New market entrants will be able to create business models leveraging this data, enabling consumers to compare product offerings with increased accuracy. The quantum of productivity benefits available to consumers however will depend on the specific characteristics of those sectors that are designated (e.g. existing switching practices and rates, the elasticity of demand, etc), and quality of solutions delivered to consumers (the extent to which they solve real customer pain points, ease of use, value proposition, etc.)

We recognise that further work needs to be done to determine the best way to enable consumers to switch products and providers within a CDR regime and ensure appropriate controls are in place to minimise associated risks. Importantly, any model for switching needs to ensure consumer protection remains the core principle of the CDR regime. We would recommend that in instances where it has been found that switching has occurred improperly, consumers should be able to reverse the action without being disadvantaged. To enable safer switching for consumers under a CDR, appropriate controls will need to be introduced to manage the combination of read and write access required.

#### *Strengthened Privacy and Data Protections / Increased Security and Privacy Concerns*

ASB agrees that a CDR framework could provide more protections than data sharing through some current techniques such as screen scraping. However, as MBIE has noted, as consumer data is shared more widely and with an increasing number of parties, there are increased risks of data breaches and increased complexity regarding the certainty of where liability rests.

It will be important then, if New Zealand is to adopt a CDR framework, that robust accreditation, privacy and consent, and redress frameworks are established from the outset. Any write access right will amplify the need for strong security and data protection risk mitigation. With this in mind, we believe that introducing write access in the initial phase introduces unnecessary complexity and risk, and therefore recommends it be introduced in a subsequent phase of implementation. See our further comments on this below.

Should a CDR be introduced into New Zealand, and once it is active and able to facilitate safe data sharing in the economy, we urge that unsafe data sharing practices, such as screen scraping, be prohibited, as these practices co-existing will cause consumer confusion and may increase the level of unsafe credential sharing. Ensuring customer data can only be accessed through the CDR in a manner that puts consumers in control and provides them with both privacy and financial protection will be critical to ensuring both uptake of the regime and the reduction of poor customer outcomes that result from non-permissioned use or inadequate operational processes.

#### *Consumer Welfare*

ASB is supportive of any CDR reforms that result in New Zealand and New Zealanders being genuinely better off. This will mean that any new regime must ensure that solutions provide consumers the productivity benefits associated with greater access to data without increasing their exposure to misuse or mishandling of data. To achieve this, reforms must be designed with a view to raising consumer awareness and place consumers in control over access to their data.

Building consumer trust and confidence will be critical for realising the potential benefits of a CDR. Low consumer awareness has been a barrier to uptake in other jurisdictions. For example, a year after Open Banking was introduced in the UK, a survey suggested only 5 per cent of the public understood the initiative.<sup>4</sup> This lack of understanding and confidence undermined the UK Government's efforts to introduce an effective data sharing regime. ASB would encourage MBIE to ensure that a New Zealand data sharing regime emphasises education for consumers on the use and proposed benefits of the regime to increase confidence in the system. ASB is already taking proactive steps to elevate customer understanding of safe data sharing practices, based on lessons from industry best practice.

#### Implementation Costs

As recognised by MBIE, a CDR regime will come with significant implementation costs, particularly for data holders. CDR delivery commitments will compete for resources with other regulatory compliance obligations. Ongoing compliance is also likely to be expensive and require a diversion of resources away from delivering customer value in other areas.

As noted at paragraph 18 above, experience has shown that many jurisdictions have underestimated the complexity and scale of CDR implementation. For example, only four of the UK's largest account providers were ready by the date mandated to launch their Open Banking initiatives and have continued to miss deadlines for ongoing delivery of Open Banking functionality. In Australia, the ACCC pushed back the timeline for implementation of the sharing of bank data under the ACDR from February to July this year, in order to complete sufficient testing of systems and security.<sup>5</sup> Strong collaboration and co-operation across industry and regulators will therefore be necessary to agree on practical implementation timeframes, and to facilitate appropriate planning and sequencing of multiple technological changes.

This planning will be particularly important for the banking sector, given the likelihood it will play an early role in CDR. The New Zealand banking industry is currently facing unprecedented demands that should be taken into consideration, including major regulatory projects such as implementation of the Reserve Bank's Capital Review requirements, and preparing for both a new financial advice regime, and new responsible lending requirements born out of the review of consumer credit law.

Any CDR implementation will need careful consideration and planning to ensure that costs relative to benefits are well understood in advance, and that investments are targeted at areas where benefit realisation is both likely, and sufficient to warrant the cost and effort involved.

