

24 July 2023

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

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 Exposure Draft of the Customer and Product Data Bill (**Draft Bill**), and the accompanying Discussion Document in relation to a proposed Consumer Data Right (**CDR**).

ASB supports the objective of providing New Zealanders with greater transparency and control over their data and improving their financial wellbeing. ASB also supports new initiatives which promote competition within the financial services sector and facilitate innovation of and improvements to consumer products and services. With those objectives in mind, the opportunities and risks of a proposed CDR should be carefully considered.

The Draft Bill and related regulations should be carefully designed to ensure that consumer benefits are maximised, in a way which appropriately protects customers' privacy, while providing clarity for participants in a CDR regime and avoiding unnecessary or duplicative compliance costs.

ASB's submission is annexed to this letter. In summary, we submit that the CDR regime should:

- A. Protect customer information and money:** To suitably protect consumer data from fraud and scams and to and mitigate the risk of privacy breaches or unauthorised access, it is critical to ensure that robust data security standards apply for all accredited requestors. In particular:
- i. All recipients of customer data and product data should be subject to appropriate safeguards under an accreditation regime. Non-accredited requestors (who are not required to comply with the CDR) should not be permitted to receive data under the CDR regime (whether from accredited requestors or by making requests directly).
 - ii. Data holders should not be required to provide machine-readable CDR data directly to customers (who may not have sufficient processes for receiving and safeguarding such information, and who may inadvertently transfer that data to unauthorised third parties). This would not affect customers' other existing rights to access information.
 - iii. At the same time, it is critical that those initiatives do not undermine consumer safety and protection. That should include imposing clear data minimisation requirements which limit the data provided to accredited requestors to that which is strictly necessary

for the provision of the requestor's relevant products and services, and ensuring that data cannot be used by requestors for unrelated purposes such as data analytics.

- B. Minimise regulatory overlap:** To avoid duplicative compliance requirements and unnecessary complexity, it will be important to minimise any potential overlap between the proposed CDR regime and other legal frameworks. In particular:
- i. The Draft Bill should be updated to make clear how it interrelates with existing laws (including laws governing data privacy, competition, consumer rights and financial services and AML and CFT obligations). We describe some of those overlaps in paragraph 3 of our submission.
 - ii. Given the risk of overlap, it will be vital to establish clear protections for data holders when acting in accordance with data requests under the CDR. In particular, service providers should be protected from liability under other legal frameworks if they have acted in good faith and complied with CDR obligations (equivalent to section 56GC of the Australian Competition and Consumer Act).
- C. Impose reciprocal obligations:** The obligations to provide customer data should be reciprocal as between data holders and accredited requestors. As in the Australian CDR regime, accredited requestors should be required to share customer data as if they were also designated data holders. Reciprocal data flows are necessary to facilitate fair competition in the financial services sector, enabling a wider range of innovations by both data holders and others who provide data-enabled products and services, and creating greater benefits for customers.
- D. Exclude "derived" data:** Derived data is the result of intricate analysis of data using proprietary methodologies developed by businesses. It often represents a significant investment of time, resources, and expertise. Including such data within the scope of the CDR regime risks undermining intellectual property rights in derived data, and may also create a "chilling effect", stifling further technological advancements within designated sectors. Derived data should accordingly be expressly excluded. Alternatively, New Zealand could adopt the Australian approach, by permitting disclosure of derived data but on a voluntary basis. Requests for voluntary disclosure of derived data could be subject to different thresholds (and potentially fees) to ensure accredited requestors do not attempt to misuse the CDR to gain unfair access to proprietary information.
- E. Set practical standards:** ASB is pleased to see that the Discussion Document recognises the value of ensuring that technical standards for the banking sector are consistent with existing industry standards (including the Payments NZ API Centre Standards), which we consider will assist with ensuring efficient delivery of the CDR. However, we are concerned to see that the provisions of the Draft Bill which govern the consultation process for introducing standards and new designations (sections 61 and 88) do not mention data holders among the other listed stakeholder groups. In our view, data holders will be best placed to comment on the design of standards (as the parties who ultimately have to implement those standards) and we recommend expressly referring to data holders in those provisions.

