Bank of New Zealand's submission on discussion document: Options for establishing a consumer data right in New Zealand

16 October 2020

1 Introduction

1.1 Bank of New Zealand ('BNZ') has prepared this submission in response to the Ministry of Business, Innovation & Employment's Discussion Document: Options for establishing a consumer data right in New Zealand ('Discussion Document').

1.2 BNZ is very engaged on the topic of a consumer data right ('CDR'), is an industry leader in the development of open APIs through the Payments NZ API Centre and welcomes the opportunity to submit on this Discussion Document.

1.3 The focus of this submission is to highlight aspects of the Discussion Document that we believe will assist in achieving the policy objective of giving consumers and businesses greater choice and control over their data, as well as aspects that we believe may not assist towards this objective.

1.4 BNZ has contributed to and supports the Payments NZ API Centre submission. BNZ also supports the submissions of the New Zealand Bankers' Association and the Financial Services Council. As an active industry participant, we have contributed to the discussion and debate on CDR with the Data Economy Collective, however the overarching response from the Collective differs from our own.

2 Key themes underlying our submission

2.1 BNZ agrees that, if designed and implemented effectively, a CDR could be a key enabler for realising a higher achieving and prosperous New Zealand by being a central driver for a data enabled and digital economy. The key is achieving **effective design and implementation**.

2.2 We have responded to each of the questions in the Discussion Document. However, our response is shaped by 7 key themes that we want to highlight upfront and which we think are critical to getting the design and implementation of a CDR right. These are set out below:

1. Be clear on intended consumer outcomes and benefits: We submit that it is critical that (a) the specific consumer outcomes of a CDR are identified from a current base scenario and (b) the design of the CDR is focused on enabling parties to deliver those outcomes. The Discussion Document does identify several benefits and intended outcomes which are broadly cast, and as a result, it is not clear in all cases what research and analysis underpins these. For a CDR to enable a blossoming economy of open sectors and support the government's digital strategy, it will be important to be clear on how the CDR fits in with that, and by what metrics it will be measured.

2. Start simple and scale up over time: The Discussion Document floats a lot of ideas some of which may only be feasible down the track. We suggest that the complexities involved in establishing an all-encompassing CDR to enable these extensive use cases may be underestimated and invite unintended delays to develop the CDR. For each function, there are legal, policy, standards, design, technology build, and regulatory considerations.

Therefore, we believe it may be more appropriate to focus initially on developing a simple CDR and getting the basics right. We consider that this should begin with a minimum level of functionality, which can be built on in subsequent phases. In the financial services sector this could mean starting with, for example, providing account information for a single individual, building on the work that has already started via the API Centre.

We suggest the CDR should focus on delivering the framework for a simple 'read' data regime and defer 'write' data and other more complex requirements until a later phase.

3. Integrate with existing frameworks: A CDR should utilise existing privacy and data protection laws (e.g.: GDPR) and fit with the emerging Digital Identity framework. Each new legal requirement should be consistent with - and not overlap with - existing laws (and all other new legal requirements). The appropriate legislation for housing a CDR should be examined only after the parameters of the new rights are further defined. Enabling entities to share via CDR consumers' digital identities, and single aspects of identities, will remove a friction point, decrease risks, and unlock efficiencies for all participants, including consumers.

4. Get the governance structure right: We understand that this has been an issue in other jurisdictions, where an entity has been given a governance role that does not really fit with the scope of a CDR. We believe a collaborative approach is required to develop an appropriate governance framework that supports CDR and an ecosystem of open sectors. We discuss our thoughts on this in more detail in response to question 25.

5. Take a principles-based regulatory approach. A prescriptive regulatory approach to designing the CDR may adversely impact efficiency, costs, compliance, and risks. It could ultimately affect whether the CDR regime delivers the desired outcomes to consumers, and the timeframes in which that happens.

A principles-based approach would specify the intention of regulation, rather than prescribing rules with detailed regulatory requirements. We believe this approach would be more appropriate because:

- It would efficiently structure New Zealand's CDR regime so that it becomes a sensible business decision for an organisation to adopt the CDR regime; and

- It is more likely to benefit all industry sectors and therefore a wider range of New Zealanders. Conversely, prescribing how the regulation must be implemented risks becoming inefficient and obstructive because it prevents better ways of achieving the goals from being adopted when they emerge.

6. Gain consumer trust: the CDR should have an effective consumer trust, security and consent framework at its core. This framework should be aligned to existing consent requirements in privacy law with clarity over "what data", for "what purpose" and for "how long". This is critical for consumer adoption of a CDR in an open digital economy. The CDR should empower consumers to:

- become more familiar with consent processes and their data rights;

- have control of their data;
- trust those managing their data and;
- receive value for sharing their data (from subscribing to innovative products and services).

7. Leverage the existing API Centre Account Information API standard: This existing standard was based on a leading international open banking regime (UK). It is secure and effective. Delivering to this standard would be faster than if NZ moves to completely new standards. In addition to these benefits, BNZ has invested substantially to deliver APIs to the existing API standards (both for sharing account information and enabling payment initiation). It would be potentially punitive to BNZ, and other banks who have allocated significant resources and effort to deliver on what the industry had agreed to, and had promised, to consecutive Ministers for Commerce and Consumer Affairs. It might also jeopardise the delivery of benefits from those standards between now and the day that a CDR comes into force.