#### Barriers to Entry

A CDR regime will require wide-scale adoption across multiple sectors if it is to realise the potential benefits for New Zealand and New Zealanders. It is important therefore that any regime is designed and implemented in a way that minimises barriers to entry for businesses. Accreditation criteria could create significant barriers for businesses wanting to participate as data recipients, whereas implementation complexity could create cost barriers for businesses that hold and are required to share data. Some sectors and business are better placed to deliver data portability than others. Some already have data work streams underway, whereas others have much more to do to prepare.

---

<sup>4</sup> Lucy Warwick-Ching, 'Open banking: the quiet digital revolution one year on', The Financial Times, 11 January 2019, <https://www.ft.com/content/a5f0af78-133e-11e9-a581-4ff78404524e>

<sup>5</sup> <https://mailchi.mp/accc.gov.au/update-to-cdr-timeline-announced>



Designing and implementing a CDR regime that lowers barriers to entry will be crucial to drive uptake, but this must be balanced with ensuring that the system overall and individual participants seeking access to consumer data meet high levels of operational integrity, security and data protection standards.

3

*Are there additional benefits, costs or risks that have not been explored in the above discussion on a consumer data right?*

While a sector-designation approach to CDR has merits, it also risks a fragmented ecosystem being developed that lacks data interoperability between industries that inhibits inter-sector innovations. Any CDR framework will need to be designed with this in mind. Furthermore, a regime in which only certain sectors are designated, and therefore where some businesses are subject to CDR legislation and others are not, could inadvertently create opportunities and loopholes for businesses to gain advantage from 'data arbitraging'.

The data portability right may lead to better outcomes for consumers, but there are risks that it could detrimentally impact certain groups as well. The consultation document does not appear to provide a clear view of how the proposed CDR, on balance, benefits consumers. This is partially illustrated by the fact that consumer benefit is not included in the assessment criteria for the proposed options. ASB is also mindful that while a CDR could create opportunities for consumers to benefit from new and improved service offerings, it also has the potential to exacerbate economic inequality and financial exclusion for vulnerable consumers through increased customer profiling by businesses. Any CDR design will therefore need to carefully consider how to avoid further marginalising these consumers.

4

*What would the costs and benefits be of applying the consumer data right to businesses and other entities, in addition to individuals?*

We think it makes sense to ultimately apply a data portability regime equally to any end user of a product or service whether that is an individual, business, or other entity. Implementation complexity however brings risks and costs, so we support taking a staged delivery approach with practical timeframes to allow data holders to deliver data portability for less complex customer categories first (e.g. individuals, small businesses), before bringing more complex categories of customers onboard (e.g. joint signatory accounts, more complex businesses). This will simplify the initial implementation and reduce delivery risk for data holders, while building trust and familiarity in the CDR framework among customers to grow adoption. The distinction between simple and complex categories of customers should largely depend on the complexity of customer consents and authorisations required.

The two sectors that are being targeted for early implementation of the CDR (banking and electricity) both commonly hold information that relates to multiple consumers (e.g. joint bank account data and electricity information that involves personal information about all occupants of a building). These accounts may also contain information about third parties (e.g. the fact that an individual's parent regularly deposits money into their child's account includes information about both the parent and child). There are privacy risks associated with disclosing joint information and information about third parties without the consent of all individuals involved. There will need to be clear guidance on controls that should be implemented to mitigate these risks. One option may be to introduce restrictions on the use of data that relates to parties that have not provided informed consent.

We note that former customers and minors are excluded from the Australian CDR regime. There is significant complexity to verifying a former customer's identity and enabling the sharing of former customer data would add significant costs for data holders, while only

providing marginal benefits. The risks of participation for minors, such as data exploitation and unfair outcomes from profiling, were considered to outweigh the benefits in the Australian CDR.

ASB is supportive in principle of broad inclusion of customer categories in any CDR regime, but recommends that where it makes sense, some categories are excluded, or brought into the regime after the initial phase.

5

*Do you have any comments on the types of data that we propose be included or excluded from a consumer data right (i.e. 'consumer data' and 'product data')?*

MBIE notes that a CDR will apply to information relating to a particular consumer that is the end user who purchases a good or service from a supplier, and a CDR should incorporate information about products or services offered to consumers by a business.