In our view, adopting these recommendations will help to create a CDR regime that is secure, reliable and beneficial to New Zealanders. In addition to ASB's submission, ASB has also contributed to the

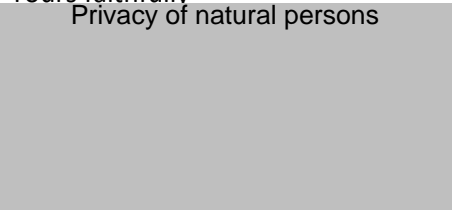
New Zealand Banking Association's and Payments New Zealand API Centre submissions and endorses the views and recommendations made therein.

ASB is keen to engage further with MBIE on the CDR proposal and subsequent development of the regulations and standards, to ensure that a resulting CDR regime can best achieve the sought objectives while maintaining sufficient safeguards and consumer protection.

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.

Yours faithfully

Privacy of natural persons



Stephen Bendall
General Counsel and EGM Business Services
ASB Bank Limited

Submission by ASB on the exposure draft of the Customer and Product Data Bill and the Discussion Document

1. Introduction

- a. ASB is supportive of the objectives of providing New Zealanders with greater transparency and control over their data and improving their financial wellbeing.
- b. In order to promote such objectives ASB has been supporting various data initiatives for some time, including:
 - i. ongoing improvements to managing the privacy of our customers' data;
 - ii. supporting Payment NZ's account switching rules,
 - iii. implementing digital identity practices to support compliance with Anti-Money Laundering (AML) obligations including Know Your Customer (KYC) requirements; and
 - iv. contributing to the development of the Payments NZ API Centre standards and standardised partnering framework.
- c. An effective CDR framework will need to ensure that customers' privacy is protected by appropriate safeguards, and that obligations for participants in the CDR regime are clearly defined (including as to their relationship with other statutory duties) in a way which minimises unnecessary or duplicative compliance costs. More broadly, there is a need for aligned and widespread consumer education on the benefits of CDR in the context of safe data-sharing practices, to instil consumer confidence and uptake of the scheme.

2. Protection of customer information and money

- a. To protect consumer data and maintain public trust in a CDR regime, it is crucial to set robust security standards for accredited requestors involved in data sharing. Stringent requirements regarding data handling, storage, and encryption must be established to mitigate and monitor the risk of data breaches or unauthorised access.
- b. In particular:
 - i. **Security standards:** Accredited requestors, who are granted access to customer data upon request, must be subject to rigorous data safety protocols to ensure the protection of individuals' privacy. The increasing prevalence of scams and fraud in the digital marketplace highlights the urgency of implementing comprehensive security measures. ASB agrees that such safeguards should include:
 1. "fit and proper person" obligations for directors and senior managers of all accredited requestors;
 2. Insurance obligations (which should be prescribed and should take account of the full range of potential liabilities arising from claims arising from loss of data or non-compliance with the CDR obligations);