Should MBIE have any questions in relation to this submission, please contact:

Paul Hay
GM Regulatory Affairs
Bank of New Zealand

DDI: (04) 474 9028
Mobile: (021) 159 8172
Email: paul_hay@bnz.co.nz

THE FOLLOWING SECTION SETS OUT BNZ'S SPECIFIC RESPONSES TO THE MINISTRY'S DISCUSSION DOCUMENT

……

2 Does New Zealand need a consumer data right? [1]

2.1 BNZ recognises the importance of the value associated with consumer data, including its role as an input to service provision. BNZ has identified numerous use cases for a CDR at BNZ. However, BNZ is highly cognisant of the risks involved in getting this wrong and considers that a CDR should only be done if it is precise in its design and delivery, with time allowed for expansion over time.

2.2 The Discussion Document links current regulatory settings to the existing lack of consumer data portability. BNZ agrees that regulatory settings have played, and continue to play, a role in this. However, consumers must also be on board with benefits that a CDR can bring, and gaining their trust will be essential. We strongly believe that the best way to achieve this is to start by requiring a clear, simple, and narrow level of functionality, that is widely communicated, and then to build from there. While it may be useful for MBIE to have in mind potential 'use cases' or services the data could enable, we recommend that officials should avoid trying to guess what types of innovation the market may be able to create.

2.3 We consider that without a simple starting point there is risk that consumers will not have a clear understanding of what they are consenting to. This lack of understanding could result in uninformed sharing of consumer data, with a greater potential benefit to organisations, rather than to consumers. A CDR must have the consumer outcomes at the heart of the design, and consumers must be in control of their data.

2.4 One of the key observations from the implementation of the CDR in Australia is that the CDR should start by requiring simple and clear primary functionality, which is then slowly expanded over time with additional functionality. We therefore commend what we are hearing from the Ministry on their desire to get CDR right and seeking insights from global experience.

Responses to specific questions

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

[1] The numbering from this heading onwards matches the section heading numbering in the Discussion Document.

2.5 Yes – consumers may not be comfortable with sharing data and empowering third parties to use it, regardless of regulatory settings. Not all data or the use cases enabled are created equal from a risks, costs and benefits perspective. Consumers must have confidence in the protection of their shared personal information across different types of data, service providers, timeframes and industries before they will share it.

2.6 Yes - there are not many genuinely reliable use cases offered via a seamless experience for consumers to transfer their data to.

2.7 Yes – it is unclear whether enough consumers are sufficiently savvy with digital tools to utilise methods to transfer their data to other organisations (both for existing and new tools).

2.8 Yes – we note that the government refrained from incorporating a data portability right into the NZ Privacy Act 2020, as had been requested by the Privacy Commissioner. Presumably this was because more information and public engagement were needed. However, it would be helpful for the government's reasoning, and any related concerns, to be clarified.

2.9 Yes – current regulatory settings do not *require* data portability. Under the current (and soon to be updated) Privacy Act, data holders must provide individuals with their personal information but there is no requirement for the data holder to provide a third party with that information – even if the relevant individual has authorised the transfer. In addition, the data holder can refuse to make the information available to the individual in their preferred format if providing the information would impair the efficient administration of the organisation. This can add friction to an already indirect transfer of information between service providers.

2.10 Yes – data portability comes with challenges regarding the interaction between technology and regulatory requirements. Regulatory settings will *not* solve for all the technology design requirements including:

- **Consent management**: including navigating complexities of joint accounts, revocation, and granularity that includes capturing information on "which data", for "what purpose" and "for how long".

- **Data architecture**: requires "meta data on meta data" for logging historic consent authorisation and revocations. This includes new processes for segregating CDR data so that it is only used for the consented purpose and doesn't then get added into the aggregate of wider data and used for other, non-consented purposes.

- **Data quality & standardisation**: particularly difficult when considering duplicate transactions, potentially changing transaction IDs and descriptions. We are happy to provide MBIE with some examples of further complexity, if that is helpful.

2.11 Further, we are not convinced that all the concerns listed in paragraph 13 of the Discussion Document are in fact hindering consumer data portability. For example, data portability required for account switching between banks works well.

2.12 In addition, although there are currently no general requirements for data to be shared in a consistent format, the Financial Services sector has started to address this with the Account Information API. BNZ has for years shared account and transaction data with online accounting services. We also send data directly to some of our own business customers using API's.

2.13 Finally, in relation to 13(e) and concerns regarding fee transparency, this is difficult to assess as there are currently too few APIs enabled for the pricing to be transparent. However, we expect this will evolve regardless of whether it is regulated. For example, it is BNZ's intention to make public its pricing for connecting to BNZ's open banking APIs once we have market-tested it and satisfied all internal sign off processes.

2. 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?

2.14 As a general comment we think it would be helpful to research and establish baseline criteria for the benefits listed. This would help to set goals and enable a measurement of success for parties to work towards. This would also allow the costs of bringing about the change to be considered ahead of regulation.

MBIE stated benefits	BNZ view
Enables innovation and grows the digital economy by allowing third parties to develop tools for consumers that use their data to match or create products and services that better suit them. Data holders may also have access to new consumers and markets.	Agree - however, in forming any regulation it would be useful to understand first the level of financial services innovation and size of the digital economy in New Zealand today, the socially desirable level of innovation and size of the digital economy, and how much a CDR could contribute to bridging the gap. Data sharing by itself will not necessarily deliver the full market benefits associated with that capability. The primary focus should be achievable functionality that enables innovative services that add significant value to consumers and move us toward an open digital economy.
Facilitates competition by allowing consumers to multi-home services (e.g. to have access to services from multiple providers in one place), access innovative products and services, increasing transparency of pricing and other factors to more easily compare products and services, and potentially encouraging the unbundling of products and service	Agree - BNZ considers that being able to manage financial services from multiple organisations through a single mechanism has merit. But would argue that this is primarily a convenience rather than competition benefit given strong competition currently exists in the financial services market.