ASB agrees with MBIE's initial view that data created by a data holder through the application of insights and analytics ("Enhanced Data") should be out of scope for a CDR as this is typically commercially sensitive and generated through proprietary means in which the data holder has invested. If enhanced data was to be included, data holders would be disincentivised to invest in data analytics and insights which will ultimately result in reduced innovation, and therefore poorer outcomes for consumers.

Careful consideration will need to be given to the extent that historical consumer data is made available under a CDR. A workable balance will be required between the potentially significant costs to data holders required to make historical data available (much of which will be stored in forms that do not conform with the CDR's standards), and the value to consumers in having access to their historical data. Other jurisdictions have approached this balancing task by including an initial holding date for in-scope CDR data, which then grows organically over time as data holders build historic data in standard formats and convert historical data to digital form. ASB recommends this as a sensible approach to any New Zealand CDR framework.

It makes sense for a CDR to include provision of product data to parties to aggregate and deliver comparison services where that promotes competition and improved customer switching. In some sectors, products are sold that are largely homogenous, with variations in price and terms, and these are ideally suited for inclusion under a CDR. But other services are more bespoke, or bundled with ancillary services, and these will be difficult for both data holders to provide, and data recipients to extract value. Given that there is sector-by-sector variation in the potential value to be derived from product data, ASB recommends the product data to be included in scope for any CDR be determined as part of the sectoral designation process, to ensure that the product data most likely to enable improved customer outcomes and competition, is prioritised in the CDR implementation in that sector.

In any CDR, identity data considerations should align with the existing digital identity work streams that are currently underway at the Department of Internal Affairs, and subject to the terms of the new Digital Identity Trust Framework. This will enable innovative new use cases where third parties are able to rely on AML / KYC data from the banks to enhance authentication and mitigate fraud.

6

*What would the costs and benefits be of including both read access and write access in a consumer data right?*

The inclusion of write access has the potential to drive economic benefit for consumers and the New Zealand economy, but would need to be carefully managed to minimise the privacy,

fraud and financial risks to consumers, particularly those most vulnerable. Strong controls must be developed to ensure the system cannot be utilised to fraudulently access consumers' information, financial facilities and savings.

Given the complexity and material risks of introducing write access into a CDR, careful consideration of the security measures, controls, technical standards and consumer protections is needed for write access to deliver the potential benefits outlined in MBIE's paper. ASB recommends that write access not be considered for inclusion in the first phase of any CDR as this will make delivery significantly more complex, and impact timeframes.

To ensure the successful introduction of write access, the following key components will be required:

- Ensuring consumers are dealing with trusted entities by introducing a higher tier of accreditation that requires specific standards and obligations of entities seeking to use write access, given the potential fraud risks for consumers.
- Controls including multi-factor authentication and confirmation notifications (e.g. warning messages), and the extension of existing refusal to disclose exemptions for data holders to include refusals to give effect to write access where the data holder considers this to be necessary to prevent physical or financial harm or abuse.
- Point-in-time multi factor authentication, aligned to industry best practice, for particular high-risk instances/ changes to account data such as making new payments and adding new beneficiaries.
- To ensure consumers have appropriate recourse for loss or misuse of CDR data, onus must be placed on data recipients accredited for write access to investigate and, where appropriate, remediate and/or reimburse any loss to consumers arising from use of their services. Data recipients should not be permitted to contract out of, or limit, liability to consumers for losses arising from their platform.
- This liability and accountability framework should be supplemented by technical standards that include standard patterns and chains of trust for non-repudiation of write access instances. For example, if a write access action was later disputed by the consumer, non-repudiation standards would provide evidence for the dispute resolution process to determine if the write access occurred due to a failure by a data recipient to adhere to the CDR Rules.
- The development of a robust, standardised approach for collecting consumer consent and API calls for write access. A robust consent solution will be required to enable a non-repudiation mechanism and enable data recipients to securely communicate consent details with data holders, improving the likelihood of identifying potential attacks and malicious activities. Further, the introduction of more granular and precise consents will be a prerequisite for write access. We support the development of technical standards that align with existing industry best practice for fraud and cyber monitoring, detection and action measures.
- Accountability for end-to-end security of the CDR ecosystem residing with the regulator, with regular independent security reviews of the ecosystem as standards change and new use cases are introduced.

