Submission

to the
Ministry of Business, Innovation and Employment
on the
Open banking regulations and standards under the
Customer and Product Data Bill

10 October 2024

Prepared by the Policy and Regulatory sub committee of Digital Identity NZ's Executive Council comprising volunteer member organisation representatives from a mix of large and small businesses.

Email: info@digitalidentity.nz **Phone** + 64 9 394 9032
Digital Identity New Zealand, c/o New Zealand Tech Alliance, PO Box 302469, North Harbour, Auckland 0751, New Zealand

Digital Identity New Zealand (DINZ) thanks the Ministry of Business, Innovation and Employment (MBIE) for the opportunity to provide a submission on the open banking standards and regulation.

We continue to support the overall intention of the proposed legislation and designation rules: to support customers realising the value of their customer data to promote competition and innovation for the long-term benefit of customers; and to facilitate secure and efficient data services.

Nonetheless there are areas where our members offer precautionary notes and specific concerns where the designation rules could be improved to achieve the intended outcomes.

As always, we are happy to provide any clarifications in writing, on a call, or in a physical meeting.

DocuSigned by:
Colin Wallis
F84DA1755B8C410...

Colin Wallis
Executive Director,
Digital Identity NZ
M +64 21 961955 Wellington

About Digital Identity NZ (DINZ)

DINZ is a not-for-profit, membership-funded association of approximately 100 organisations across the public and private sectors, representing a variety of industries as well as individuals. Recognised as the foremost industry voice for Digital Identity in NZ, it is part of the New Zealand Tech Group (NZTech), connecting the digital identity community and seeking to actively influence policy and solutions. DINZ members help facilitate digital identity and digitisation across the board in instances such as public-facing government services, open banking, account opening and customer & product data under consultation here, which are all underpinned by digital identity in concert with AI, biometrics and cloud computing. Some members deploy digital ID and verification software and related solutions both in NZ and other countries, others rely on, or consume them.

Relevance to DINZ

We appreciate that the CPD Bill would give under the banking designation an accredited requestor, with the consent of the customer, access to certain customer and product information which is held by the data holder. Certain rules protecting the circumstances for which that request can be made, how consent is given etc is therefore necessary to ensure customer data is used appropriately and data is safe and secure. We also appreciate that certain standards for data and communications are needed insofar as they support consistency in the safe and secure sharing/exchange of customer and product data between the data holder and the accredited requestors. In the context of Open Banking, these standards have so far been set by PaymentsNZ for the safe and secure sharing of data between banking members which has been successful in establishing and implementing shared API protocols and best practice. We appreciate that the implementation of these rules, however, has not been as fast as some industry participants and parts of government would like. As an industry body with a sizable cohort of identity and access solution providers, we wish to convey another aspect for which MBIE should consider as relevant in establishing the designation rules.

Email: info@digitalidentity.nz **Phone** + 64 9 394 9032
Digital Identity New Zealand, c/o New Zealand Tech Alliance, PO Box 302469, North Harbour, Auckland 0751, New Zealand

The identity layer that enables access into an organisations data repository (traditionally known as Identity and Access Management (IAM) systems and initially used in the enterprise prior to being extended to the broader consumer ecosystem) provide a gateway to an organisation's data repository and can manage digital identities, grant access, and assign privileges to users based on certain attributes. Nowadays best practice approaches IAM on a 'zero trust' basis which digital systems can make possible through assigning role-based-policies whereby only those with a need-to-know basis can access data and systems needed to complete their work. This is not dissimilar to how a paper-based access policy would work, but with digital systems, roles and permission levels can be assigned and revoked fast and in near-real time.