	It is not clear that a CDR is currently the most efficient way to address a perception of limited pricing transparency, or a culture of 'haggling'. In any event this would need to be considered as part of a "product data" right which we consider distinct from a CDR. (See below in para 2.21 for further detail on this.)
Increased productivity by reducing search and switch costs and allowing products to interact more with other services (e.g. cloud-based accounting using bank data to reconcile multiple bank accounts).	Agree, to some extent – BNZ notes increased productivity is often heralded as a benefit of new technologies. In practice, new technology can result in the same amount of time being spent; although less time is spent interacting with each service provider, more services providers or channels must be interacted with. We doubt that banking search and switch costs would be reduced noticeably by a CDR. In addition, of all FinTech services, cloud-based accounting, is already deeply integrated with most banks today. We wouldn't expect data portability to add any materially larger volumes of data into those cloud accounting companies than they already have secured by linking up directly with banks for years now. The benefit would come in flow the other way. Sharing the aggregated consumer financial data held in cloud accounting platforms should be enabled under a CDR, to be used by other third parties (such as other aspiring FinTech micro cloud accounting businesses).
Strengthened privacy and data protections by improving security when data is shared, giving individuals and businesses greater control over the information held about them and the ability to use this data for their benefit.	Neutral - BNZ strongly supports efforts to improve the privacy and protection of ported data. We also believe that perceptions of strong privacy protections will assist uptake and engagement from consumers. However, there are difficulties inherent in providing strong privacy and data protections in a CDR regime that makes data more available to more parties than the status quo. In addition, a CDR should consider whether current practices such as screen

	scraping require attention. While they fall under the Privacy Act, we feel consumers are often left with insufficient clarity about: - what they are consenting to before allowing access to their data, - whether the data provided is the minimum required for the service being provided, - the fact that data can only be used for that purpose and not added to a pool of data for later use without their awareness or consent, -the period the third party can hold that data and, -the means of revoking access or extent of rights to have their data deleted by the third party they passed it to. It is also unclear what knowledge and control the consumer has on that data being passed on or sold to another third party. Eliminating unsecure practices such as screen scraping is an important measure the CDR should address to ensure widespread adoption of the safer data sharing methods the CDR enables. Otherwise, screen scraping could be used by some entities to avoid the costs and liabilities of complying with CDR requirements. BNZ has gained useful consumer consent insights while building and deploying the two API Centre API standards. For example, the consent must be specific, clear and easy for the consumer to understand (especially because concepts like open banking are not widely understood by the general public in New Zealand). The API Centre standards were adopted from the UK Open Banking experience, as modified for NZ. We think they work well

	and recommend the API Centre Account Information standard and consent model be adopted as the initial standard for a CDR in financial services. That would bring forward the achievement of financial services benefits, retain the investment third parties and banks have made in those standards, and facilitate ongoing investment in the period until any regulation is in force.
Consumer welfare will be improved by strengthening existing privacy rights for individuals and giving consumers greater control of their data. Consumers will have the power to make more informed buying decisions through greater transparency and will be able to access a wider range of products and services. Consumers will also be able to seamlessly switch product providers without losing data.	While consumer welfare could be improved by giving individuals greater control of their data, complex marketplaces with information asymmetries can cause decision fatigue. Consumer welfare may well be improved for sophisticated consumers only. However, there may be little to no benefit and possibly disadvantage, to other consumers (particularly those who are digitally excluded or otherwise vulnerable). It is not clear that access to a wider range of products and services is always a benefit. The banking industry has until recently offered a broad range of products and services; it is now simplifying these to make them easier to understand.

Costs	BNZ view
Increased security and privacy concerns: as consumer data may be accessed by more companies there may be an increased risk of a data breach, and it may be difficult to determine where liability rests.	Agree – however we think many of these issues can be mitigated by taking a 'privacy by design' approach, including the use of Privacy Impact Assessment(s). We are comfortable that the security measures specified in the API Centre standards adequately protect data during transmission between the data holder and data users. Those standards would be a good starting point for a CDR.

	Regarding information storage, the key will be to ensure appropriate accreditation standards for companies that want to receive data. This will reduce the risks from 'hacker arbitrage' – hackers identifying information accessed by companies with lower security standards and targeting those companies (rather than banks, for example). BNZ has developed minimum data security standards that data users must comply with before we send them data. These include data security due diligence checks. Our experience in using these standards with third parties is that they are aligned with good practice that experienced companies are already following. We would be happy to share that with any emergent accreditation body, and for regulation or rule drafting. BNZ has developed good insights about API use liability, including data breach, while working with the API Centre and negotiating bi-lateral API agreements with third parties. We think it has been straight forward to identify and agree between API providers and users where liability at any point sits.
Implementation costs for government and industry may be significant. It would require extensive changes to information technology (IT) systems to make data available. Depending on how a CDR is designed, these changes could be significant for smaller businesses (as data-holders), and large businesses that have multiple IT systems.	Generally agree - but we believe this can be mitigated with good CDR design and planning. A key theme of this submission is that the CDR should start by requiring simple primary functionality, which is then expanded.
May impose barriers to entry by requiring businesses to hold consumer data in a particular way so that it can be shared in the appropriate format.	Neutral - BNZ considers this may be an issue for some businesses that are data holders. However, providing consumer data in a common format should lower entry barriers for data users.
May delay innovation in sectors where progress has been made if those sectors choose to wait for regulatory intervention, or choose not to invest in	Agree - this is a matter for the Ministry to consider, particularly in the context of financial services and the API Centre.