3. Prescribed IT security obligations which reflect industry best practice, with requirements to promptly implement updates as relevant standards evolve.
 - ii. **Mandatory Accreditation:** Non-accredited requestors (who are not required to comply with the CDR) should not be permitted to receive CDR data. ASB does not agree with proposed section 21 of the Draft Bill, which would create a requirement to provide designated product data to any person. Obliging data holders to share data with non-accredited entities (who have not contributed to the data exchanged under the CDR regime or the costs of that regime) undermines the fundamental purpose of the CDR framework (i.e. secure data transfers to reliable and accountable third party recipients). That draft obligation appears particularly onerous in the absence of clear limits on the scope of “product data” (currently broadly defined in section 9 of the Draft Bill). We submit that product data should instead be carefully defined and limited to information about products that is publicly available (for example, information about lending products, interest rates and fees which are available on a bank’s website), similar to the approach taken in Australia.
 - iii. **Appropriate Limits on Access:** Data holders should also not be required to share machine readable data directly to customers themselves (as proposed under section 14 of the Draft Bill). With ever increasing online security threats and incidents, allowing customers direct access to their data in machine readable format presents a significant cyber security risk. Customers themselves will not have been through accreditation process to vet security systems and allowing system access directly to customer will increase the risk of cyber attacks and similar security concerns. ASB suggests that further consideration be given to this requirement, particularly as to whether it offers sufficient benefit when considering the risks which it may pose.
- c. These measures are critical for ensuring that the CDR regime achieves its intended purpose: the provision of machine-readable data *securely* to trusted third parties via APIs. That can only be achieved by the inclusion of strict security standards, mandatory accreditation for all requestors (and careful limits on the scope of “product data”) and appropriate limits on direct access given the complex nature of machine-readable data and the potential harm arising from misuse or misinterpretation.

Fraud and Scams

- d. Over the last financial year we have seen significant increases in the number of customers exposed to frauds and scams. This trend is expected to intensify as frauds and scams activity becomes more sophisticated. Any CDR regime therefore needs to be robust with appropriate security safeguards to ensure that it cannot be exploited by those involved in fraudulent activity.
- e. The importance of ensuring appropriate security safeguards is highlighted by the recent measures introduced in Australia and the United Kingdom to permit more time for data holders to check recipients’ credentials (following frauds and scams). For example, in Australia, the expansion of the CDR to the telecommunications, superannuation and insurance sectors has been paused until 2024, to allow more time to focus on ensuring that the CDR in banking is working as effectively as possible. Non-bank lending will be the only expansion over the next two years.

3. Minimising regulatory overlap

- a. Given that the banking sector is already extensively regulated across multiple frameworks, ASB submits that it will be crucial to ensure that the new CDR regime minimises any overlap with other existing legal frameworks. Wherever possible, the New Zealand CDR regime should align to and build on existing compliance obligations to avoid duplication.
- b. Regulatory overlap can lead to confusion (for regulators and data holders), duplicative requirements, increased compliance costs, and potential contradictions in legal obligations.
- c. Several areas of regulatory overlap may arise in this context, including:
 - i. *Privacy Laws*: It is vital to ensure that the CDR regime aligns with the Privacy Act 2020 to avoid conflicting obligations. Currently, the Draft Bill only briefly deals with the intersection with the Privacy Act, and does not engage with various detailed questions which require clearer articulation. For example:
 1. The Draft Bill should clarify that, if a breach of a CDR obligation is seen as a breach of an information privacy principle (**IPP**), remedies for such a breach should be limited those available under the Privacy Act (and in particular that section 31 of the Privacy Act continues to apply).
 2. The drafting notes in sections 27 and 48 of the Draft Bill also raise the possibility that a breach of certain CDR obligations may be seen as an “interference” under the Privacy Act, regardless of whether there has been any customer harm. That would create a significant widening of the current approach to liability under the Privacy Act, and should be avoided.
 3. The Draft Bill should clarify whether and how it applies to any applicable codes of practice under the Privacy Act (e.g. the Credit Reporting Privacy Code) and any disclosures of information in accordance with those codes.
 4. The Draft Bill does not clarify whether or how the mandatory notification of data breaches in Part 6 of the Privacy Act applies in relation to CDR disclosures (e.g. if it is discovered that CDR data has been disclosed without an individual’s authorisation) and further which participant makes the notification. We submit that where personal information has been disclosed to an Accredited Requestor, they should be responsible for notification of any privacy breaches in relation to that information (and for the other obligations under the Privacy Act). The Draft Bill should make that clear.
 5. The Draft Bill proposes that the CDR regime applies regardless of “where the customer or product concerned is, or was, located” (section 11(2)(c)). Any obligations under the CDR regime to disclose information to overseas customers should be carefully considered to ensure that they do not inadvertently engage or breach regulatory obligations for

cross-border data transfers under the Privacy Act (or overseas frameworks with extra-territorial provisions such as the EU General Data Protection Regulation (GDPR)).