IAM platforms do not cater well for scenarios where identity and access permissions are determined by external parties directly. Sometimes an identity user policy, for example from a federated social media platform, is used to confirm the identity of the requesting party (sometimes called identity pools). As envisaged here in the CPD bill with open banking, an additional layer is introduced whereby the individual for whom would usually have access to their customer data is delegating this authority to a third party (i.e. accredited requestor). Without adequate mechanisms to claim, validate, verify, and express the accredited requestor's identity, timely processing of consumer and product data is challenging at scale. Therefore, getting the roles-based permissions right up front will be important to the bank, as will determining how the validity (in-real time) of the accredited requestor's request. Without this the bank may not know that the accredited requestor has had consent revoked or its accreditation removed. This is where the Digital Identity Services Trust Framework and associated rules ('DISTF rules') as well as the attributes, metadata and exchange format for verifiable credentials are relevant and must be developed in parallel because they will be vital in the up-to-date accreditation required for the trusted requestor.

Our understanding to date has been that neither the DISTF rules nor MBIE's designation rules accommodate this situation today, because what little is known about the DISTF pilots is that they are currently 3 party - Issuer (e.g. RealMe),

Customer with Holder App and Verifier/Relying Party (e.g. Bank). We urge MBIE and DIA to work closely together and publish a perspective on this including how an accredited requestor could become a trusted relying party under the DISTF rules. In doing so, then real use cases where data is open across government (e.g. MyIR, MyMSD), which may be just as important to a customer as its banking information, can be accessed by a comprehensive and trusted (in real time) accredited requestor.

Opening statement

DINZ joined forces with FinTechNZ to host a 'town hall' styled dynamic submission webinar for MBIE on July 17, 2023 in response to the initial consultation and on the Draft Exposure Bill. Alongside our overall support, matters raised there look to be reflected in the Bill, for which we are grateful. Precautionary notes and specific concerns follow, to further frame our support for the designation rules.

Precautionary Notes

Do not assume 'we'll build it and they will come':

Banks and electricity retailers simply opening up their books for accredited requestors to be able to request information (or request a transaction be made on their behalf) is simply one side of the equation (although evidence on why these were the first designated sectors seemed absent from the consultation documents). A strong cohort of competitive third-party data requestors, where the customer has a choice between multiple requestors to authorise data access and transactions is another side. But a bigger picture emerging is how customers are informed, empowered to act on this information and given options to choose from a range of suppliers and at a minimal cost. (Many third party providers charge a subscription fee to the customer, so access to data is not free even if the bank is mandated to make fulfilment of the request free up to a point. In some cases subscriptions can be quite expensive and prevent uptake – or prolonged uptake – of a service.)

Customers will need to be informed in order to choose (and have a strong ongoing consent mechanism - the international standards, formats and message protocols for which are not yet widely adopted in NZ) with third parties. How this ongoing consent mechanism works should also be carefully considered within the Digital Identity Services Trust Framework. For now, we understand MBIE is suggesting an 'opt out' consent approach. From an ethics viewpoint this is highly questionable, and that aside, is not ideal given an accredited requestor could potentially have broad and unfettered consent in place and requesting data which is beyond the customer's ongoing needs or understanding. Negative public perception arising from these shortcomings could adversely impact adoption. These accredited requestors should also ideally have services that can enhance their offering across a customer's data footprint, according to the customer's desire for integration across transactions like taxes, bank accounts, budget services etc. To do that, others outside of the designated sector should be included within the CPD - something that the NZ Commerce Commission highlighted in its recent report: A stronger Kiwibank and open banking could shake up NZ banking sector, 20 August 2024. Again, negative public perception around the scope of benefit could adversely impact adoption.

Foster a competitive environment:

For a good supply of data requestors there needs to be not only sustainable business value for them but also the regulations that support this legislation will need to be internationally interoperable (i.e. use international standards for information sharing). Without this, New Zealand providers will develop solutions that cannot interoperate and be sold overseas. Furthermore, an international-standards and interoperable regulatory system will mean off-the-shelf solutions can be offered in the New Zealand market, supporting a more innovative and cost-effective ecosystem whereby New Zealand customers benefit from a competitive range of solutions.

Learn from overseas regimes:

We urge caution in rushing with the rules where arguably the detail is most important to the successful implementation of the CDR. In rushing, MBIE risks pushing this on to the market before fully appreciating the current landscape

and lessons learned from overseas. It appears MBIE is following a path forged by the UK and Australia, with a view that increased data sharing would offer the potential for greater competition, enable the development of alternative business models, and provide transparent and comparable information about pricing and products in order to inform customers in their purchasing choices. A worthy pursuit but it needs careful implementation and consideration.