new data-gathering methods due to the concern that they may be required to share this data or incur costs in making data available.	The Ministry continues to encourage API Centre participants to keep delivering API Centre standards and working to make API adoption easy. Creating uncertainty on the ongoing use of the API Centre standards would increase the risk of parties stopping investment. We consider a CDR would strongly benefit from continuing the API Centre Account Information standard. It would be helpful to have a prompt formal decision on this (and regarding the Payment Initiation API standard).

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

- **Yes - innovation and competition does not trump consumer data privacy, control and security rights.** There is a risk that, if innovation is valued over consumer privacy, control and security rights protections may get watered down to lower barriers to entry for innovators.

  Our strong preference is to encourage high standards for data users, with high grades of privacy, control and security rights for accessing consumer data. New Zealand can then work back from a position of consumer trust, rather than starting with low requirements for data user access that can be increased if things go wrong.

- **Yes - loss of data sovereignty and national sovereignty.** BNZ is concerned that CDR regulation may enable global data giants to connect to all the New Zealand open sectors and make use of the data outside of consumer control and outside of New Zealand control. We understand New Zealand's Privacy Commissioner also has concerns along these lines.[2] We would welcome the Ministry's views on this and any thoughts it has on mitigation.

  We understand this issue was planned to be addressed in Australia by requiring broad reciprocal data rights that would have required all data users to share "equivalent" consumer data with domestic data holders. It appears the definition of 'equivalent data' was subsequently adopted to be data that is in essence the same data set; this substantially reduced the effect of this requirement. In any event, in our view, strong data reciprocity rules look to be, at best, a partial solution. The data giants should not be disproportionately

[2] See, for example, https://www.privacy.org.nz/blog/facebook-what-this-is-really-about/ and https://privacy.org.nz/news-and-publications/statements-media-releases/media-release-google-agrees-to-protect-privacy-better/

enabled by a CDR to access any data unless they have first demonstrated to the Privacy Commissioner that New Zealand privacy requirements are being, and will be, followed. Solving these issues is central to ensuring that New Zealand businesses can compete on a level playing field and that New Zealanders' data and privacy is adequately protected.

- **Yes - maintaining New Zealand's adequacy status.** A CDR could strengthen New Zealand's ability to maintain a positive adequacy decision under the General Data Protection Regulation (GDPR). A positive adequacy decision benefits New Zealand as it facilitates trade with the European Union and those subject to the GDPR's substantial extra-territorial reach. To maintain its adequacy decision, New Zealand must provide an 'essentially equivalent' level of privacy protection to the GDPR, which has a right to data portability. A functioning CDR in New Zealand could help to provide a continuing 'essentially equivalent' level of protection.

- **Yes - overlapping compliance obligations.** Participants in the CDR ecosystem may be challenged to meet CDR requirements if they are subject to overlapping regulations. A New Zealand data holder could hold information that is - at the same time - subject to the New Zealand Privacy Act access request process, the GDPR's data portability regime, and a new CDR regime. Accordingly, we support a CDR in New Zealand that aligns with the obligations of the Privacy Act, or potentially, forms part of the Privacy Act itself. We also support a CDR that aligns with the obligations of overseas legislation such as the GDPR. This view is shared by the Privacy Commissioner, who recommends a right to data portability in New Zealand that at a minimum entitles individuals to rights comparable to the GDPR.[3] We would strongly recommend a collaborative and aligned approach between the different regimes so that a business is not required to consider multiple processes when aiming to achieve one objective for the consumer.

- **Costs.** There is a risk that costs fall largely on data holders if data portability is mandated at below cost or no fees at all. In BNZ's view, it appears commercially unviable to enable a data recipient to make a commercial return without paying data holders for raw materials (e.g. data) and maintenance costs of the systems associated with storing and providing that data. In addition, this is unlikely to encourage innovation or drive the best consumer outcomes. The UK experience has been that prohibiting fees has contributed to unstable open banking technology that does not operate smoothly or consistently.

  We foresee a poor outcome for consumers if meeting the CDR requirements becomes simply a regulatory compliance exercise, with an incentive to deliver compliance at the minimum possible cost because data holders cannot recover their reasonable costs.

- **Assumption of benefits.** There is an underlying assumption that a CDR will benefit consumers by providing choice and control for them. While there is certainly merit in this assumption, the alternative should be rigorously considered as part of this consultation

[3] The Privacy Commissioner recommended a 'data portability' right in its Report to the Minister of Justice in 2017, https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-report-to-the-Minister-of-Justice-under-Section-26of-the-Privacy-Act.pdf paragraph 12.

process. For example, we found that the Right Now[4] and Financial Rights Legal Centre[5] submissions on the Australian CDR both challenged our own tacit acceptance of such assumed benefits.

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

2.15 We support the concept of a business data right (BDR) in theory. However, we think it is quite different to a CDR (which would need to be re-named, so the title did not refer only to 'consumers'). We are not convinced that this is a priority for regulation. Financial institutions already have many tools for passing businesses their financial data in an electronic, machine readable form. Banks already send consenting businesses' transaction details to cloud accounting services, to put into user accounts. Any BDR should be considered separately, in future, on its own merits, as measured against defined goals that the regulation seeks to achieve.