- ii. *Consumer credit laws:* The Credit Contracts and Consumer Finance Act 2003 (**CCCFA**) imposes various obligations on lenders. The CDR regime should clarify (whether in the Draft Bill or regulations) how those obligations intersect with the CDR regime. For example:
 1. Lenders are obliged to provide assistance to borrowers to enable them to make informed decisions as to whether or not to enter into a consumer credit contract and in all subsequent dealings. It is unclear whether the disclosure of consumer data to borrowers under the CDR would be considered a discharge of those obligations.
 2. Similarly, section 24 of the CCCFA permits borrowers to request disclosure of certain specified information, including loan repayment information, fees and charges. It will be essential to ensure that such obligations are not breached by disclosing information under the CDR regime in a format which (though compliant with the CDR regime) does not conform to the specific requirements the CCCFA.
- iii. *Financial Services Regulations:* It will be essential to consider how the CDR will align with existing financial services regulations, such as the Financial Markets Conduct Act 2013 (**FMCA**). Under the FMCA, financial service providers are already subject to various extensive obligations including under the fair dealing obligations in Part 2, and (from early 2025) new obligations under the 'Conduct of Financial Institutions' (**COFI**) amendments to the FMCA. It will be important to clearly articulate and understand the relationship between those obligations to treat customers fairly and transparently, and related disclosure duties under the CDR regime.
- iv. *Anti-Money Laundering obligations:* Data holders in various designated sectors (including the banking sector) will need to conduct customer due diligence on customers under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (**AML Act**) before opening an account, which may cause a delay or require more information before performing actions under clauses 17 or 18 of the Draft Bill. The Draft Bill should make clear whether the AML Act applies to such scenarios, or whether reporting entities under the AML Act are exempt from the usual customer due diligence requirements where the CDR regime applies.
- v. *Intellectual Property:* Intellectual property laws protect data holders' proprietary information, copyright, and trade secrets. The Draft Bill should include appropriate exclusions for disclosure of any such confidential and proprietary data (such as "derived data") similar to the Privacy Act's right to withhold trade secrets.
- vi. *Competition Laws:* It will be important to ensure that the mandatory sharing of product information and other CDR data does not inadvertently trigger any of the prohibitions on cartel conduct, or any other regulated obligations under the Commerce Act 1986. This should be addressed by creating appropriate exemptions and safe harbour provisions to permit such disclosure.

Risk of resulting liability

- d. In addition, regulatory overlap could result in significant liability for data holders where genuine efforts to comply with the CDR regime result in unintentional breach of other contradictory legal obligations. These matters should be carefully considered and clarified as a matter of priority.
- e. Those risks could be alleviated by ensuring that the CDR regime includes clear protections for data holders when responding in good faith to customer requests under the CDR. This could include introducing a safe harbour provision to provide service providers with immunity from liability under other laws for actions taken in good faith under the CDR regime (equivalent to section 56GC of the Australian Competition and Consumer Act). In our submission, this protection is necessary to encourage data holders to participate actively in data sharing initiatives, and it is also fundamentally fair: data holders should not face unwarranted legal repercussions where they have, in good faith, shared data in accordance with the CDR regime.
- f. The Discussion Document briefly sets that option aside on the basis that “*compliance with an Act should not, as a matter of law, create liability.*” While that may be true in principle, in this particular context (where the CDR obligations will be new and untested, and where they overlap substantially with other detailed regulatory frameworks) there is a very real risk that an action intended to comply with the new regime may constitute the inadvertent breach of another.
- g. Therefore, we submit that the Draft Bill should include appropriate liability protections, contingent upon data holders acting in good faith and complying with the requirements stipulated by the CDR regime. This ensures that any potential misuse or negligent behaviour is appropriately addressed (while data holders may still be held accountable for any intentional wrongdoing or breaches of obligations).
- h. Similarly, where data holders comply with standards and regulations under the CDR regime, they should not be held responsible for data quality issues or customer complaints in relation to that data. Data holders will often have no direct control over data inputs and should not be held responsible for the quality of the data outputs where they have otherwise met the applicable CDR standards.