We note there may be other data fields that could be enabled for write access, for example, preferences. In these instances, we make the following recommendations:

- At a minimum, an additional validation or authentication step in the consent and authorisation flow be required (e.g. multi-factor authentication)
- Introducing additional controls, such as time delays before any change is given effect, providing data holders, data recipients and the consumer the opportunity to detect fraudulent changes.
- The CDR rules should allow data holders to approach these requests in line with their existing approaches for handling such requests.
- Allowing data holders to apply additional security mechanisms they consider appropriate to protect consumers.

We recognise that write access enabling third parties to initiate payments on behalf of consumers, with the consumer's consent has the potential to lessen friction in payments and facilitate a range of use cases to address issues raised by MBIE in respect to retail payments. In recognition of these potential benefits, the payments industry, via the API Centre, has developed a standard payment initiation API specification that banks are currently building to. A number of third parties have expressed strong interest in utilising this API once available to deliver new payment choices to consumers.

#### What form could a consumer data right take in New Zealand?

7

*Do you have any comments on the outcomes that we are seeking to achieve? Are there any additional outcomes that we should seek to achieve?*

ASB agrees with the high-level outcomes MBIE is seeking to achieve, although notes that these are described in the discussion document in very general terms only. ASB is supportive of the aims of improved consumer welfare through greater choice and control over their data, and economic development through growing the digital economy. However, the case for introducing a CDR is not well-substantiated in the discussion document.

To ensure we achieve the best possible outcome for new Zealanders and New Zealand, ASB believes a detailed outcomes and cost/benefits analysis should be undertaken, prior to any formal policy decisions being taken, and data holders committed to resource heavy and costly projects.

ASB recommends a collaborative cross-Government/industry foundational work stream be established to better define the policy problems and potential solutions, before focusing on design. This would include -

1. Clarifying the NZ problem(s) we are looking to solve, taking a consumer-focussed approach.
2. Quantifying the current situation and target state, as well as measures of success.
3. Identifying what tools / legislation / initiatives already exist that could be used/amended to close the gap between current situation and desired target state, and then consider what else is needed, which may be something less than a CDR.

We see this collaboration involving a range of sectors, as well as consumer representatives, the Office of the Privacy Commissioner, Commerce Commission and MBIE, given the privacy, innovation and competition aspects involved.

This work will be important, as overseas, similar data right initiatives have required significant levels of industry investment and resource as well as presenting considerable implementation challenges. Therefore, a solid evidence base is essential. In the current economic climate, it is

especially important that such a potentially significant initiative is fully considered, before wide-scale investment and effort is undertaken.

*Do you have any comments on our proposed criteria for assessing options? Are there any additional factors that should be considered?*

While we believe more foundational work is needed before taking decisions around the design of a CDR, we have made some general comments on the criteria below.

ASB generally agrees with MBIE's criteria for assessing options, but notes that the criteria seem to be focused at the system level, while consumer outcomes have not been specifically contemplated, despite being the central driver of a CDR. An additional criterion should be added which considers which of the options delivers the most value to New Zealanders and New Zealand businesses, but without placing undue cost and risk burden on other participants.

This criterion should make clear what assumptions have been made about the consumers, in respect of the perceived benefits of a CDR and the problems MBIE are hoping to solve. Have a range of consumer vulnerabilities been considered when establishing the pros and cons of various designs for a CDR? Are there other solutions which may minimize negative impact for those who are in vulnerable circumstances? What mitigants (against increased risk for detriment to those in vulnerable circumstances) have been considered?

We also suggest considering a criterion that considers the extent to which an option creates a level playing field for potential data users that will ultimately optimise competition outcomes for the benefit of consumers, or conversely, which options might create an uneven playing field that restricts competition outcomes. ASB agrees that Trust will be crucial to the successful implementation of any CDR regime. MBIE's description of Trust focuses on mechanisms that can protect consumers, and while these are important, the Australian experience teaches us that consumer trust relies on:

- Good experiences, starting with fewer things done well. Implementing simple, low risk activities first before addressing more complex and higher risk activities (such as write access) is more likely to provide good experiences for consumers on which to build confidence and trust; and
- A robust consent framework from the outset that provides consumers with confidence they are in control of how their data is being shared, with whom, and what it is being used for.

ASB agrees that costs, together with risk, is an important criteria, but until the model and scope of any CRD is better understood, it is difficult to assess any of the options in relation to the likely quantified costs, risks or benefits.

*Do you have any comments on the discussion of Option one: Status quo?*

While we believe more foundational work is needed before taking decisions around the design of a CDR, we have made some general comments on this option.

While ASB acknowledges that the status quo option is not currently delivering optimal outcomes, ASB considers that MBIE's assessment of this option is more negative than is warranted.