2.16 It is also possible that businesses don't have sufficient contractual rights or technical capability to access their financial data held at cloud computing companies and government agencies. There may be benefit in opening access to that data. There may also be increased benefits for smaller businesses looking to provide a better cloud accounting service.

2.17 However, there are greater technical complexities for a BDR - particularly to determine and authenticate who has authorisation to act on a business account. This is complicated further where different people have different levels of authorisation for a single business. In such cases the 'consent' process needs to work to differentiate between people who can each log in to a business account but have different levels of permissions. There is a related issue of accounts that require multiple signatories to authorise actions. That issue is being worked on now in the UK, two and a half years after their open banking rules went into force. The API Centre is staying abreast of those developments. We think this timeframe illustrates the additional complexity of introducing a BDR.

2.18 Accordingly, a BDR would significantly increase cost without a certain corresponding increase in benefit. It could also delay delivery or quality of the initial CDR functionality. This runs counter to our thesis that an incremental roll out of a CDR will be more secure and stable, thus building trust and maximising the benefits that open sectors can deliver over time – to consumers and, if necessary, to businesses.

[4] http://rightnow.org.au/opinion-3/consumer-data/
[5] https://financialrights.org.au/wp-content/uploads/2020/06/200522_TreasuryCDRExtension_Sub_FINAL.pdf and https://financialrights.org.au/submission/

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')?

2.19 We agree that only "observed" or "provided" data, not "derived" data, should be subject to a CDR. We suggest that the initial focus of the CDR should be for read access data only.

2.20 A CDR regime also needs to consider what data needs to be shared and how to limit sharing of consumer data to only that which enables the consumer outcomes sought e.g. do we need to provide address or proof a consumer resides in NZ?; do we need date of birth or to know the consumer is over 18?; all transaction statement information or proof income has exceeded $X over 6 months? If we can limit the data provided to only that which is needed for a particular outcome, it would reduce the impact of a data breach or data misuse and enhance trust without compromising outcomes.

2.21 We do not think that "product data" should be conflated with "consumer data". Product data is distinct from consumer data. We acknowledge that there may be good social, business and competitive benefit reasons for regulating transfer of product data. However, in our view this should be discussed in its own right and for its own merits rather than as a part of the CDR portability definition or rationale. Including product data in the CDR would add unnecessary complexity and require consideration of a range of different issues including:

- **Complexity of product types:** the financial sector in New Zealand has no existing common definition of product types. Each business has developed its own product labelling for its own internal use. Therefore, any product data requirement will first require the creation of a common classification for financial services products within the regulation, then time for data holders to classify all their products before common product data can be accessed. Even then it is likely some products will be too differentiated to be captured by a common classification.

- **Standardisation of product features**: even products classified in the same category would usually have different features. The result of defining the scope of product features falling under a CDR may be that banks remove or standardise features they currently offer. For example, a home loan might currently appear to be a standardised product, with competition driven entirely by price. However, each bank offers home loans that differ across many factors, including whether: (i) the mortgage can be re-drawn after being paid back (revolvers); (ii) the consumer gets 'cash back'; (iii) if so, what percentage of cash is given back and whether there is a limit to how much of the borrowing that percentage is calculated on; (iv) fees are charged for application, valuations, or other parts of the process; and (v) there is a premium for low equity borrowing (high 'loan to value' borrowing). These features are over and above any service features (such as mobile mortgage managers) and - most importantly for any consumers - each bank's credit policies that determine whether a loan will be granted (which will remain confidential in any eventuality).

- **Reducing competition**: There is a risk that requiring products to conform to an established common classification regime will have the unintended consequence of limiting innovation

of products that fall outside of those classifications. It is an open question whether it is possible to mitigate this risk.

- **Retrospective product data**: While we do not think product data should be included in the CDR, if it were included, it would be important for product classifications to start from a given date. If retrospective product data were required, then adding product data would become an even more complex, expensive, and error prone process; it may also result in the wrong consumer outcomes. It could even entail business investment to standardise data for products that are no longer available to consumers.

2.22 We understand that the Australian CDR has faced challenges with product data, resulting in non-standardised information being provided via CDR.

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

2.23 As with "product data" we recommend that "write data" is considered separately for a later phase and on its own merits before the Government decides whether to include it in a CDR. We note that the Australian CDR has initially launched as 'read' only data, with a current inquiry examining whether the regime should be extended to write access. 'Write access' carries bigger risks and is more complex. We agree there are some obvious benefits of write access given it potentially allows for a wider range of services to be offered to consumers. And, of the examples of write access given in the Discussion Document, we support:

a) enabling the updating of contact details or personal information across multiple service providers; and

b) consumers initiating payments through trusted third parties. This is a core capability we have supported through the API Centre. Provided the CDR work does not disincentivise other banks to invest, we are expecting them to follow suit and deliver Payment Initiation APIs. For that reason, we do not see a benefit to including payments write access in any expanded CDR, until at least write access has been considered comprehensively and the inclusion of payments has had separate, detailed consideration. We encourage MBIE promptly to confirm publicly that investment in payments API's will not be jeopardised by this regulatory process.

2.24 However, we are not comfortable with the compliance and consumer risks of enabling third parties to open and close of accounts on behalf of consumers using 'write access' instructions. This feature should be considered for later phases of the CDR on the proviso there is a national Digital Identity service in effect by that time.