Declining requests

- i. For the same reasons, rather than being obliged to satisfy all requests on a mandatory basis we submit that it is essential that data holders are permitted to decline requests in certain circumstances as they can under other pieces of legislation for example sections 49-53 of the Privacy Act and other laws such as the new reporting requirements proposed under the RBNZ’s cyber risk framework, and tipping off under AML/CFT legislation.

4. Reciprocity

- a. The Draft Bill does not include a principle of reciprocity. In our view, the obligations to provide data should be reciprocal as in the Australian CDR regime. That is, accredited requestors should be required to share specific CDR data as if they were designated data holders (in order to ensure greater symmetry in the data flows between holders and others who provide data-enabled products and services).

- b. The principle of reciprocity is appropriate, and is essential to maintain fairness and to avoid creating a disproportionate advantage for accredited data requestors. By requiring accredited requestors to adhere to the same data access and sharing obligations as data holders, the CDR would create a more balanced exchange of information would likely result in greater innovation and consequential customer benefits.

5. “Derived” data:

- a. The Draft Bill proposes to include “derived data” within the scope of customer data subject to the CDR regime. Derived data is the result of intricate analysis and processing of raw data, combined with various algorithms and proprietary methodologies developed by businesses. It often represents a significant investment of time, resources, and expertise.
- b. ASB submits that the CDR Regime should exclude “derived” data (being data that has been created by a data holder through the application of insights and analytics) from the scope of potential designation for mandatory data sharing. Derived data plays a crucial role in driving innovation, and enhancing customer experiences.
- c. Including derived data within the scope of the CDR regime would not only undermine intellectual property rights in derived data, but may stifle further technological advancements within designated sectors.
- d. As an alternative, New Zealand could adopt the approach from Australia which delineates mandatory data and voluntary data (derived). Requests for voluntary disclosure of derived data could be subject to different thresholds (and potentially access fees) to ensure customers or accredited requestors do not attempt to misuse the CDR rights to gain access to data holders’ proprietary information.

6. Ensuring standards are practical

- a. ASB is pleased to see that the Discussion Document recognises the value of ensuring that technical standards for the banking sector are consistent with existing industry standards (including the Payments NZ API Centre Standards), which we consider will assist with ensuring efficient delivery of the CDR. Ensuring conformity with existing industry standards and initiatives offers numerous benefits, such as promoting interoperability, reducing implementation costs, and leveraging existing technical expertise. Leveraging the Payments NZ API Centre Standards could (if adapted for other industries) facilitate data portability across various service providers and platforms.
- b. Above all, aligning with the Payments NZ API Centre Standards ensures that the required technical infrastructure is already well-developed and widely adopted. The industry-led design of the Payments NZ API Centre Standards has involved substantial collaboration and consultation among stakeholders in the banking and fintech sectors resulting in robust and well-documented API specifications. This alignment also avoids the creation of duplicative or conflicting technical standards, thereby streamlining operations and promoting greater clarity and uniformity across the industry. Furthermore, these technical standards are a local adaptation of the UK Open Banking standards that have already been in use for a number of years.