In MBIE's assessment, the status quo model does not strengthen the ability for individuals to use or share their data. We believe that the industry-led standards work being done through

the API Centre is in fact strengthening the ability for individuals to use and share their data, although ASB recognises that the benefits from this work programme have yet to be realised.

The paper's assessment of this option also suggests that under the status quo, barriers to entry for new entrants will remain because of the need to have bi-lateral agreements between data holders and data recipients. ASB considers this issue to be overstated, and not in need of regulation or a CDR framework to address. It is ASB's opinion that most data recipients are likely to connect to banks (as data holders) via an intermediary (a switch or gateway) and therefore sign a single contract with them, rather than having to manage multiple API connectivity arrangements to connect to every data provider individually. Furthermore, any barrier that exists as a result of bi-lateral arrangements would be simply replaced with accreditation as the new barrier under a CDR regime. In any case, the API Centre is about to commence a programme of work to streamline and standardise the onboarding process for data recipients, and also create a single multi-party agreement to address this issue.

MBIE further supposes that the economic opportunities associated with a CDR will be hindered under this option as it is likely to lead to inconsistencies in the approach taken within individual sectors and across different sectors of the economy. ASB observes from decades of experience in the payments industry, however, that common rules and standards can be achieved consistently and efficiently without regulation. ASB also notes that MBIE has classified inconsistencies across different sectors as a 'con' under the status quo option, while classifying "design and implementation can be carefully tailored to designated sectors" as a 'pro' under the Sectoral-Designation approach.

MBIE has also concluded that the status quo does not strengthen existing privacy rights and will not address privacy or security concerns that have emerged. ASB would highlight, however, that the industry-led API Centre standards are fundamentally taken directly from the UK best practice Open Banking United Kingdom and General Data Protection Regulation security and consent models, and therefore do in fact address these issues.

As a general comment, a more formal involvement from Government to agreeing API delivery outcomes and timeframes in the banking sector would go a long way to addressing the issues MBIE has raised for the status quo option in that sector.

In any case, ASB considers that current momentum under the status quo needs to be maintained while any CDR regime is being worked through and implemented. This will require that MBIE provides certainty to industry as early as possible regarding the likely CDR end-state so that participants can be confident that their investment in open data projects already underway are still relevant.

---

10 *Do you have any comments on the discussion of Option two: A sectoral-designation process?*

---

While we believe more foundational work is needed before taking decisions around the design of a CDR, we have made some general comments on this option.

In conjunction with continued momentum under the status quo, ASB agrees that the implementation of any CDR would be best determined on a sector-by-sector basis to define in-scope and out-of-scope data, data rules and standards etc. required for specific sectors. Some over-arching legislation would still be required to establish the core mechanisms required for a CDR to operate, and this would address at a high level common elements such as the designation model, consent requirements, liability and dispute resolution mechanisms, reciprocity and accreditation principles.

Under a sectoral-designation model, industry participants should remain primarily responsible for the establishment of rules and standards for the CDR's implementation in their sector, with Government providing oversight and contributing as required. In this sense, ASB views this option as building on the status quo to address areas of weakness and concern. The open data economy is more likely to be successful if data holders are able to treat the CDR as an opportunity rather than approaching it as merely a compliance exercise, and therefore innovate and invest accordingly. Experience from the payments industry shows that an industry-led approach will enable sector experts to collaborate to solve the complexities of their sector and drive outcomes for the collective benefit.

11

*Do you have any comments on the discussion of Option three: An economy-wide consumer data right?*

While we believe more foundational work is needed before taking decisions around the design of a CDR, we have made some general comments on this option.

Per our response to question 10 above, an economy wide-CDR would need to have in place common elements such as designation and consent requirements, liability and dispute resolution mechanisms, reciprocity and accreditation principles.

The frameworks need to be interoperable across industries. Standardising data sharing standards and processes as much as practical across industries is consistent with the core principles of data portability, and will reduce transaction costs for consumers in using their data across the economy (for instance in enabling energy providers to recommend a customer new ways of paying for their energy bills, or by helping banks provide insights to a customer on their energy usage).

12

*Do you have any comments on the discussion of Option four: Sector-specific approach?*

While we believe more foundational work is needed before taking decisions around the design of a CDR, our general comment on this option, is that a sector-specific approach is likely to bring additional complexity without material additional benefits when compared to Option two.