2.25 The Discussion Document's proposal, in the context of financial services, appears to be a temporary power of attorney, as the third party might be enabled to make payments, move money, open and close products, and enter and exit contracts on behalf of the consumer. The 'write access' proposal in the paper should be discussed and considered in that light. Today financial services powers of attorney are usually given to a consumer's closest and most trusted associates - not to temporary occurrences of service providers.

2.26 As a financial service provider, anyone acting on behalf of a consumer is subject to a high level of control, to protect the consumer. We urge the Ministry to place the highest weight on protecting consumers when it balances consumer protection against ease of third-party access - particularly for write access. If bad actors can breach third party security and access controls, consumers could lose a lot of data, or money, in micro-seconds with limited recovery capability.

3 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?

3.1 We agree that the outcomes set out in paragraph 26 are good aspirations for a CDR. However, they are cast in very broad terms. We think it would be helpful to be more specific about the intended outcomes and the relative priority of each of the outcomes. This should start with clarity on the status quo and specifying the future state sought for each consumer outcome. Further research is then required to see if the proposed outcomes: (a) could be achieved by a CDR; (b) are of value to individual consumers; and (c) would have benefits that outweigh the costs.

3.2 In terms of additional outcomes, we would add:

- Reducing the cost of doing businesses by enabling easier transfer of information between consumers and businesses i.e. where transfer was previously of analogue information or underpinned by manual process; and

- Reducing the cost of assurance and complying with regulation around the verification of consumer data by allowing for consumer trust and reliance in regulation.

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

3.3 Each of the criteria that is outlined in paragraph 28 is important but we consider they should be given different weightings and be recast slightly. As per our key themes – ensuring consumer trust is central to a well-functioning CDR and should be given the most weight.

The definition of **Trust** should be edited to refer to the likelihood an option will "~~maintain~~ strengthen the security" of consumer data.

In the definition of **Speed**, it is unclear whether 'widespread throughout the economy" refers to the number of industries touched or - more concerningly - the speed at which NZ can achieve the maximum total amount of data moving around. In our view, Speed should be considered as the likely time it will take to deliver the first tangible consumer benefit and then to deliver further benefits.

3.4 In this vein, we think it is important to add "beneficial consumer outcomes" and "simplicity" as evaluation criteria. Collectively, we need to be able to clearly articulate how the consumer benefits will be delivered under the CDR. Keeping the CDR principles-based will more likely enable an efficient and speedier implementation.

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

3.5 We think it is important to recognise that a lot of progress can happen without any regulation e.g. Plaid is a United States' aggregator service connecting thousands of consumer-facing apps to thousands of financial institutions. We also consider that the introduction of a CDR should work with the status quo i.e. that the API Centre's industry standard for sharing account information be adopted under the CDR and the use of the payment initiation standard not be put in jeopardy.

3.6 There are many benefits of having the API Centre Account Information standard carry on as part of a CDR. For example, using it as a financial services initial release could be a good first step to cement in quick wins. In addition, this standard can be used to develop consent styles that consumers understand, which can be refined and feed through practical experience into the forming regulation. With active regulator support and endorsement this would seem to provide a good base from which to develop a CDR.

3.7 Conversely, if support for the ongoing use of the API Centre standards is uncertain ahead of a new CDR, the industry-led work would likely stop. Stopping the API Centre standards project will cause significant delay to CDR replacement standards and, more importantly, delay building consumer trust in data right experiences.

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

3.8 The Discussion Document identifies a sectoral designation approach, like the Australian CDR, as the preferred model. We agree that a principles-based framework could work well in New Zealand but stress the importance of learning from the Australian experience. This is discussed further in section 3.17 below.

3.9 As noted in the "cons" in paragraph 34 there are limitations in targeting one sector at a time. From a consumer's perspective, the relevant data for an application could be data from a wider range of sectors than those designated. Designating sectors sequentially will result in consumers not being able to see all of their relevant data, at least initially.

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

3.10 We think the differences between Option 2 and Option 3 are less clear-cut than the Discussion Document suggests and should be studied further. We consider that Option 3 could be helpful if concerns around control, privacy and security are not satisfactorily addressed, or are perceived as such, under Option 2. It may be beneficial to have some nation-wide higher order principles that apply to all consumer data use, even while Option 2 sectoral-designation introduced specific requirements for sectors.

3.11 We do not agree that reliance on high level principles would make this option difficult to implement in practice. The Privacy Act is based on high level principles (the Information Privacy Principles) and operates effectively. Clearly, however, more detailed standards will need to sit below the high-level principles to ensure consistent implementation and interoperability.

3.12 An economy-wide CDR would most closely align with the GDPR, and hence provide the strongest support to New Zealand's ability to maintain its positive adequacy decision (see also Section 2 paragraph 3(c)).

3.13 Option 3 could, however, introduce risks. Large-scale legislative changes have more to get right first time. There is also a greater risk of unintended consequences, particularly in sectors for which no one has yet thought through the issues of applying a CDR. There could be benefits in taking a staged approach, by starting with a lower-impact option, while intending to move to a larger-impact option later, once consumers and businesses are more engaged and see benefits.

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

3.14 BNZ does not consider this a readily viable option. In addition to the cons listed at paragraph 38, it introduces the risk of significant re-work; if many sectors have different approaches, at some point this is likely to be inefficient and require alignment. In our view, any sector-specific approach needs an over-arching baseline in legislation, so all sectors are aligned on an underlying basis. That appears to be best achieved via Option 2 or 3 (or a combination of both).