- c. However, we are concerned to see that the provisions of the Draft Bill which govern the consultation process for introducing standards and new designations (sections 61 and 88) do not mention data holders among the other listed stakeholder groups. In our view, data holders will be best placed to comment on the design of standards (as the parties who ultimately have to implement those standards) and we recommend expressly referring to data holders in those provisions.
- d. Timing of the development of standards is also important. As MBIE has indicated, the substantive detail will be included in the regulations. Therefore, early indication as to what is contained in the standards is important to ensure industry has sufficient time to scope, fund, build and implement robust business solutions to enable the CDR regime, particularly with other elements of regulatory change, notably the introduction of Deposit Takers Act.

7. Other matters

- a. *Regulatory model:* ASB would welcome further clarification on the proposed framework for regulatory oversight (including ongoing maintenance and oversight of the scheme and standards) involving MBIE, the Privacy Commissioner, and potentially the establishment of a new dispute resolution scheme. While the Draft Bill does not confirm details at this stage, we are concerned that a “multiple-regulator” structure may not lead to good customer outcomes (as dealing with disputes will be delayed and hard to navigate). We submit that the roles and responsibilities of the relevant regulators should be clearly defined in the Draft Bill so that participants are clear on which regulator to engage with.
- b. *Industry guidance and support:* Regulatory bodies should provide comprehensive guidelines and support materials to assist data holders and other participants to understand their obligations under the CDR regime. Regular reviews and consultations should be conducted to ensure the ongoing relevance and effectiveness of these guidelines and standards.
- c. *Staggered implementation:* We consider that a staggered approach to implementation of a new CDR regime, phasing it in gradually over time, will be essential to the success of such a regime. ASB understands that unrealistically short implementation timeframes in the UK and Australia resulted in poor customer outcomes for a significant period following implementation.
- d. *Penalties:* We appreciate that the Draft Bill does not yet outline the specific remedies or enforcement options for breach. However, based on the comments in the Discussion Document regarding the proposed tiered approach, we are concerned that there is a risk that the CDR regime will impose significant penalties for potentially minor, technical, or inadvertent issues (even where unlikely to result in any customer harm). That may discourage participation in the regime, and we submit that the Draft Bill should clearly delineate between different levels of contraventions. In particular, we note that the examples given for “Tier 1” and “Tier 2” breaches are identical, including for example “Failure to maintain transaction records”, even though significantly higher penalties apply for Tier 2 (commensurate to the most severe penalties under the CCCFA) than for Tier 1.
- e. *Compliance policies:* We question whether there is any value in mandating the adoption of specific CDR compliance policies (as proposed under section 42 of the Draft Bill).

Given that many businesses already publish terms and conditions and privacy policies (among other policies) imposing additional duties to publish CDR policies may lead to “policy fatigue” for consumers, and additional administrative burdens for data holders with little corresponding benefit. We consider it would be preferable to allow data holders to have discretion as to how they address the CDR within their existing policy frameworks.

- f. *Consent for de-identification:* We strongly oppose any requirement to oblige data holders to seek consent from customers before de-identifying information. That requirement is unnecessary and contrary to the approach permitted under the Privacy Act (which is limited to “personal information”; i.e. information about an identifiable individual). The Privacy Act includes specific exemptions for the use of de-identified information for research or statistical purposes, which is a widely accepted practice. Requiring explicit consent for de-identification would unduly restrict the valid uses of anonymised data, limiting the ability to derive beneficial insights. On that basis, we submit that option 1 on page 39 of the Discussion Document (ethical requirements for accredited requestors) is a strongly preferable method of safeguarding customer data.
- g. *Te ao Māori:* ASB acknowledges the significance of tikanga considerations, which are prominently recognised in the Draft Bill. However, it is important to ensure that such considerations are clearly explained within the legislation, and that any intended differences in approaches to Māori customers (who are referred to separately from general "customers" under section 60(1)(a) of the Draft Bill), are plainly articulated. That will help avoid inadvertent compliance breaches and promote a clear understanding of the obligations and rights concerning Māori data subjects.

Thank you for the opportunity to participate in this consultation. We are available for further discussions or to provide clarification on any of the submissions above should MBIE require.