Australia right now is undergoing a review of its CDR legislation and learning that the supporting regulations are just as important as the legislation itself to deliver on the intent. That there has been low (although estimates at around 0.3% are likely to be largely understated) uptake, and this may be in large part because of the carve out of derived data. The Australian banks have spent an estimated $1.5b on implementing and operating the CDR regime.

The experience in Australia over the nearly four years is not encouraging. Implementation costs were substantially higher than predicted, as are operational costs. Uptake has been described as “extremely low”, with no evidence that any of the desired outcomes will be realised. The Assistant Treasurer Stephen Jones, Australian Government, describes their CDR experience as “It’s a good idea, poorly executed”. Much of the execution is prescribed in the Act, similar to the NZ Bill. We need to learn and not just copy, to achieve the success we all want to see.

CPD’s relationship with other regulations and sectors:

It’s clear that there has been some consideration of identity verification of all entities in the chain in advance of customer consent to authorise sharing, but the Bill’s intent is much less clear in pinpointing that it needs to be designed in and implemented from before the start of any data exchange. Enacting this Bill without the proper data exchange could attract fraudsters and scammers keen to take advantage of new systems that hold personal data, to be used for future nefarious purposes. Any breach of this ecosystem will erode trust immediately.

In this Discussion Paper - Open banking regulations and standards under the Customer and Product and Data Bill published by MBIE in August 2024 and the subject of this submission - we note that ‘Officials from the Department of

Internal Affairs and the Ministry of Business, Innovation and Employment are working together to ensure alignment between the DISTF and the Bill to fully realise the benefits of both initiatives and minimise compliance costs for system participants'. While this is laudable and welcomed, it must be appreciated that the DISTF has only just come into force (1 July 2024) with the rules still being worked through the legislative process by the Department of Internal Affairs. While we all hope for the best outcome and the DISTF is widely adopted, it's too early to estimate adoption. There's no question that on the face of it, the principles can be aligned, but it's less clear that DISTF's full suite of standards can be adopted uniformly in every sector. The first designated sector is banking and it's easy to see how the CPD Bill augments open banking use cases in that sub sector of banking. However, the established international standards, protocols and code libraries for open banking that enable cross border interoperability in that sector are not identical to the standards suite underpinning the DISTF, even if the essential parts needed for conformance and interoperability were capable of being mapped. If it came to pass that Payments NZ's API suite used those open banking standards, protocols and code libraries for its identification, verification authorisation and consent, and in turn banks used those for their open banking deployments rather than the DISTF standards suite then the future take up of CDP in this sub-sector might be impacted.

For a good supply of third-party data requestors, the regulations that support this legislation (and DISTF) will need to be internationally interoperable (i.e. use international standards for information sharing). Without this, New Zealand providers will develop solutions that cannot interoperate and be sold overseas. This legislation potentially drives IT related spending, so it could be good for those DINZ members who develop software and services in the digital identity ecosystem to serve this demand. Furthermore, an international-standards and interoperable regulatory system will mean off-the-shelf solutions can be offered in the New Zealand market, supporting a more innovative and cost-effective ecosystem whereby New Zealand customers benefit from a competitive range of solutions. This was another lesson learned from the Australia CDR.

Specific Concerns:

- We understand that data holders or accredited requesters will be required to maintain policies relating to customer data, product data, and action performance. We believe that as far as it is relevant to the intent of this regulation, to improve access to customer data, these policies can serve as a way for an organisation to gain trust and provide further transparency to its customers.

- We caution against issuing prescriptive guidance and unnecessarily burdensome requirements, such as publishing geographical location of data and in such a case leave it to accredited requestors to assess their security controls and risk posture and decide. Requiring accredited requestors to disclose where they store customer data could create significant security risks. This information could be exploited by bad actors to target those data storage locations for malicious activities. Furthermore, mandatory disclosure could incentivise companies to store data in less secure locations for perception reasons, rather than prioritising robust cybersecurity.