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

3.15 As noted above, BNZ considers there is value in considering a hybrid approach of Options 1, 2 and 3. The status quo could then carry on and provide consumer experience and regulator insights until the regulation takes effect. From that point, CDR implementations can take over and integrate the status quo activities to the extent appropriate in each case.

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

3.16 No, except that we do think there are other criteria that have not been assessed, as discussed at paragraph 3.4 above.

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

3.17 As mentioned above, we agree that a principles-based framework is the best approach and that there are benefits to a staged approach i.e. starting with a lower-impact option while intending to move to a larger-impact option later. However, we think it is critical to learn from the Australian experience.

- **A detailed roadmap is imperative.** This should start with a simple data-sharing functionality and add complexity in later phases. The timing of the phases should relate to the complexity of the tasks involved.

- **A Privacy Impact Assessment is required**, along with clarity on the respective roles of privacy law and the CDR. We understand there is some complexity in the Australia model regarding what data falls under CDR vs. being personal information, and the extent to which those two categories overlap. A Privacy Impact Assessment conducted at an early stage should be used to inform the design of the CDR, rather than an assessment of the final solution once key design decisions have already been made.

- **The designation/accreditation system should be tiered or enable the use of third-party intermediaries or aggregators** to provide a connection point for smaller third parties. In this sense, tiering would involve lower accreditation requirements for third parties undertaking lower risk activities e.g. an accountant could obtain an 'accountant accreditation' to receive their clients' information. Again, such tiering brings further complexity, so should be introduced in subsequent phases.

- **Data reciprocity needs careful consideration.** It has limited value if it is defined too narrowly i.e. only the exact same data set needs to be reciprocated.

- **Where there are multiple governance and implementation bodies, they need to be able to work together** to ensure that the legislative, regulatory and policy outcomes support common standards and technology, and an open ecosystem, that are consistently understood by the market. One body must be the ultimate decision maker. The lack of clarity on how things were to be implemented in Australia created inconsistent consumer and business outcomes.

4 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?

4.1 We consider that Digital Identity needs to form a more prominent part of the design than simply an inclusion as a strengthened privacy safeguard. Once developed, a person's Digital Identity will include a collection of pieces of information that could be shared in different combinations via the CDR regime. For example, entities could provide confirmation that a person is over 18 years old, or lives at a specified address, or lives within a certain electorate. This approach will decrease risk, such as by sharing the minimum amount of data needed for a particular end use. At the same time, it will unlock further efficiencies within the digital economy, by shortening the time needed to confirm specific information about a person.

4.2 We agree an accreditation regime is a key element of a CDR. It will be vital to gaining consumer trust that the regime provides for a public register of accredited parties.

4.3 The regulation should consider the extent to which a business receiving data can rely on the quality of that data in their processes. This is a complex issue that must be considered in depth when designing a liability model. Should the business receiving data be liable where their service generates an incorrect outcome if the only cause was an error in the underlying data they received via CDR? Should a data holder be liable for data after it has been provided? Does that imply a data holder must invest to increase the quality of data beyond the level its own business requires solely so it can be provided via CDR? Where should any losses sit if no party is at fault? The Digital Identity Trust Framework has begun to consider some issues of this nature.

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

4.4 We agree that consumers will need a certain degree of literacy on how consent and data rights each operate, to ensure they understand the potential risks posed by consenting to their data being shared and used by a third party. We query whether this onus should fall only on the organisation seeking consent though. Whilst that organisation clearly has a strong onus, there could also be a centralised information hub to provide transparency about CDR generally. More generally, we believe a broad public education effort is a prerequisite to delivering a CDR regime that is understood and used safely by consumers.

4.5 To assist with data literacy, consumers should be prompted annually to reaffirm the approvals they have given in relation to transferring and using their data so they can decide if they wish to continue the service arrangement.

4.6 We agree that consent is a crucial element of any proposed CDR and that additional privacy safeguards may be required. We would be interested in further discussions around potential gaps under the current and impending Privacy Acts, and what additional privacy safeguards might look like.

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

4.7 The appropriate place for housing overall principles for the type of principles-based regime we are recommending is primary legislation or, potentially, secondary legislation that applies across sectors.

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

4.8 We agree protecting the interests of vulnerable consumers must be part of the CDR design.

4.9 The CDR needs to be considered in conjunction with the government's wider digital inclusion strategy and the Human Rights Commission guidelines. The API Centre has also developed a section on vulnerable consumers in their consent guidelines. Some initial considerations we think need addressing are: What is a "vulnerable consumer" in the context of a CDR? How many vulnerable consumers will be accessing this technology?

How much do (or don't) vulnerable groups overlap with 'digitally excluded' groups (i.e. those without access to the relevant technology or skills to use digital tools)?

4.10 Care must be taken not to create a new disadvantaged group from those that haven't built up 'a portfolio' of 'good' data and who then get excluded from the data economy.

4.11 At present, banks advise customers not to click on email or website links and then enter their banking login credentials to combat phishing attacks. The online customer journey for the legitimate new open banking processes can be problematic to distinguish from the illegitimate processes we advise customers against. This opens consumers up to fraud risk, as phishing websites may pose as legitimate open banking websites.

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?

4.12 We agree that it is important to have (and publish) a clear understanding of Maori principles and views on data and ownership to assist the design, and ensure that those principles and views are respected in the CDR.

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

4.13 We agree that it is important the CDR should state data holders and third parties must have processes and controls in place to support the needs of disabled people or those with accessibility issues.