13

*This discussion document outlines four possible options to establish a consumer data right in New Zealand. Are there any other viable options?*

Subject to more foundational work being carried out, ASB considers that a hybrid of options one and two with a staged implementation to build momentum, trust and confidence is likely to achieve the best outcome. This would ensure that industry-led work underway continues, a set of common principles and framework is established economy-wide, while recognising the particular requirements and complexities of specific sectors.

14

*Do you have any comments on our initial analysis of the four options against our assessment criteria?*

Subject to more foundational work being carried out, our view is that a hybrid approach as set out in our response to question 13 above, best matches the assessment criteria, providing a balanced combination of regulatory and market driven approaches, and allowing for a practical implementation timeframe. Building on existing current industry-led programmes will maintain momentum and best meet the speed criteria to spread data portability through the economy allowing benefits to be realised as quickly as possible. A staged approach built out from the current programme will leverage existing investment and enable benefits to be

achieved sooner before investing further in subsequent phases. Faster benefit delivery will build trust and confidence with consumers. An over-arching framework across industries will support a reciprocity principle, and together these will maximise reach. Sector designation will allow for flexibility with solutions tailor-made for the needs of the sector. Reciprocity together with the reach and flexibility of this approach will best allow for competition to thrive and deliver value to consumers, although a consumer awareness program will be required to encourage uptake.

15

*Do you agree or disagree with our assessment that Option two is most likely to achieve the best outcome using the assessment criteria?*

See our response to question 13 above.

### How could a consumer data right be designed?

16

*Do you agree with the key elements of a data portability regime as outlined in this section? Are there any elements that should be changed, added or removed?*

ASB agrees with the key elements of a data portability regime as identified by MBIE, but as previously discussed, ASB also considers reciprocity to be a key element.

17

*Do you have any feedback on our discussion of any of these key elements?*

ASB comments as follows on the various key elements of data portability for inclusion in a CDR framework.

#### Designation Process

We agree that sectors should be designated in areas where a CDR is most likely to have the greatest benefits for consumers and overall economic benefits for NZ. Designation of a sector needs to be considered based on a quantitative economic cost / benefit assessment, although we acknowledge the complexity in such an assessment, the uncertainty of future benefits, and the tendency to underestimate costs.

As MBIE has identified, the definition of sectors will need to be clear and carefully classified to avoid unintended outcomes where the definition can be applied differently to create a 'data arbitrage' advantage. Furthermore, the clear lines between sectors is now blurring, and some businesses may in fact operate in more than one sector. Designation for data portability should be applied based on the nature of the data to be shared as well as the services provided by business in those sectors, and grounded in the principle of a level playing field for data holders and data users. For example, the banking sector includes non-bank entities that offer accounts, payments, lending and various other financial services. In order to meet the objective of facilitating competition, businesses offering similar services to banks should also be required to share the consumer and product data they hold and use, if the banking sector is designated.

#### Rules and Data Standards

ASB anticipates that a CDR regime would define what data is in and out of scope in a designated sector along with some high level data sharing principles that provide clear operational guidelines regarding the availability and quality of data, and providing technical specifications for security, connectivity, and exception handling. Technical and granular standards and rules however should be developed and maintained by sector participants to enable the interoperability of their data with that from other organisations.



### Accreditation

ASB agrees that an accreditation model is required in a CDR regime to ensure that ecosystem participants that handle, store and share data can be relied on to meet and maintain adequate levels of security and operational integrity. ASB has mixed views on a tiered accreditation model. We support the principle of not imposing unreasonably high standards where they are not warranted thereby creating cost barriers for some participants. ASB is however also concerned that lesser data privacy and security standards in relation to some data types or sectors could cause confusion, erode consumer trust, and potentially create 'data-arbitrage' opportunities where data or sector definitions are insufficiently clear.

### Consent

Consent management will be an important aspect of any CDR, as consumers will need to have the ability to easily provide and revoke consent to the sharing of different attributes with different third parties. Australia has found the introduction of consumer consent dashboards to be a useful tool and their consumer experience guidelines ensured consumers were considered throughout the design process. We recommend continuous engagement with consumers throughout the design and implementation of the CDR.

Transparency is an important aspect of consent as consumers need to be informed of what will happen to their data in order to provide informed consent to the disclosure. While data holders will play an important role in providing consumers with notice about what will happen to consumers' data disclosed pursuant to the CDR mechanism, it would be useful for any governing body to supplement these notices with information that consumers could access that explained the CDR.