- We instead recommend that the regulations set the clear expectation that data holders' and accredited requestors' data policies will articulate how they comply with existing data protection requirements under the New Zealand Privacy Act 2020; e.g. requiring the accredited requestor to confirm compliance with the NZ Privacy Act. New Zealand's existing privacy principles already provide consumers transparency on how their data is collected, used, and secured. Accredited requestors could confirm that information has been disclosed to a recipient located in another jurisdiction and confirm whether that jurisdiction has comparable privacy safeguards.

- It is unclear why MBIE has proposed an additional location disclosure requirement beyond the requirements set by the Privacy Act. It seems misaligned with the approaches taken in Australia and the UK, where open banking is already established. We understand that MBIE would like to maintain as much parity as possible with international open banking frameworks, and this disclosure requirement may have the undesired effect of misaligning NZ's framework with current international practices.
- The current approach to derived data in the CPD Bill could severely restrict how small businesses share their data with trusted third parties, such as accountants or connected apps. This part of the open banking regulations should also be aligning with the existing Privacy Act framework, enabling customers to share derived data freely once it has been transferred with their consent. This alignment will help avoid stifling innovation and ensure the CPD regime is workable for all participants.

Email: info@digitalidentity.nz **Phone** + 64 9 394 9032
Digital Identity New Zealand, c/o New Zealand Tech Alliance, PO Box 302469, North Harbour, Auckland 0751, New Zealand

Appendix A: Supporting Notes

Australian CDR research key points (see Appendix C for the reference):

- Implementation costs between $1m to $100m for data holders. Annual operating costs levelling off at ~$3000 per customer.
- Data Schemas do not vary greatly from existing access to data customer exported queries and downloadable statements.
- Fintech startups find the prescriptive system constraining.
- Low uptake with high churn and early deceleration. Slowing down rollout to other industries while viable use cases are developed.

Note: References to “Increased Data Sharing” or similar constructs presumes data is an asset that is held by the data holder for the data subject. That is technically inaccurate. Businesses collect and store information about their business activity, which is a data asset that they create, own, and maintain. It contains information about the data subject (customer), but they are not providing a “data holding” service. Consequently, data is shared with customers and 3rd parties when there is value in doing so. The competitive market determines when data sharing is worthwhile. There is substantial data sharing with consumers by data holders. Within legal guardrails and where there is an economically viable use case, data is shared between industry players and competitors.

Email: info@digitalidentity.nz **Phone** + 64 9 394 9032
Digital Identity New Zealand, c/o New Zealand Tech Alliance, PO Box 302469, North Harbour, Auckland 0751, New Zealand

Appendix B: Examples of data holders sharing their data with consumers or other industry players.

- Financial: Customer Online Services (queries, exports, statements), data feeds to personal accounting services such as Xero, MYOB, and others. Identity and Access Management Permissions for Accountants to access client accounts and information, and more. Open Banking will expand this further. Broking Accounts provide access to raw data as well as data analysis.

- Power: Customers have access to their data through the online portals, this includes usage, billing payments history, etc. Comparison sites for informed choices exist such as PowerSwitch and SwitchMe, Power Compare, Consumer NZ papers, etc. Also the Electricity Authority's registry under the Electricity Industry Participation Code 2010. It would seem that customers being able to first access and utilise information in the registry through an intermediary agency run by the government could serve the interests of making price comparisons of power and regulating the competitive pricing across power providers.

- Telcos: TM Forum's eTom and SIDs enable global integration of service provision to the individual.

- Health: Konnect provides real time insurance approval of medical expenses, Health 360 provides sharing of prescription, tests, medical history between health providers. Health monitoring devices such as smart bands enable the download of data collected by the user.

- Nearly all providers of products and services offer online registration, account & profile management, and access to customer information directly with the customer. CRM's (Customer Relationship Management) are integrated with e-commerce.

Appendix C: References

Australian CDR Cost review:
https://treasury.gov.au/sites/default/files/2024-08/p2024-512569-report.pdf

Accenture research for Australia Banking Association:
https://www.ausbanking.org.au/wp-content/uploads/2024/07/CDR-Strategic-Review_July-2024.pdf