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?

4.14 In our view the starting point should be getting a CDR to work for New Zealand consumers first. Alignment with useful elements of other jurisdictions should be a secondary priority.

4.15 However, the NZ CDR legal framework should be aligned to GDPR, as the international gold standard for data protection. The same does not hold for tech standards, as there is no single international standard. That said, the Payments NZ API Centre standards have benefitted greatly from adopting the proven UK Open Banking Standards as their starting point, then modifying for New Zealand content (e.g. account number formats) and needs (e.g. third parties saw the need for an enduring consent for payments to reduce consumer authentication friction).

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

4.16 The Privacy Act already regulates how personal information must be collected, stored, used, shared and deleted, so is a natural starting point to consider for additional regulation of CDR data. However, the Privacy Act may not be such a natural home for any provisions relating to non-personal information or matters beyond data privacy. It is hard

to determine where CDR rights would sit best without knowing more about the content of those rights. We suggest that this question be revisited once the parameters of a CDR are defined more tightly.

4.17 The key requirement is that all laws are consistent, both internally and with other laws. NZ should avoid having overlapping laws that treat a common issue in two different ways.

4.18 As discussed above, we consider "product data" to be distinct from a CDR, so could be dealt with elsewhere, and we do not consider a business data right an initial priority.

4.19 There is an existing mechanism under the Privacy Act which could be used as part of implementing a CDR: Privacy Act Codes of Practices.[6] They allow the Privacy Commissioner to:

- Prescribe more or less stringent privacy standards than exist under the Information Privacy Principles.
- Restrict application to specific classes of information, organisations, activities and industries.
- Prescribe procedures for dealing with complaints of breaches of the Code.
- Establish a review of the Code.

This mechanism appears suited to both Option 2 and Option 3.

4.20 We note that Privacy Act protections only apply to individuals. This point will need consideration if CDR were to apply to a wider user group.

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

4.21 It would be best to start by setting out general principles that any governance body must be able to achieve. BNZ would include the following points in any list of principles. We encourage MBIE to consider this further and publish a list of relevant principles:

- One central body should sit at the top, with overall responsibility for CDR.
- The body should be comfortable with, knowledgeable about, and experienced at running a large-scale technology delivery project; that is what ecosystem participants will be asked to deliver.
- The body should be consumer focused. There is a risk that businesses, both large and small, could capture the CDR agenda.

[6] See Part 3 Subpart 2 of the Privacy Act 2020

- The body must be familiar and comfortable working with businesses in a collaborative way, rather than through enforcement mechanisms.

- The body should be capable of doing the foundation preliminary work to set social policy targets that CDR participants can work towards achieving.

4.22 Once the principles are established, the Government could assess existing regulators and entities to see whether any fits the requirements. If not, a new body should be formed. If an existing body is used, it will need to be allocated further resources (as noted in paragraph 71 on page 25 of the Discussion Document).

4.23 The governance body or bodies will need to be responsible for supporting a CDR ecosystem, developing and publishing data standards, assisting with implementation guidance, accrediting data users (including their ongoing certification), and monitoring compliance. Given this range of tasks and the range of sectors regulation could apply to, the central body may want or need to delegate out specific activities, whether generally or for a specific sector. Again, delegation could be to an appropriate existing body, if one exists, or to a new body or partner.

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

4.24 Informed by our understanding from Australia, BNZ considers that having overall governance sitting with two agencies should be avoided. The issue appears to be that there is a greater risk of lack of alignment, so gaps/problems can arise. It also diffuses responsibility and prevents having one final decision maker.

4.25 While there should be a single body in charge of governance overall, it could perhaps delegate certain tasks or areas. See our previous answer for more thoughts on delegation.

4.26 Also, there is a growing body of feedback that a competition regulator may not be the right body given a CDR is largely a technology-based privacy and data implementation project. Moreover, a CDR regime will require collaboration within and across each industry that is designated as a CDR sector. This would be a challenge for any competition regulator, whose role inevitably involves independent monitoring of the nature and extent of collaboration amongst competitors.

4.27 As evidence of these points, the Australian Treasury is now consulting on a change to the governance framework for CDR. Specifically, they are proposing that the detailed rule-making and sector designation powers move from the Australian Competition and Consumer Commission (ACCC) to the Department of Treasury.

4.28 We understand that having a single entity - the Open Banking Implementation Entity - in the UK worked well from an implementation perspective, but the banks had to fund it. This wouldn't seem equitable for an industry wide consumer data right initiative in NZ.

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

4.29 One of our key themes is the need for clarity on the intended benefits of a CDR and we have discussed this throughout this response. We feel very strongly that the effectiveness of the end CDR will benefit greatly from work put in up front on what success looks like at each point down the track. This means expanding on the general benefits and outcomes outlined throughout the Discussion Document to create a set of specific, base-lined, measurable outcomes. This will help both the drafting of the legislation (to focus on driving the desired benefits vs. 'nice-to-haves') and sensible phasing of delivery. Equally, once the CDR is in place, all participants - including data holders, third parties, CDR governance bodies, and regulators - can work together to support delivery and measure effectiveness of those outcomes for New Zealand.

4.30 A starting point could be to break out the benefits listed in the table at paragraph 16 on page 10 of the Discussion Document into measurable activities:

- what's the relevant baseline?
- what's the measurable improvement desired from a CDR?
- at which points in time?

That could be accompanied by assessing whether further proposed benefits should be added (and then, if added, also measured against these criteria).

END.