Consumer consent is critical to protecting the privacy of customers, but needs to be balanced with user experience, and costs that do not create unnecessary barriers to entry for smaller participants. There is significant overseas experience that New Zealand can draw on as best practice to ensure that a local CDR facilitates the management of informed and meaningful consent in a transparent and efficient manner.

### Fraud Protection

Fraud protections will be an important element of a CDR and can draw on other pre-existing regulatory frameworks, such as anti-money laundering and counter financing of terrorism obligations.

### Liability and dispute resolution frameworks

A strong liability and dispute resolution framework will be important to maintain confidence in the integrity of the CDR. At present, liability is addressed through bi-lateral contracts where data holders and recipients can assess for themselves the extent to which they trust the counter-party and negotiate appropriate liability provisions into the contract. Under a CDR, they will need to rely on the legislative framework which will have to be very clear so as to provide certainty to participants about where liability will lie, and recourse where a liable party who they did not choose to deal with is unable to settle any liability claim.

ASB is mindful that the regime need a workable balance between not creating unnecessary barriers to entry for small data users, while protecting data holders from 'de facto' liability where a data recipient has caused losses for consumers, who then turn to their bank (for example) for recourse where the service provider at fault is unable to meet their liability obligations.

While the Australian CDR has a comprehensive liability framework, anecdotally, there are concerns in market around the uncertainty as to how the courts will rule on liability issues.

Uncertainty as to liability under a New Zealand CDR could limit uptake of the CDR, so it will be crucial for a robust liability framework to be in place from day one, to provide businesses with clarity regarding their liability risk profile, so that they can prepare accordingly.

Consistency with other legislation

Any CDR regime will need to ensure its rules are consistent with existing legislation such as The Privacy Act 2020, Unsolicited Electronic Messages Act and other digital identity workstreams. ASB recommends that MBIE considers updating existing legislation to meet the needs of a data portability regime rather than initiating new legislation, where this makes sense.

18

*Are there any areas where you think that more detail should be included in primary legislation?*

We believe that more foundational work is required before this question can be answered.

19

*How could a consumer data right be designed to protect the interests of vulnerable consumers?*

A CDR should be designed with a consumer focus. The growing digital economy and rise of data portability schemes presents new challenges and requires a reframing and reconsideration of who is considered vulnerable in the context of a CDR regime. The increasing prevalence of digitisation and open data raises a broad range of issues for consumers including access to technology; data empowerment; bias; data literacy; and data ethics.

These issues will potentially exacerbate existing difficulties faced by vulnerable consumers and create new challenges for this broad segment. These issues are expected to intensify with the significantly increased online activity and economic uncertainty associated with the COVID-19 pandemic. Furthermore, there may be additional, yet to be assessed, risks to a broader set of vulnerable cohorts than traditionally considered, such as people who choose not to participate in data sharing regimes, and people with low financial literacy who are highly engaged users of digital platforms.

As digital literacy and access to technology are pre-requisites for consumers to benefit from a CDR, vulnerable groups will face the same structural barriers that are associated with any digital financial service. These include access to supporting infrastructure and internet access in regional and remote areas, and the lower access to and use of smartphones by older consumers, people on low incomes, people experiencing (or at risk of) homelessness, people with disability, and consumers with low English proficiency.

In general, vulnerable consumers face a number of risks of disadvantage and discrimination including greater susceptibility to coerced or uninformed consent, fraud, predatory lending, elder abuse and other unethical conduct, mis-selling or denial of services. Greater access to consumer data is likely to increase the risk of exploitation if proper measures are not put in place.

However, a CDR also has the potential to play a valuable role in helping vulnerable consumers manage their financial data and protect their financial wellbeing. For example, making consumer data available to trusted third parties to monitor accounts where a consumer or their personal legal representative may have concerns about financial abuse by another person with access to the consumer's accounts. These types of ancillary consumer protection may prove a compelling use case to increase rate of customer adoption and of community

advocacy for Open Banking. If the decision is taken to introduce a CDR in New Zealand, ASB is committed to working with MBIE and others to ensure that the design of the CDR is inclusive of the needs and choices of all consumers and specifically provides benefits for traditionally vulnerable consumers.

20

*Do you have any suggestions for considering how Te Tiriti o Waitangi should shape the introduction of a consumer data right in New Zealand?*

Māori data is a living tāonga and subject to the rights articulated in Article 2 of the Te Tiriti o Waitangi, which should play a primary role in shaping any New Zealand CDR framework. ASB recognises there is expertise already available on this topic, such as Te Mana Raraunga (the Māori Data Sovereignty Network). A CDR must recognise the strategic value of Māori data and Māori tino rangatiratanga over their data. As such, there must be Māori representation in the design and ongoing governance of the CDR, including any groups charged with managing industry rules and standards. Funding should be allocated to ensure that specialist advice and input is provided to the design and oversight of a CDR in respect to Te Tiriti o Waitangi and Māori Data Sovereignty.

21

*How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?*

It is important that any CDR framework is developed in a manner meets the needs of all New Zealanders. As noted above, we believe any CDR should be consumer-focused and led by their needs. ASB believes a CDR needs to be developed in around key principles that promote inclusion and recognises that many New Zealanders have additional or bespoke information, communication, education, access and support needs. Many individuals need other people to act on their behalf in certain circumstances. All New Zealanders should expect to be able to access the opportunities and benefits that a data portability regime will provide, irrespective of their personal circumstances. To ensure that the CDR considers issues for disabled people or those with accessibility issues, it is important that it is developed and managed with input from the disability sector. Ongoing communication, education and consultation will need to be formally built into the framework.

22

*To what extent should we be considering compatibility with overseas jurisdictions at this stage in the development of a consumer data right in New Zealand?*

Data portability regimes have been implemented differently in different jurisdictions, each with their own unique drivers and objectives. Although there are some similarities with some other countries, New Zealand's objectives are unique and reflect our unique set of circumstances. In ASB's view, while there may be some benefits in trans-Tasman interoperability, our priority should be to develop a fit-for-purpose New Zealand CDR. Where it makes sense and can be achieved without additional cost or risk, standards that are interoperable with the Australian and overseas standards can be considered.

23

*Do you have any comments on where a consumer data right would best sit in legislation?*

Noting the interaction between the CDR and NZ's competition, consumer and privacy laws, given that the CDR framework sits across all three of those areas, and potentially beyond them, it may require a separate piece of legislation.

24

*Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?*

The design and successful implementation of a CDR will require careful planning, coordination and collaboration of a wide range of stakeholders and activities. Similarly, the ongoing planning, prioritisation and monitoring of work and outcomes will require coordination and oversight. There are multiple models that could be used to achieve this. ASB has an open mind as to the best approach, and considers that this would be best addressed once a decision has been made as to whether a CDR is required, and there is more clarity on the form that might take, and specific outcomes we are seeking. In principle, however, any governance model needs to be inclusive and simple, with the design and implementation of the CDR predominantly industry-led.

25

*What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?*

In terms of regulation, a single regulator is preferable, though we are open-minded as to the best approach, noting that the CDR framework is likely to sit across NZ's competition, consumer and privacy laws, and potentially beyond them; but it is important that governance of the CDR is clearly established in the early stages of its development.

We have seen from Australia's experience that having multiple regulators involved in the governance and regulation of the ACDR (the OAIC, the ACCC and the Data Standards Body) has caused uncertainty regarding responsibilities for implementation and/or regulation of particular aspects of the ACDR regime.

26

*If government decides to establish a consumer data right, do you have any suggestions of how its effectiveness could be measured?*

ASB supports the desired outcomes of consumer welfare and economic development that MBIE sets out as the drivers for a CDR in New Zealand, however in the discussion document, MBIE has not quantified the current situation (baseline) or target state with measurable facts against which to determine a successful outcome.

ASB would support further collaborative Government and industry foundational work to better define the policy problems and potential solutions, including a quantitative approach to assessing the need for, and potential effectiveness of a CDR is addressing the problems, taking into account the likely investment required economy-wide to implement a CDR.

## Other comments

New Zealanders and New Zealand businesses are facing unprecedented times as we grapple with the impacts of the COVID-19 pandemic. As a Bank we have a vital role to play in helping support our customers and the New Zealand community, and we have a unique privilege and responsibility to serve our customers during this period. As a sector, we are diverting significant resources to prioritise initiatives that support our customers and the New Zealand economy towards a path to recovery.

The financial impacts of COVID-19 to our customers will be varied and long lasting and it is important that we consider any CDR regime through this prism. Further, there are particular risks that must be carefully managed to ensure the integrity and security of the ecosystem, and to ensure consumer protections are embedded into the design of any CDR. As such, we recommend MBIE considers a

staged approach and practical timelines for any potential CDR given the significant lead times for implementing technology reforms of this kind.